



## O TRATAMENTO DE DADOS DAS CRIANÇAS E ADOLESCENTES CONFORME A LEI Nº 13.709/2018 E A PROBLEMÁTICA DOS BRINQUEDOS CONECTADOS

Laura Regina Echeverria da Silva \*

Marcelo Mazin\*\*

Valter Moura do Carmo \*\*\*

### RESUMO

O objetivo do presente estudo consiste na análise do tratamento dos dados pessoais de crianças e adolescentes, o papel da família e a problemática dos brinquedos conectados. Por meio do método dedutivo, analisa-se de forma documental e bibliográfica, a Lei nº 13.709/2018. Essa análise propõe um maior resguardo à privacidade das crianças e adolescentes. O crescimento das interações eletrônicas, principalmente em momentos de pandemia, deve se desenvolver em um ambiente Seguro com adoção de mecanismos que propiciem o acesso dos usuários a sites e plataformas seguras, sem abusos.

**PALAVRAS CHAVES:** Dados pessoais. Crianças e adolescentes. Privacidade. Segurança. Brinquedos conectados

### THE PROCESSING OF DATA ON CHILDREN AND ADOLESCENTS IN ACCORDANCE WITH LAW NO. 13.709/2018 AND THE PROBLEM OF CONNECTED TOYS

### ABSTRACT

The objective of this study is to analyze the treatment of personal data of children and adolescents, the role of the family and the problem of connected toys. Through the deductive method, the Law 13.709/2018 is analyzed in a documental and bibliographical way. This analysis proposes a greater protection to the privacy of children and adolescents. The growth of electronic interactions, especially in times of pandemic, must develop in a safe environment with the adoption of mechanisms that provide the access of users to safe sites and platforms, without abuse.

**KEY WORDS:** Personal data. Children and adolescents. Privacy. Security. Connected Toys.

\* Doutoranda em direito pela Universidade de Marília. Mestre em Direito pela Universidade de Marília. Mestre em Responsabilidade Civil pela Universidade de Girona (Espanha). Pós-graduada em Registros Públicos e em Direito e Processo do Trabalho.

\*\* Doutorando em direito pela Universidade de Marília. Mestre em Direito pela Universidade de Marília. Pós-graduado em Registros Públicos e em Direito e Processo Penal.

\*\*\* Doutor em Direito pela UFSC. Pós Doutor pela Universidade de Marília. Professor Assistente Doutor da UNIMAR. Diretor de relações institucionais do CONPEDI. Membro da Comissão de Estudo de Identificação e Descrição da ABNT.



## INTRODUÇÃO

O presente trabalho tem como tema o tratamento de dados das crianças e adolescentes conforme a Lei nº 13.709/2018 e a problemática dos brinquedos conectados, a importância da citada legislação que traz uma mudança de paradigma no tocante ao tratamento dos dados pessoais, o necessário acompanhamento dos pais ou responsável legal na proteção dos dados das crianças e adolescentes e como se dá o manejo de tais dados conforme a nova legislação.

Nota-se que a preocupação com a proteção de dados pessoais é uma crescente no mundo. A União Europeia em 04 de maio de 2016 publicou o GDPR (*General Data Protection Regulation*- EU 679/2016), o qual é o sistema regulatório de proteção de dados pessoais dos cidadãos da zona comunitária.

O regulamento de proteção de dados europeu é de aplicação uniforme nos 28 países membros da União Europeia, bem como em outros três nações do EEE (Espaço Econômico Europeu), são estes Noruega, Islândia e Liechtenstein.

Tal normativa serviu de inspiração para a Lei nº 13.709/2018 (LGPD- Lei Geral de Proteção de Dados, alterada pela Lei nº 13.853/2019) a qual regulamenta no Brasil o tratamento dos dados pessoais de seus cidadãos.

A LGPD entraria em vigor no ano de 2020, com a alteração trazida pela Lei nº 13.853/2019, pois em seu artigo 65 foi estabelecido que esta vigorará após vinte e quatro meses de sua publicação, a qual ocorreu em 15 de agosto de 2018 e trará regulamentações para inúmeras condutas que tratam na coleta, armazenamento, compartilhamento, eliminação de dados, dentre outras de dados pessoais.

Ocorre que, no dia 29 de abril de 2020, foi publicada a Medida Provisória nº 959/2020, a qual no artigo 4º prorrogou a entrada em vigor da LGPD para o dia 3 de maio de 2021, no tocante ao artigo 65, II a Lei nº 13.709/2018.

Ocorre que tais prorrogações geram preocupações, pois o aumento das interações eletrônicas, principalmente após a pandemia instalada pela COVID-19, tem gerado inúmeras formas de capturas indevidas de dados pessoais, uma delas se dá pelos brinquedos conectados, conforme será exposto adiante.



Salienta-se que no artigo 14 a Lei nº 13.709/2018 regulamentou o tratamento dos dados pessoais das crianças e adolescentes, prevendo a participação obrigatória dos pais, ou pelo menos um deles, ou responsável legal, por meio de consentimento específico e em destaque autorizando o manejo de tais dados.

Por fim, por meio do método dedutivo, analisa-se de forma documental, bibliográfica e jurisprudencial a Lei nº 13.709/2018 e alterações trazidas pela Lei nº 13.853/2019, como a maneira de propor maior resguardo aos direitos consumeristas e à transparência na manipulação de dados pessoais das crianças e adolescentes, bem como a proposição do desenvolvimento de um ambiente virtual mais seguro.

### 1. Conceito introdutórios de família

O conceito de família tem passado por importantes transformações em virtude da dinâmica social em constantes arranjos. Destaca que o direito contemporâneo pode ser dividido em dois grandes livros, são estes: 1) direito existencial: fundado na pessoa humana, normas de ordem pública; 2) direito patrimonial: fundado no patrimônio, normas de ordem privada:

[...]

*O Direito Existencial de Família* está baseado na pessoa humana, sendo as normas correlatas de ordem pública ou cogentes. Tais normas não podem ser contraídas por convenção entre as partes, sob pena de nulidade absoluta da convenção, por fraude à lei imperativa (art. 166, VI do CC). Por outra via, o *Direito Patrimonial de Família* tem o seu cerne principal no patrimônio, relacionado a normas de ordem privada ou dispositivas. Tais normas, por óbvio, admitem livremente previsão em contrário pelas partes (TARTUCE, 2018, p. 1314).

Segundo Carlos Roberto Gonçalves:

O vocábulo família abrange todas as pessoas ligadas por vínculo de sangue e que procedem, portanto, de um tronco ancestral comum, bem como as unidas pela afinidade e pela adoção. Compreende os cônjuges e companheiros, os parentes e os afins (GONÇALVES, 2018, p. 303).

Nesse sentido, importante destacar que os direitos de família são direitos de natureza personalíssima, portanto irrenunciáveis, intransmissíveis por herança, ressalta Silvio Rodrigues “ninguém pode transferir ou renunciar sua condição de filho” (RODRIGUES, 2004, p. 14). Assim, seu regramento se dá por normas de natureza cogente e sua proteção é de interesse público e dever de todos.



A Constituição Federal dispõe no artigo 227 que é dever também da família assegurar à criança e ao adolescente, dentre outros à dignidade, respeito, liberdade e à convivência comunitária, além de protegê-los de qualquer forma de discriminação, exploração ou violência.

Ademais, tem-se entendido família como entidade ligada pelo afeto, lastreados por conexões de amor, este foi o entendimento do Superior Tribunal de Justiça ao tratar da igualdade de condições aos parceiros do mesmo sexo que vivam em união estável:

A quebra de paradigmas do Direito de Família tem como traço forte a valorização do afeto e das relações surgidas da sua livre manifestação, colocando à margem do sistema a antiga postura meramente patrimonialista ou ainda aquela voltada apenas ao intuito de procriação da entidade familiar. [...] A defesa dos direitos em sua plenitude deve assentar em ideias de fraternidade e solidariedade, não podendo o Poder Judiciário esquivar-se de ver e de dizer o novo, assim como já o fez, em tempos idos, quando emprestou normatividade aos relacionamentos entre pessoas não casadas, fazendo surgir, por consequência, o instituto da união estável. A temática ora em julgamento igualmente assenta sua premissa em vínculos lastreados em comprometimento amoroso. Inserção das relações de afeto entre pessoas do mesmo sexo no Direito de Família, com o consequente reconhecimento dessas uniões como entidades familiares (BRASIL, STJ, REsp 1.026.981/RJ, 2010).

Tais deveres também estão tratados na Lei nº 8.069/1990, estatuto da criança e adolescentes (ECA), artigos 4º e 5º. Esclarece também tal estatuto que a proteção da dignidade se refere a impedir que tais seres não sofram, “qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor”, artigo 18 (BRASIL, 1990b).

Já no tocante ao 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 [...]”, artigo 17 (BRASIL, 1990b).

Quanto à liberdade compreende, dentre outros, opinião, expressão, participar, sem discriminação da vida comunitária e familiar, artigo 16 (BRASIL, 1990b).

Ademais, o princípio da paternidade (entende-se também da maternidade) responsável, previsto no artigo 226, parágrafo 7º da constituição Federal, exige a participação efetiva dos pais e responsáveis na formação, orientação e proteção de seus filhos, enquanto estes não possuírem a maioridade civil (aquisição de 18 anos completos), etapa esta em que a



lei presume a aquisição de maturidade pelo indivíduo para praticar e se responsabilizar por si próprio pelos seus atos praticados.

Assim, tem a família autorização constitucional e legal de resguardar os interesses as crianças e adolescentes no que pertence aos seus dados pessoais seu melhor interesse, estes, muitas vezes, expostos ao lado mais hostil das mídias sociais.

Portanto, cabe à família e a toda sociedade resguardar, orientar e proteger a dignidade dos mais vulneráveis, no caso do presente estudo, às crianças e adolescentes, nas relações cibernéticas no tocante à proteção de dados pessoais, os quais resguardam direitos da personalidade da criança e do adolescentes, tudo sem abuso ou prejuízo a convivência destes na vida comunitária.

## **2. Breve explanação sobre o sistema de proteção de dados da União Europeia: GDPR**

*General date protection regulation-GDPR* se trata do sistema regulatório de proteção de dados criado e regulamentado na União Europeia, o qual confirma uma tendência mundial de cuidado, zelo dos legisladores, autoridades e da sociedade no tocante a proteção de dados pessoais de seus cidadãos.

Tal regulamento europeu, o GDPR, foi publicado sob o n. 2016/679, em 4 de maio de 2016 e entrou em vigor no dia 25 de maio de 2016, tendo como o período de dois anos para adaptação dos países membros do bloco.

O GDPR tem aplicabilidade extraterritorial, pois se aplica a qualquer pessoa física ou jurídica que, em qualquer lugar do globo, armazenem, colem ou processem de qualquer forma, dados pessoais de cidadãos europeus. Portanto, tem aplicabilidade além dos limites territoriais da União Europeia.

Desta forma, é de interesse de brasileiros que operam dados pessoais de cidadãos europeus, ou seja, de nacionais que prestem serviços ou forneçam produtos para a Europa e serviu de inspiração para a lei brasileira de proteção de dados pessoais, Lei nº 13.709/2018.

O aumento das relações pessoais e comerciais pela internet, telefones e outros equipamentos eletrônicos, trouxe rapidez, aumento de oferta de produtos e serviços e a praticidade de se estabelecer relações, as transações comerciais, o denominado *E-Commerce*, ou seja, prática de negócios por meio de transferências de informações por meio da rede mundial de computadores.



Assim, quaisquer informações dos consumidores interessados em produtos e serviços por meio da internet devem fornecer seus dados pessoais e bancários. No que cabe ao fornecedor, este deve fornecer os dados referentes aos produtos e serviços oferecidos, as maneiras de efetivação do negócio e informações sobre a empresa fornecedora, prazos, garantia, sistema de entrega e demais fatos importantes que contribuam para a transparência do negócio jurídico a ser firmado.

Desta forma, esclarece-se que:

Apesar de o E-Commerce ser, ainda, um conceito de alguma forma recente, uma vez que, embora tenha dado os seus primeiros passos na década de 1990 só se tornou num conceito consistente no início do século XXI, tem sido notório o esforço de adaptação e confiança impostos no mesmo pelos seus utilizadores. Assim, a globalização deste novo conceito permitiu que as pequenas e médias empresas conseguissem beneficiar de uma estratégia comercial num contexto internacional, direcionada para a venda online. Desta forma, podemos dizer que o E-commerce está a transformar-se em algo “viral”, sendo interpretado como uma tecnologia de informação e comunicação que tem como foco a sua evolução mundial. (COUTO, 2016, p. 2).

Surge, então, a necessidade de regulação do tratamento e gerenciamento de proteção dos dados das pessoas que realizam quaisquer transações que envolvem o fornecimento de suas informações pessoais.

A normatização europeia, por envolver inúmeras Nações, necessita da cooperação mútua destes para a eficácia e eficiência do GDPR, bem como sua aplicação de forma uniforme em todos os Estados.

Já no Brasil a Lei nº 13.709/2018 dispõe que os operadores de tratamento dos dados *on line* ou *off line*, por meio cibernético, devem empregar medidas de programas de segurança (*privacy by design, by default*) e de ordem técnicas e administrativas idôneas visando a proteção da intimidade, das informações pessoais de acessos não autorizados, bem como “de situações acidentais, ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito” (BRASIL, 2018).

Ademais, a legislação nacional esclarece que os controladores e operadores de dados podem formular regras de boas práticas e de governança, *compliance*, ou seja, o agir conforme a lei, colaborar para o seu efetivo cumprimento. Portanto, condutas padronizadas e



normatizadas em âmbito interno que organizem procedimentos a serem adotados no tratamento dos dados pessoais (BRASIL, 2018, artigo 32).

### 3. O contexto legislativo trazido pela Lei nº13. 709/2018 (LGPD)

Em 2018 foi publicada no Brasil a Lei nº 13.709/18, a qual dispõe sobre a proteção de dados pessoais, inclusive por meios digitais, ou seja, não importa o modo pelo qual o dado foi coletado se de maneira pessoal ou eletrônica, e altera a Lei nº 12.965/2014, conhecida como

“Marco Civil”, a qual estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (JESUS; MILAGRE, 2014, p. 17).

Tal norma trouxe originalmente em seu texto a previsão de entrada em vigor no ano de 2020. Ocorre que em dezembro de 2019 foi publicada a Lei nº 13.853/2019, a qual alterou a LGPD e prorrogou a sua entrada em vigor em mais seis meses, totalizando vinte e quatro meses de sua publicação em 2018.

A exceção se dá nas regras referentes à criação da Autoridade Nacional de Proteção de Dados, que já estão em vigor, conforme artigo 65, I e II, da Lei nº 13.709/2018, alterada pela Lei nº 13.853/2019.

Ocorre que, no dia 29 de abril de 2020, foi publicada a Medida Provisória Nº 959/2020, a qual no artigo 4º prorrogou a entrada em vigor da LGPD para o dia 3 de maio de 2021, no tocante ao artigo 65, II a Lei Nº 13.709/2018.

Tais prorrogações causam preocupação, pois tal norma trará regulamentações mínimas para inúmeras condutas que tratam da coleta, armazenamento, compartilhamento, eliminação e anonimização de dados pessoais. Condutas estas de tratamento que tem aumentado muito diante do crescimento das interações eletrônicas ocasionadas pelo isolamento social que se instalou mundialmente no intuito de diminuir os riscos de contágio da COVID-19.

Nesse sentido, *“internet no es lo mismo que libertad, ya que em sus usos y aplicaciones no se respeta el derecho e la protección de datos personales, plasmación del derecho a la libertad como autodeterminación informativa”* (GALINDO; CARMO, 2017, p. 81).



Assim, esta normativa visa “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (CAVALCANTE, 2019, p. 64). Tal norma teve como inspiração a GDPR, o regulamento de proteção de dados da União Europeia, leis estas surgidas em decorrência das relações comerciais e pessoais de forma eletrônica, por meio das novas tecnologias.

Nesse contexto:

Por isso, também, é que se compreende a necessidade de regular o direito à privacidade sob uma perspectiva econômica, focada no já mencionado fluxo internacional de dados – um elemento fundamental para a economia globalizada dos séculos XX e XXI. Portanto, referidos direitos fundamentais, como o da privacidade, ganharam maior necessidade de proteção legal, como por meio da LGPD, assim como da *General Data Protection Regulation* (GDPR), norma da União Europeia que inspirou a legislação brasileira, diante da quantidade avassaladora de dados coletados na era digital e do elevado grau de organização e inteligência empregado sobre eles (progresso quantitativo e qualitativo), viabilizando análises valorativas, não apenas pelo Estado sobre os cidadãos, mas também por empresas privadas (VAINZOF, 2019, p. 22).

Porém, é de extrema importância que haja estudo e discussão sobre o tema do tratamento de dados pessoais nos meios eletrônicos, assunto trazido por tal norma que sofreu inspiração do GDPR, o regulamento geral da proteção de dados, trouxe a uniformização de condutas, no contexto comunitário, acerca do tema na União Europeia.

Ademais,

[...]

A ética dos dados se tornou um dos valores mais importantes da época contemporânea, como um ponto da geopolítica global, de forma que a inteligência artificial se liga diretamente com a vida cotidiana dos indivíduos. Ou seja, atualmente, ao falar em privacidade e dados pessoais, não se está mais diante de um tema referente a individualidades, mas, sim a um tema estratégico do ponto de vista da tecnologia e do sistema econômico mundial. O poder dos métodos estatísticos, a massa de dados, o barateamento de tratamento, bem como o ambiente em que esses dados são formados, são fatores que apenas fortalecem um laço indissociável entre dados e inteligência artificial (QUINELATO, 2019, p. 250).

Portanto, condutas como coleta, armazenamento, compartilhamento ou eliminação de dados exigirá de todos comportamentos éticos, transparentes também em ambientes virtuais, cibernéticos, pois se trata de dados que refletem os direitos da personalidade do indivíduo, sua vida privada, íntima.





#### 4. Do tratamento dos dados pessoais

A Lei nº 13.709/2018, conforme já salientado, tem por objetivo proteger os dados pessoais, entendido tais como aquele relacionado “a pessoa natural identificada ou identificável”, artigo 5º I (BRASIL, 2018).

Nessa seara, nota-se que o conceito adotado pelo Brasil no que concerne aos dados foi o expansionista, ou seja,

Pelo qual não somente a informação relativa a pessoa diretamente identificada estará protegida pela Lei, mas também aquela informação que possa – tem o potencial de- tornar a pessoa identificável. Assim, 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, às convicções políticas, religiosas e filosóficas; números de telefone, registros e ligações, protocolos de 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 atual vida em sociedade. (VAINZOF, 2019, p. 89).

Ademais, artigo 5º da Lei nº 13.709/2018 dispõe sobre conceitos das condutas tratadas na norma. O inciso X trata do conceito de tratamento de dados pessoais, sendo este:

toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Nesse contexto, tem-se o tratamento dos dados pessoais a partir do momento em que são coletados por pessoa física ou jurídica diferente do seu titular, por meio de captura, recepção, dentre outros; compreendendo o armazenamento ou descarte das informações, bem como o compartilhamento e da difusão.

A proteção de dados, agora regulamentada legalmente, fará surgir uma nova cultura empresarial acerca do tratamento de dados coletados de seus clientes,

[...]

Com o surgimento de um *enforcement* maior no âmbito da proteção de dados pessoais, observa-se que o grande desafio que engloba todo o mundo é a criação de uma nova “nova” cultura empresarial, preocupada com a ética no tratamento de dados pessoais, de forma a respeitar a vida privada dos indivíduos, suas particularidades, bem como garantir a estes que estejam



prevenidos de decisões automatizadas que influenciem em suas vidas sem que tenham conhecimento (QUINELATO, 2019, p. 249).

Portanto, a proteção legal dos dados envolve o resguardo da personalidade do ser humano, por isso o seu manejo deve garantir o sigilo, ser adequado e responsável pelas informações da pessoa humana.

Ademais, o artigo 7º da lei de proteção de dados dispõe que o tratamento pode ser realizado da seguinte forma,

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; 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; 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 (BRASIL, 2018).

Tais bases legais taxativas são as que legitimam o tratamento de dados pessoais, e os incisos II a X preveem ocasiões em que o consentimento é desnecessário.

Assim, importante tratar do real alcance da conduta prevista no inciso I, qual seja, a autorização do tratamento dos dados pessoais quando houver o fornecimento de consentimento pelo titular.

A partir da interpretação sistemática da lei, o artigo 5º XII informa que consentimento é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Desta forma, manifestação sem vícios, prolatada depois do esclarecimento do real motivo para que os dados sejam necessários, o que demonstra a transparência da relação



firmada e a indubitosa vontade de fornecer tais dados, pois a disposição de tais dados pelo seu titular demonstra a plena confiança que este detém perante à aquele que vai receber tais dados.

Fornecer dados pessoais é compartilhar informações privadas que envolvem o exercício de direitos da personalidade, como por exemplo: o nome, estado civil, ou a livre manifestação de pensamento como: religião, crença, identidade de sexo etc.

Por isso, o acesso e manuseio de tais dados deve ser responsável, sigilosa e ter uma finalidade específica perfeitamente esclarecida para o titular. Nesse sentido destaca-se:

[...]

Importante observar o que diz respeito à granularidade, por meio da qual não se pode ter como válido o consentimento manifestado no formato de “tudo ou nada”. Nesse sentido, nas situações em que houver coleta de dados para diferentes finalidades, o titular dos dados deve ter a possibilidade de escolher, de uma a uma, a finalidade específica em relação a qual autoriza o tratamento de dados, sendo inválido se não houver essa opção. (LIMA, 2019, p. 181).

Desta forma, o consentimento deve ser granulado, ou seja, fracionado para cada finalidade específica, tal entendimento encontra-se respaldado pelo princípio da transparência, este contemplado no artigo 9º da Lei nº 13.709/2018, o qual prevê resumidamente que o titular deve ter acesso facilitado das informações relativas ao tratamento dos seus dados no que concerne às finalidades específicas, forma e duração, identificação do controlador, informações sobre o uso compartilhado de dados pelo controlador e para qual finalidade, responsabilidades dos agentes que farão o tratamento, bem como a confirmação retificação, anonimização e até mesmo a eliminação de tais dados.

Ademais, diante das normas constitucionais dispostas no art. 5º, incisos X e XII (direito à intimidade e sigilo de dados, entre outros), da Constituição Federal de 1988, estes considerados direitos fundamentais e possuem observância obrigatória, tais cadastros de dados pessoais devem ser seguros, com dispositivos eficazes de resguardo, sigilo, a privacidade e intimidade de seu titular.

Nesse sentido o Supremo Tribunal Federal já salientou que a comunicação de dados, ainda que mantidas em computador, estão protegidas pelo sigilo:

[...]

Com efeito, também com relação aos dados em geral – e, conseqüentemente, os constantes de computador que pode armazenar as mais sigilosas informações de seu proprietário -, estão eles cobertos pela garantia do



disposto no inciso XII do artigo 5º da Constituição [...] dos dados contidos naquele microcomputador, para mandar decodificá-los ao seu alvedrio, como fez, acobertados que se achavam pelo sigilo, o qual, conquanto se possa ter por corolário da inviolabilidade do próprio recinto dos escritórios da empresa acha-se especificamente contemplado no inc. XII, do mesmo artigo, ao lado da correspondência e das comunicações telegráficas e telefônicas. Aliás, nos tempos modernos, em que todos os trabalhos datilográficos das empresas é realizado por meio de digitação, a invasão da memória dos computadores implica fatalmente a quebra do sigilo não apenas de dados em geral, desde os relativos a simples agenda até os relacionados a fórmulas e cálculos, mas também de toda correspondência epistolar e telegráfica, em relação aos quais o manto constitucional é de natureza absoluta, já que não deixou espaço reservado ao trabalho normativo do legislador ordinário, como se fez com as comunicações telefônicas. (BRASIL, 2006, p. 15)

Portanto, a nova LGPD encontra respaldo na Constituição Federal e jurisprudência, pois visa assegurar à privacidade, intimidade e sigilo das comunicações que envolvam dados obtidos de maneira *on line* ou *off line*.

## **5. Do tratamento de dados pessoais de crianças e de adolescentes**

Conforme o estabelecido na Lei nº 8.069/1990b (Estatuto da Criança e do Adolescente – ECA), entende-se por criança toda pessoa com até 12 (doze) anos incompletos e pessoa adolescente é aquela que possui entre 12 (doze) e 18 (dezoito) anos incompletos.

O tratamento de dados de criança e adolescentes, previsto a partir do artigo 14 da Lei nº 13.709/2018, deve obedecer ao princípio da proteção integral, prevista no artigo 1º do ECA, pois estes são sujeitos de direitos inerente a condição que possuem, qual seja, de seres em desenvolvimento, seres em construção, os quais necessitam de proteção, apoio e orientação.

Crianças e adolescentes são pessoas que necessitam de terceiros (família, estado e sociedade) para que possam exercer ou ter acesso a certos direitos, pois detém a capacidade de direito, mas não a capacidade de fato, ou seja, de exercerem por si só os atos da vida civil.

Ademais, o Decreto nº 99.710/90, o qual promulgou a convenção internacional sobre os direitos da criança

Os Estados Partes envidarão os seus melhores esforços a fim de assegurar o reconhecimento do princípio de que ambos os pais têm obrigações comuns com relação à educação e ao desenvolvimento da criança. Caberá aos pais ou, quando for o caso, aos representantes legais, a responsabilidade primordial pela educação e pelo desenvolvimento da criança. Sua



preocupação fundamental visará ao interesse maior da criança (BRASIL, 1990a).

Portanto, observa-se que existem várias normas que garantem nacional e internacionalmente os direitos de crianças e adolescentes visando sua proteção integral e prioritária.

Com o surgimento de novas tecnologias de interação comunicativa e aumento do acesso a dispositivos conectados, cresceu também o acesso de crianças e adolescentes às plataformas sociais e aos jogos eletrônicos.

Nesse sentido, já se constatou que excesso de exposição às mídias sociais gera consequências que vão além da mitigação da privacidade. Pois, tem-se diagnosticado o adoecimento de jovens, tendo em vista o aumento de casos de depressão e ansiedade em pessoas na faixa de 14 a 24 anos que passam muito tempo interagindo nas redes sociais.

Motivo pelo qual, a partir de 1º de janeiro de 2022, a Organização Mundial de Saúde passará a constar de sua classificação estatística internacional de doenças e problemas relacionados à saúde a CID 11, a qual qualifica o uso abusivo de jogos eletrônicos (*gaming disorder*), na seção correspondente as formas de transtornos viciantes considerando uma espécie de distúrbio mental, que gera comprometimento do indivíduo nas áreas pessoal, familiar, educacional, laboral etc. (THEES, 2018, p. 1).

Diante da constatação da Organização Mundial da Saúde de que o uso abusivo de jogos eletrônicos provoca distúrbios no sono, impulsividade, ansiedade, depressão, aumento da agressividade e violência nos jogadores compulsivos, principalmente em crianças e jovens.

Diante dos perigos eletrônicos que rondam as redes, fazendo vítimas pessoas mais vulneráveis dentro de suas próprias casas, o legislador brasileiro previu regras mais rígidas quando se trata do tratamento de dados pessoais de crianças e adolescentes.

Salienta-se, que o artigo 14, parágrafo 2º informa que apenas o tratamento dos dados pessoais de crianças deverá ser realizado com consentimento específico e em destaque os pais, ou pelo menos um deles ou do responsável legal.

Entende-se por consentimento específico, aquele em que a pessoa é perfeitamente esclarecida acerca de toda etapa do tratamento dos dados, antes mesmo de sua coleta. Já no



que cabe ao consentimento em destaque é aquele em que o seu conteúdo foi destacado do resto do texto, ou seja, para que fique em evidência.

Nesse sentido,

Importante observar que o consentimento será entendido como “específico” quando, antes da coleta dos dados, no contrato, na política de privacidade ou em outro documento relacionado, houver detalhamento sobre o ciclo de vida do tratamento dos dados pessoais, com referência objetiva e clara sobre todos os limites e as finalidades em relação aos quais os dados serão tratados, inclusive sendo granular, cabendo ao usuário a seleção sobre o tratamento que deseja efetivamente autorizar. Já o consentimento “em destaque” será alcançado quando for clara a identificação do usuário em relação ao tratamento que será realizado com seus dados pessoais. Isso é especialmente relevante quando o consentimento estiver contemplado dentro de documento que comtemple outras autorizações, situações em que o trecho relacionado ao tratamento de dados pessoais deve ser realçado, em relação às demais partes do texto, do vídeo ou do áudio (LIMA, 2019, p. 209).

Todavia, a legislação também prevê exceção à regra do consentimento específico e em destaque para o tratamento de dados pessoais de crianças dado por pelo menos um dos pais ou responsável legal, este pode ser realizado apenas uma vez, sem a ocorrência do armazenamento de tais dados, tendo por finalidade específica contatar os pais ou responsável ou para resguardar, proteger a criança. Mas neste caso é vedado o compartilhamento com terceiros (artigo 14, parágrafo 3º da Lei nº 13.709/2018).

Dessa forma, entende-se que dados referentes as crianças e adolescentes não podem ser utilizados por meio de *big data*, ou seja, utilizados por espécies de linguagem de programação complexas com uso de algoritmos, estes desenvolvidos no intuito de processamento de dados em massa, com aplicação de algoritmos, fórmulas matemáticas de análise de dados.

Já que estes induzem ao cometimento de condutas que possam gerar prejuízos a criança ou ao adolescentes, pois são expostos a uma intensa carga de propaganda de produtos e serviços baseados em perfis criados com a extração de importantes informações dos usuários como: hábitos, desejo de consumo; o que gera a possibilidade de envio de propagandas direcionadas, específicas daquele cliente em potencial. Fatos este que cria vantagem competitiva à empresa que pratica tal conduta, bem como o aumento do seu lucro.

Nota-se, que muitas vezes o *big data* gera um bombardeio abusivo de publicidades e propagandas indesejadas para o titular dos dados fornecidos.



Os controladores no tratamento de dados de criança e adolescentes devem manter pública a informação quanto aos dados coletados, como este será utilizado e quais os procedimentos para o exercício dos seguintes direitos (artigo 14, parágrafo segundo e artigo 18 da LGPD): os relativos à confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; 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 artigo 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; revogação do consentimento. Estes podem ser solicitados a qualquer momento mediante requerimento (artigo 18 da Lei nº 13.709/2018).

Destaca-se que em virtude dos princípios que norteiam a proteção integral de crianças e adolescentes, entende-se que a previsão de manutenção pública da informação sobre o tratamento e dos tipos de dados coletados deve ser aplicado também aos adolescentes, embora a lei se refira, neste aspecto, somente ao parágrafo que trata dos dados da criança.

O legislador também se preocupou com os dados de crianças coletados para que estas tenham acesso a jogos, aplicativos de internet e outras atividades. Tal disposição se encontra no artigo 14, parágrafo 4º, e prevê que os controladores, nesses casos só podem requerer as informações estritamente necessárias à atividade solicitada.

Ocorre que a menção do citado parágrafo 4º de se exigir apenas as informações pessoais estritamente necessárias à atividade é um tanto subjetiva, de ampla interpretação. No caso, entende-se que as vão variar de conformidade com os jogos, aplicativos ou atividades solicitadas, como, por exemplo, a faixa etária do solicitante e contato das pessoas responsáveis pelo menor.

Importante lembrar, que se entende, também, ser necessário que o previsto no artigo supra (artigo 14, parágrafo 4º) seja aplicável ao tratamento dos dados dos adolescentes, em nome dos princípios da proteção integral, intimidade e adequação.



Ademais, deve o controlador de dados pessoais verificar se o prévio consentimento realizado na conformidade da lei foi efetivamente dado pelo pai, mãe ou por representante legal do titular, para isto deve aprimorar os mecanismos de coleta, utilizando o sistema eletrônico ou pessoal de sua realização.

Por fim, o artigo 14, parágrafo 6º, dispõe que as informações sobre o tratamento de dados de crianças e adolescentes devem ser fornecidas de forma simples, clara e acessível, bem como devem ser 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, ou seja, devem respeitar as regras e soluções de acessibilidade tratadas na Lei nº 13.146/2015 (Estatuto da Pessoa com Deficiência).

Diante do exposto, devem os pais e responsáveis legais, quando da necessidade de informação dos dados pessoais e de seus filhos ou pessoa sob sua responsabilidade, menores de 18 anos, agirem de forma a preservar a dignidade destes e com responsabilidade, conforme preceitua o artigo 226, parágrafo 7º da Constituição Federal, pois a exposição destes em situações de risco, vexatórias ou que causem quaisquer espécie de danos à criança e ao adolescente, implicará em responsabilização, não só do controlador dos dados, mas também dos pais ou responsáveis que não agiram com a devida cautela quando de seu fornecimento.

Assim, quanto às infrações cometidas nas condutas reguladas na Lei nº 13.709/2018, os responsáveis estarão sujeitos às seguintes sanções administrativas (artigo 52): advertência; multa simples de até 2% do faturamento da empresa grupo ou conglomerado no Brasil; multa diária; publicização da infração e bloqueio dos dados pessoais, não substituindo às sanções previstas no Estatuto da Criança e Adolescente, Lei nº 8.069/90, conforme artigo 52, parágrafo 2º da Lei nº 13.709/2018.

## **6. Brinquedos conectados**

Muitos dispositivos eletrônicos têm trazido verdadeiras armadilhas de captura de dados, pois realizam tal conduta de maneira sutil, discreta, sem nenhuma espécie de aviso ou consentimento de quem os adquire.





Nesse sentido, autoridades francesas de regulação e proteção de dados detectaram que os dados de crianças e adolescentes passaram a ser capturados por meio de brinquedos conectados (CNIL, 2019, p. 1).

São considerados brinquedos conectados objetos de aparências inofensivas como bonecas, babás eletrônicas, relógios, vídeo game, dentre outros, que capturam informações e as enviam por ondas de rádio (*bluetooth*, *wi-fi*) e pela *internet*.

Tal captura de dados pessoais é uma das mais abusivas e nefasta, pois viola o ambiente privado de seres vulneráveis em momentos íntimos com sua família, como é o caso dos aparelhos denominados babás eletrônicas, as quais são vendidas como equipamento que buscam informar e tranquilizar seus pais ou responsáveis, por meio de sons e imagens, do ambiente em que se encontra a criança, tornando assim mais seguro e monitorado o local onde o infante está.

Deste modo, alguns equipamentos se utilizam dos dados coletados e os transmitem para um servidor sem autorização dos proprietários dos aparelhos, sujeitando seus usuários a riscos de fraude, exposição indevida etc.

A autoridade de proteção de dados francesa (*Commission Nationale de l'Informatique et des libertés*-CNIL) informa por quais meios os consumidores podem se proteger da captura de dados pessoais por meio desses objetos, dentre eles estão: a verificação do brinquedo acerca da existência de permissões de conexões de terceiros por meio de *smartphone* ou *internet*, para isso se requer botão de acesso ou uso de senha. Outro informe de segurança é verificar se o objeto acende quando se ouve ou transmite informações pela rede mundial de computadores, bem como execute atualizações de segurança regularmente (CNIL, 2019, p. 1).

Salienta-se que o regulamento de proteção de dados da União Europeia possui regramento específico de obrigação dos fabricantes em proteger as informações coletadas em seu artigo 121 e evitar que sejam distorcidos, corrompidos ou acessado por terceiros.

Ademais, tal normativa prima pela lealdade, transparência e licitude que deve reger as relações, em especial, no presente caso, as que realizam o tratamento de dados em ambientes tão vulneráveis como o interior das residências de seus consumidores de maneira



furtiva, silenciosa e, na maior parte das vezes sem o conhecimento e consentimento de seus titulares ou responsáveis.

Diante dos fatos supra, constata-se a importância de se tomar conhecimento da dimensão que tem atingido o monitoramento virtual, os objetos e equipamentos por meio do qual os dados são obtidos, as formas empregadas, tempo e período de captura, seus detentores e realizadores, motivos, local de armazenamento, a ocorrência ou não de compartilhamento, eliminação, dentre outros.

Esse comportamento intrusivo do mercado virtual ocorre, principalmente, porque os usuários da rede e autoridades não se atentaram para a dimensão da usurpação que os operadores cibernéticos realizam, já que são métodos sutis, discretos, de operabilidade remota, criados por meio de linguagem de programação e uso de algoritmos complexos.

As técnicas de linguagem de programação de monitoramento de perfis e captura de informações de usuários não podem invadir o território da intimidade, diante da lesão da dignidade de seus titulares. Por isso, a importância da transparência dos mecanismos dos produtos eletrônicos, bem como a informação se este realiza ou não compartilhamento virtual de dados.

Apenas com o conhecimento de tais práticas, discussões sobre tais questões, conhecimento e fiscalização da legislação regulamentadora, será possível criar limites, propor soluções, impor responsabilidades e proporcionar um ambiente mais leal, transparente e seguro para os usuários de quaisquer equipamentos que se conecte a dispositivos virtuais.

O fornecimento de produtos seguros aos consumidores é direito previsto na Lei nº 8.078/90 (Código de Proteção e Defesa do Consumidor - CDC). Portanto, a adoção de práticas tecnológicas que firam a segurança da proteção de dados e intimidade de consumidores e usuários, infringem não só a legislação de proteção de dados, mas também a consumerista, o que sujeita o infrator as penalidades administrativas previstas no artigo 56 do CDC, dentre elas apreensão de produtos e proibição de sua fabricação.

## **CONCLUSÃO**

O aumento das operações realizadas no âmbito cibernético, gerou a necessidade de regulação mínima do tratamento que se dá aos dados pessoais fornecidos nas plataformas digitais. Na intenção de tornar mais seguro o tráfego dos dados em âmbito digital.



Nesse sentido, surge na União Europeia e em outros países, como o Brasil normatizações que preveem regras normativas para o gerenciamento, armazenamento, proteção e compartilhamento de tais dados.

É sabido que um farto banco de dados de clientes gera valor agregado ao patrimônio de uma empresa. Portanto, deve esta agir de maneira ética, sigilosa e com boas práticas (*compliance*) no manuseio (tratamento) de tais dados, por isso o estabelecimento de sanções rígidas no caso de desrespeito às normas previstas na Lei nº 13.709/2018 (artigo 52), tudo após a instauração do devido procedimento administrativo que assegure o amplo direito de defesa e o contraditório (artigo 52, parágrafo 1º).

Tratar com respeito e zelo de informações importante para qualquer ser humano, pois dados pessoais resguardam direitos da personalidade do indivíduo, e em especial daqueles mais vulneráveis, como as crianças e adolescentes é o que se espera de uma sociedade justa e solidária.

Desta forma, como cabe também a família zelar pela orientação, proteção e convivência comunitária saudável de suas crianças e adolescentes, nada mais correto do que prever a participação efetiva dos pais ou responsáveis legais quando do fornecimento do consentimento para a realização do tratamento de dados pessoais de tais menores, bem como a previsão legal de conduta mais rígida e cautelosa dos controladores de tais dados, desde da sua coleta até a sua eliminação.

Ademais, comportamento intrusivo do mercado virtual, com utilização dos recursos proporcionados pela inteligência artificial, vem sendo constatado das formas mais sutis e abusivas, um exemplo são os brinquedos conectados, objetos de aparência inofensiva como bonecas, babás eletrônicas, relógios, vídeo game, dentre outros, que capturam informações e as enviam por ondas de rádio (*bluetooth, wi-fi*) e pela *internet*.

Práticas estas nocivas e covardes, pois invadem a privacidade dos indivíduos e sem o consentimento destes, capturam seus dados de maneira furtiva, sem menção do real motivo ou da extensão de sua prática.

Assim, com base no que foi tratado neste trabalho, busca-se motivar novas pesquisas e estimular o acompanhamento da LGPD quando da sua entrada em vigor, observar seu



amadurecimento doutrinário e jurisprudencial, principalmente, no tocante aos dados daqueles mais vulneráveis, no caso as crianças e adolescentes.

O mundo cada vez se torna mais automatizado, mais influenciado pela inteligência artificial. Por isso a importância de leis como a LGPD que busca a regulamentação mínima de determinadas questões que envolvem práticas no meio eletrônico, como forma de tornar um pouco mais humano aquilo que ainda torna necessária a existência humana no globo.

## REFERÊNCIAS

- BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de outubro de 1988**. Brasília, DF: Presidência da República, [2019]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm). Acesso em: 10 fev. 2020.
- BRASIL. **Decreto nº 99.710 de 22 de novembro de 1990a**. Decreto- promulga a convenção da criança e adolescentes. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/decreto/19901994/d99710.htm](http://www.planalto.gov.br/ccivil_03/decreto/19901994/d99710.htm). Acesso em: 12 ago. 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](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em: 15 nov. 2018.
- BRASIL. **Lei nº 13.853/2019 de 08 de julho de 2019**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2019/Lei/L13853.htm](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm). Acesso em: 20 dez. 2019.
- BRASIL. **Lei nº 8.069 de 13 de julho de 1990b**. Estatuto da criança e do adolescente. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L8069compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/L8069compilado.htm). Acesso em: 13 ago. 2019.
- BRASIL. **Medida Provisória nº 959 de 29 de abril de 2020**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/Mpv/mpv959.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm). Acesso em: 30 abr. 2020.
- BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.026.981/RJ**, partes: Severino Galdino Belo e Caixa de Previdência dos Funcionários do Branco do Brasil. Relator: Nancy Andrichi, Data de Julgamento: 04/02/2010, Terceira Turma, Data Publicação: DJ 23/02/2010.
- BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 418.416-8 SC**, partes: Luciano Hang, Antônio Nabor Areias Bulhões e outros, Ministério Público Federal. Relator: Min. Sepúlveda Pertence, Data de Julgamento: 10/05/2006, Tribunal Pleno, Data de Publicação: DJ 10-12-2006.
- CAVALCANTE, Márcio André Lopes. **Principais novidades legislativas de 2018: selecionadas e comentadas**. Salvador: JusPodivm, 2019.
- CNIL. *Commission Nationale de l' Informatique et des libertés*. **Brinquedos conectados: que conselhos para protege-los?**. 2019. Disponível em: <https://www.cnil.fr/fr/jouetsconnectes-queles-conseils-pour-les-securiser>. Acesso em: 18 jan. 2020.



COUTO, Maria Laís dos santos Alegria. **O E-Commerce à luz do direito** – Análise do Regulamento Geral da Proteção de Dados – A Uniformização da União Europeia. 2016. 2 f. Dissertação (Mestrado em Direito Geral) - Universidade Católica Portuguesa: Faculdade de Direito do Porto, Porto, 2016.

GALINDO, Fernando; CARMO, Valter Moura do. ¿Libertad e Internet? **DIXI**, v. 19, n. 26, p.73-83, mayo 2017. DOI: <http://dx.doi.org/10.16925/di.v19i26.1952>. Disponible en: <https://revistas.ucc.edu.co/index.php/di/article/view/1952/2065>. Acceso en: 29 abr. 2020.

GONÇALVES, Carlos Roberto. **Direito Civil 3**. 5 ed. São Paulo: Saraiva, 2018.

JESUS, Damásio de; MILAGRE, José Antônio. **Marco civil da internet comentários à Lei n. 12.965/14**. São Paulo: Saraiva, 2014.

LIMA, Caio César Carvalho. Do tratamento de dados pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD – Lei geral de proteção de dados comentada**. São Paulo: Thomson Reuters Brasil, 2019. p. 179-219.

QUINELATO, Pietra Daneluzzi. A proteção de dados pessoais no âmbito das startups. *In*: OIOLI, Erik Frederico (coord.). **Manual de direito para startups**. São Paulo: Thomson Reuters Brasil, 2019. p. 243-250.

RODRIGUES, Silvio. **Direito Civil**: volume 6. 28. ed. São Paulo: Saraiva, 2004.

TARTUCE, Flávio. **Manual de Direito Civil**: volume único. 8. Ed. Rio de Janeiro: Método, 2018.

THEES, Vanessa. OMS inclui vício em games na sua lista de distúrbios mentais. **Portal PEBMED**, 03 jan. 2018. Disponível em: <https://pebmed.com.br/oms-inclui-vicio-em-games-na-sua-lista-de-disturbios-mentais/>. Acesso em: 27 abr. 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho 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 (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eurlex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Acesso em: 30 abr. 2020.

VAINZOF, Rony. Lei 13.709/2014 de 14 de agosto de 2018 – disposições preliminares. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD – Lei geral de proteção de dados comentada**. São Paulo: Thomson Reuters Brasil, 2019. p. 19-178.