



**ANTONIO MENEGHETTI FACULDADE
BACHARELADO EM DIREITO**

PEDRO HENRIQUE HERMES

**UM ESTUDO SOBRE A PROTEÇÃO DE DADOS PESSOAIS NO APLICATIVO
NETFLIX A PARTIR DOS SEUS TERMOS DE USO E DECLARAÇÃO DE
PRIVACIDADE**

Restinga Sêca, RS

2020

PEDRO HENRIQUE HERMES

**UM ESTUDO SOBRE A PROTEÇÃO DE DADOS PESSOAIS NO APLICATIVO
NETFLIX A PARTIR DOS SEUS TERMOS DE USO E DECLARAÇÃO DE
PRIVACIDADE**

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Direito, da Faculdade Antonio Meneghetti – AMF, como requisito parcial para a obtenção do título de Bacharel em Direito, sob a orientação da Prof. Dr.^a Rosane Leal da Silva.

Restinga Sêca, RS

2020

PEDRO HENRIQUE HERMES

**UM ESTUDO SOBRE A PROTEÇÃO DE DADOS PESSOAIS NO APLICATIVO
NETFLIX A PARTIR DOS SEUS TERMOS DE USO E DECLARAÇÃO DE
PRIVACIDADE**

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Direito, da Faculdade Antonio Meneghetti – AMF, como requisito parcial para a obtenção do título de Bacharel em Direito, sob a orientação da Prof. Dr.^a Rosane Leal da Silva.

COMISSÃO EXAMINADORA



Prof. Dr.^a Rosane Leal da Silva
Orientadora
Faculdade Antonio Meneghetti



Prof. Dr.^a Liége Alendes de Souza
Faculdade Antonio Meneghetti



Prof. Me. Andrey Oliveira Lamberty
Faculdade Antonio Meneghetti

Restinga Sêca, RS

2020

UM ESTUDO SOBRE A PROTEÇÃO DE DADOS PESSOAIS NO APLICATIVO *NETFLIX* A PARTIR DOS SEUS TERMOS DE USO E DECLARAÇÃO DE PRIVACIDADE¹

Pedro Henrique Hermes²

Rosane Leal da Silva³

SUMÁRIO: Introdução. 1 A evolução legislativa brasileira e a proteção de dados pessoais no ambiente digital. 2 A ascensão do *streaming*: *Netflix* e o sistema de recomendação de conteúdo baseado na técnica do *profiling*. 3. *Netflix* e proteção de dados pessoais: é possível se falar em usuário suficientemente protegido frente aos Termos de Uso e Declaração de Privacidade? Considerações Finais. Referências.

RESUMO: O presente trabalho investiga a proteção de dados no aplicativo *Netflix*, notadamente acerca da proteção de seu usuário a partir dos termos e condições de uso e declaração de privacidade. Nesse sentido, busca responder se é possível afirmar que o aplicativo de *streaming Netflix*, considerado provedor de aplicação e controlador de dados, adequou suas políticas de proteção de dados e respectivos termos de uso com a legislação brasileira, objetivando o regular tratamento dos dados pessoais de seus usuários. Para responder a tal questionamento, utilizou-se o método de abordagem dedutivo, partindo-se da premissa geral de proteção de dados para a análise do caso concreto, o que foi feito com o método de procedimento do estudo de caso. Concluiu-se que a base de princípios que dá sustentáculo hermenêutico às regras previstas na Lei Geral de Proteção de Dados Pessoais permite afirmar a existência de deficiência nas informações prestadas por *Netflix* em sua declaração de privacidade e termos de uso, especialmente se tomado o usuário como a parte vulnerável da relação jurídica estabelecida.

PALAVRAS-CHAVE: Netflix; Políticas de Privacidade; Proteção de dados pessoais; Streaming; Termos de Uso.

ABSTRACT: The present work investigates data protection in the Netflix application, notably about the protection of its user based on the terms and conditions of use and privacy statement. In this sense, it seeks to answer whether it is possible to affirm that the Netflix streaming application, considered an application provider and data controller, adapted its data protection policies and respective terms of use with Brazilian legislation, aiming at the regular treatment of personal data of your users. In order to answer this question, the deductive approach method was used, starting from the general premise of data protection for the analysis of the specific case, which was done with the case study procedure method. It was concluded that the base of principles that hermeneutic support to the rules foreseen in the General Law of Protection of Personal Data allows to affirm the existence of deficiency in the

¹ Artigo apresentado como requisito parcial para aprovação na disciplina Trabalho Final de Graduação II do Curso de Direito da Antonio Meneghetti Faculdade – AMF.

² Acadêmico do 10º semestre do curso de Direito da Antonio Meneghetti Faculdade (AMF). E-mail: pedrohermes.1@hotmail.com.

³ Doutora em Direito pela Universidade Federal de Santa Catarina (UFSC). Professora Associada do Curso de Direito da Universidade Federal de Santa Maria (UFSM) e da Antonio Meneghetti Faculdade (AMF). E-mail: rolealdasilva@gmail.com.

information provided by Netflix in its privacy statement and terms of use, especially if taken the user as the vulnerable part of the established legal relationship.

KEY-WORDS: Netflix; Privacy Policies; Protection of personal data; Streaming; Terms of use.

INTRODUÇÃO

A proteção de dados pessoais é tema constantemente debatido desde a promulgação da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, que regulamentou as questões atinentes aos dados pessoais dos usuários da rede. Todavia, tal temática já vinha sendo abordada no Brasil, mesmo que brevemente, desde o Marco Civil da Internet, Lei nº. 12.965/14, conferindo certa proteção aos usuários da internet em plena sociedade em rede.

Tais legislações têm surgido como uma necessidade de regular a exponencial utilização dos meios informáticos na sociedade e aumento na criação de plataformas digitais que se utilizam da coleta de informações de seus usuários para prestação do serviço que se propõem, sendo que a regulamentação de tal coleta, tratamento e demais formas de manipulação de dados objetiva a adequada proteção dos usuários em sua privacidade, intimidade, autodeterminação informativa, entre outros direitos que se busca proteger diante do contexto criado pela sociedade em rede.

Nesse sentido, observa-se que é crescente a utilização dos aplicativos de *streaming* pelos usuários da rede para consumo de mídias diversas, a exemplo de séries e filmes, notadamente pela utilização do aplicativo *Netflix*. Aplicativos de *streaming* são provedores de aplicação que, ao invés de descarregarem as informações, vídeos, etc, no dispositivo do usuário, prestam o serviço sem a necessidade de realizar a transferência do arquivo, possibilitando a utilização em tempo real, mediante fluxo contínuo de dados. O acesso a tais aplicativos se dá mediante prévio cadastramento - com o fornecimento das informações pessoais - do usuário na plataforma, cuja utilização das funcionalidades, na maior parte das vezes, ocorre por meio do pagamento de dinheiro a partir de planos previamente estipulados pelo provedor, possibilitando determinado número de acessos ou acesso ilimitado ao usuário.

É inevitável afirmar que tais aplicações possuem fáceis meios de acesso às informações pessoais do usuário, notadamente nome, endereço, conta bancária para pagamento contemplando, inclusive, informações a partir das quais é possível identificar gostos musicais, religião, localização do usuário e dados de terceiros. Tais procedimentos, se

não bem regulamentados nos termos de uso e políticas de privacidade, podem facilmente gerar violações aos direitos do usuário e suas informações pessoais por diversas maneiras.

Diante disso, impõe-se o seguinte questionamento: é possível afirmar que o aplicativo de *streaming Netflix*, considerado provedor de aplicação e controlador de dados, adequou suas políticas de proteção de dados e respectivos termos de uso com a legislação brasileira, objetivando o regular tratamento dos dados pessoais de seus usuários?

Para responder a esse questionamento, utilizou-se o método dedutivo, tendo em vista que se partirá de uma visão geral a respeito dos dados pessoais e sua legislação no Brasil para uma visão mais específica até os termos de uso e políticas de privacidade do aplicativo *Netflix*. Por sua vez, o método de procedimento escolhido foi o estudo de caso, posto que será abordada a temática com foco em termos de uso e políticas de privacidade específico do provedor *Netflix*, verificando-se a sua adequação com a legislação brasileira, o que configura estudo de caso.

Além disso, a temática de pesquisa do presente trabalho se filia à linha de pesquisa Política, Direito, Ontologia e Sociedade do Curso de Direito da Antonio Meneghetti Faculdade e se ampara nas pesquisas realizadas no Grupo de Pesquisa Direito e Internet, integrado pelo acadêmico. A adequação se mostra evidente, tendo em vista que o objetivo da pesquisa diz respeito a utilização de novas plataformas oriundas da sociedade em rede e da necessária proteção de dados pessoais que este uso enseja.

Inicialmente, será realizada uma análise sobre a proteção de dados pessoais na rede e da legislação vigente no Brasil, examinando-se, após, o funcionamento do aplicativo e os termos de uso e política de privacidade do provedor *Netflix*, sendo que, ao final, verificar-se-á a conformidade desses documentos e da forma de funcionamento do provedor com a regulamentação brasileira.

1 A EVOLUÇÃO LEGISLATIVA BRASILEIRA E A PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE DIGITAL

Com o advento da internet, ascenderam novas formas de comunicação, novas ferramentas e, principalmente, novas mudanças na sociedade. Como bem aponta Manuel Castells, “a Internet é um meio de comunicação que permite, pela primeira vez, a comunicação de muitos com muitos, num momento escolhido, em escala global” (CASTELLS, 2003, p. 08). Com esse crescente aumento na sua utilização pelos internautas,

ocorre, no mesmo patamar, a coleta cada vez maior de informações dos próprios usuários pelos provedores de conexão e aplicação na internet⁴.

Na esteira do desenvolvimento tecnológico, ampliando as fronteiras de transmissão da internet, intensificaram-se também os fluxos de informações e possibilidades de armazenamento delas. Essa ampliação da tecnologia trouxe como consequência imediata a crença de que a internet era um ambiente neutro e seguro (SARLET; CALDEIRA, 2019, p. 02), posto que, na mesma medida de seu desenvolvimento, seu uso se democratizava. Nesse cenário, o maciço aumento de sua utilização passou a trazer mudanças no conceito de privacidade, de forma que a informação passou a ser estruturada, evidenciando riscos de violação dessa privacidade pela possibilidade de uso indevido dessas informações (FINKLESTEIN; FINKELSTEIN, 2019, p. 285).

Manuel Castells, trabalhando a partir de uma lógica de vigilância da rede, alerta que “o entusiasmo com a liberdade trazida pela Internet foi tamanho que esquecemos a persistência de práticas autoritárias de vigilância [...]” (CASTELLS, 2003, p. 143), sendo que grande parte desses mecanismos são efetivados com o próprio consentimento do usuário, detentor dessas informações. É dentro desse contexto que se afirma que os novos meios de comunicação oriundos da sociedade em rede vão na contramão da preservação da privacidade das pessoas, que têm obstáculos em assumir o controle das informações que delas são extraídas (RUARO; GLITZ, 2019, p. 342).

Nesse sentido, “uma vez que dados são coletados em forma digital, todos os itens de informação contidos no banco de dados podem ser agregados, desagregados, combinados e identificados” (CASTELLS, 2003, p. 142), demonstrando que, na verdade, é necessário haver cautela no que diz respeito à utilização da rede para a adequada proteção do usuário da internet. Ressalta-se ainda que as ferramentas conexas ao “acesso à internet, telefones móveis, televisão interativa, entre outros, extraem dos cidadãos/usuários uma gama crescente de dados pessoais que são oferecidos ‘gratuitamente’ aos fornecedores de bens e serviços” (BUCHAIN, 2019, p. 210). Normalmente, as formas de tratamento, coleta e utilização dessas informações são realizadas sob o argumento da utilização para execução contratual ou com o próprio consentimento do usuário, que, para ter acesso ao serviço, acaba aceitando as condições. Todavia, a lição de Rodotà é de que “o problema dos excessos na coleta de informações e dos abusos na sua utilização pode ser enfrentado com técnicas que não confiem somente no consentimento dos interessados.” (RODOTÀ, 2008, p. 81), ou seja, mediante a utilização de

⁴ Segundo o Marco Civil da Internet, aplicação de internet é o “conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”. (BRASIL, 2014).

instrumentos jurídicos e tecnológicos que efetivamente protejam o usuário, mesmo que este tenha dado seu consentimento.

É dentro dessa questão que se debate acerca da proteção de dados pessoais⁵ dos usuários, especialmente mediante a criação dos instrumentos jurídicos mínimos que possibilitem a salvaguarda dos internautas. Diga-se que “a experiência legislativa segue justamente nessa direção, confirmando como é impossível prescindir de uma estratégia institucional articulada e integrada” (RODOTÀ, 2008, p. 81), devendo constituir efetiva atuação estatal na gestão e criação dos mecanismos necessários de regulação das práticas do ambiente da informação, que transcendem as fronteiras e a soberania de qualquer Estado. Sendo assim, “[...] a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas – *i.e.* é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos” (RODOTÀ, 2008, p. 17).

Alerta Danilo Doneda (2019, p. 24) que é “necessário que o ordenamento jurídico estabeleça critérios proporcionais de tutela da pessoa nesta área, que é muito fortemente ligada ao desenvolvimento da tecnologia”, uma vez que “a internet constitui um ambiente de exercício de diversos direitos fundamentais [...] a proteção da privacidade e dos dados pessoais apresenta-se como um pressuposto para o exercício desses direitos”. (MENDES, 2016, p. 38). Essa preocupação já vem de décadas no continente europeu, fazendo surgir marcos normativos acerca da proteção de dados, a exemplo da Convenção 108, de 1981, do Conselho da Europa, da Diretiva 95/46/CE e do Regulamento Geral de Proteção de Dados da União Europeia. Além disso, ao longo do tempo foram promulgadas diversas iniciativas legislativas dos países nessa temática, a exemplo da Lei 78-17, denominada *Informatique et Libertés*, e 1978, na França; da Lei do *Land* alemão de Hesse, em 1970, na Alemanha; *Datenschutzgesetz*, Lei n.º. 565/1978, da Áustria; da Lei de Proteção de Dados Pessoais n.º 25.326, de 2000, na Argentina.

No Brasil, “a proteção de dados pessoais no ordenamento jurídico brasileiro somente se estruturou em torno de um conjunto normativo unitário muito recentemente” (DONEDA, 2019, p. 259), sendo seu contexto de formação decorrente das disposições de direitos fundamentais previstas na Constituição da República, “cuja relação, propósito e alcance são

⁵ Conforme lição de Sarlet e Caldeira (2019, p. 2), “dados pessoais são todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular”. Tal conceito é ainda ampliado quando se fala em dados pessoais sensíveis, que são “aqueles que tratam sobre a origem racial e étnica, as convicções políticas, ideológicas, religiosas, as preferências sexuais, os dados sobre a saúde, os dados genéticos e os biométricos” (SARLET; CALDEIRA, 2019, p. 2).

fornecidos pela leitura da cláusula geral da personalidade” (DONEDA, 2019, p. 259). Esse amparo constitucional dos dados pessoais tem tido seu alcance a partir dos direitos fundamentais da privacidade, intimidade, além da própria dignidade da pessoa humana, que vinham servindo de substrato teórico constitucional para essa fundamentação⁶.

Uma das primeiras legislações brasileiras a dispor, de forma mais sistematizada, sobre a regulação da internet foi o Marco Civil da Internet, promulgado no ano de 2014, iniciando no país uma nova fase no que tange aos direitos do usuário na internet. Tal legislação “denota a transformação do pensamento e os esforços do legislador brasileiro para regulamentar o uso da Internet com o estabelecimento de princípios, garantias, direitos e deveres” (CRESPO; RIBEIRO FILHO, 2019, p. 171). Além disso, “inevitavelmente a instituição do Marco Civil da Internet também trouxe ao meio jurídico o debate sobre a necessidade de uma norma jurídica que recepcionasse e reconhecesse direitos, dentro do contexto da internet no Brasil” (FORTES, 2016, p. 120).

Amparado em nove princípios não taxativos dispostos no artigo 3º, com especial enfoque aos princípios da proteção da privacidade e dos dados pessoais, o documento legal fundamenta o direito à privacidade como necessário para utilização da internet (FORTES, 2016, p. 127), bem como assenta a neutralidade da rede como um de seus fundamentos. Diga-se que “acertou o Legislador ao estabelecer um regime jurídico de proteção de dados pessoais no âmbito da regulamentação do uso da internet no país.” (MENDES, 2016, p. 38), tendo em vista que a lei adiantou-se na disciplina das informações dos internautas, prevendo regramentos mínimos para as operações envolvendo dados pessoais (FORTES, 2016, p. 128). Observa-se, então, que “além de proteger a privacidade em geral, o Marco Civil dá ênfase à proteção dos dados pessoais, informações que podem identificar uma pessoa e que comumente são utilizadas ou requeridas pelos provedores de acesso à internet ou provedores de serviços no Brasil” (JESUS; MILAGRE, 2014, p. 22).

Dentre os principais pontos de avanço do Marco Civil da Internet, é recepcionado o consentimento, de forma expressa, sobre a coleta, uso, armazenamento e tratamento de dados pessoais, abrindo, inclusive, a “possibilidade de exclusão definitiva dos dados pessoais que tiverem sido fornecidos para determinada aplicação de internet, a requerimento do

⁶ Recentemente, o Supremo Tribunal Federal, no julgamento das ADIs nº 6387, 6388, 6389, 6390 e 6393, na qual se postulava a inconstitucionalidade de medida provisória de compartilhamento de dados do IBGE para políticas oriundas da pandemia de coronavírus, reconheceu a proteção de dados pessoais como um direito fundamental implícito, em linha semelhante daquilo que já vinha fazendo a doutrina especializada e outras cortes constitucionais.

interessado” (FORTES, 2016, p.128), sendo que aqueles que violarem os dados pessoais poderão também ser responsabilizados. Veja-se que

Na oportunidade, o legislador houve por bem sedimentar a proteção à privacidade e trouxe um capítulo exclusivo para a salvaguarda dos dados pessoais, cuja aplicação, contudo, depende do uso da internet. Ainda que a referida Lei não estivesse voltada, fundamentalmente, à autonomia dos dados pessoais, sua contribuição foi de grande valia (CRESPO; RIBEIRO FILHO, 2019, p. 171).

Apesar dessas inovações trazidas, o Marco Civil da Internet “trouxe a necessidade de regulamentação de dispositivos específicos como é o caso da seção que trata da proteção da privacidade e dos dados pessoais na rede” (FORTES, 2016, p. 172). No mesmo sentido das legislações mundiais, a proteção de dados, especialmente no ambiente informático, exige sua normatização através de lei específica.

Diante disso, surgiu a Lei Geral de Proteção de Dados Pessoais, qual seja a Lei nº. 13.709, promulgada em 2018, atendendo a uma exigência já existente no Marco Civil da Internet em seu artigo 3º, inciso III. A LGPD⁷, como é chamada, disciplina “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), inovando nas disposições sobre a proteção de dados, segurança na rede, governança digital, além de criar a Autoridade Nacional de Proteção de Dados Pessoais.

Fortemente inspirada pelo Regulamento Geral de Proteção de Dados europeu⁸, a lei brasileira fez crescer ainda mais o debate acerca da proteção de dados pessoais, trazendo inovações, conceitos e regramentos referentes ao tratamento de dados no Brasil. Como ponto de partida ao estudo, observa-se que a lei conceitua dado pessoal como a “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018), além de

⁷ Não se olvida no presente trabalho a proteção também conferida pelo Código de Defesa do Consumidor no tocante aos bancos de dados dos consumidores. Nesse sentido, “no Código de Defesa do Consumidor, a Seção VI do Capítulo V é dedicada aos bancos de dados e cadastros de consumidores e tem no art. 43 o seu principal dispositivo. Ele garante o acesso às informações arquivadas sobre o consumidor e suas respectivas fontes, além de estabelecer um prazo máximo da permanência delas no cadastro, o dever de informar sua abertura e de proceder à imediata correção de informações falsas ou equivocadas, a pedido do consumidor” (OLIVEIRA; LOPES, 2019, p. 67). Todavia, dado o enfoque na temática acerca da declaração de privacidade e da forma de tratamento dos dados, submetido a legislação própria, não será realizada a análise sob o viés consumerista, apesar da proximidade das temáticas.

⁸ Sobre esse ponto, Ruaro e Glitz (2019, p. 346) referem: “A legislação europeia foi a grande norteadora da Lei Geral de Proteção de Dados Pessoais no Brasil, servindo de grande inspiração e refletindo importantes contribuições em nossa lei. Porém, o ponto mais emblemático desta inspiração legislativa está justamente no fato da diferença cultural existente entre a União Europeia e o Brasil. A comunidade europeia possui uma cultura de preservação da sociedade [...]. Em contrapartida, a população brasileira possui uma cultura bastante distinta da europeia, na qual o titular dos dados, por exemplo, não vê mal algum em fornecer o número de seu CPF para obter um mísero desconto em uma farmácia”.

categorizar como dado pessoal sensível 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” (BRASIL, 2018). Em síntese, o âmbito de proteção do dado pessoal sensível é mais específico e com maiores regramentos, exigindo especial atenção por parte do agente de tratamento, dada a natureza dessas informações.

Além disso, um dos principais pontos é o conceito conferido ao tratamento de dados pessoais, que é

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

Em resumo, o tratamento – aqui se tratando em relação aos dados de meios digitais – contempla, por exemplo, qualquer tipo de cadastro, solicitação de serviços, consumo de mídias pela internet, para o qual é necessário o fornecimento das informações ao provedor, demonstrando a verdadeira amplitude daquilo que é o tratamento feito na rede pelos provedores de aplicação⁹. Além disso, com essa forma de operação das informações em meios digitais, Doneda (2020, p. 151) pontua uma “mudança qualitativa no tratamento dos dados pessoais, à qual aludimos, baseia-se na utilização de novos métodos, algoritmos e técnicas”, sendo, dentre essas técnicas, a do *profiling*, que consiste em traçar o perfil do usuário, comumente utilizado para mapear gostos e interesses do usuário, com o objetivo de qualificar a prestação do conteúdo.

Com isso, assume especial relevo no atual panorama do tratamento dos dados pessoais nas mídias a questão referente ao consentimento. Apesar de já ter sido previsto no Marco Civil da Internet, a Lei Geral traçou contornos mais específicos sobre o instituto, definindo-o como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018), tratando-se de um ato unilateral do titular, vinculado, normalmente, à disposição contratual (DONEDA, 2006, p. 378).

⁹ Destaca-se que a LGPD não utiliza a nomenclatura provedores de aplicação, utilizada pelo Marco Civil da Internet. Diferentemente, separa os agentes da rede por critério de agentes de tratamento, dividindo-os em controlador, que é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018) e operador, que é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (BRASIL, 2018).

Conectado com o fundamento da autodeterminação informativa, previsto no artigo 2º, inciso II, “o consentimento do titular dos dados recebeu tutela destacada na LGPD, ainda que não seja, vale lembrar, a única hipótese legal para o tratamento de dados pessoais nem hierarquicamente superior às demais” (TEPEDINO; TEFFÉ, 2019, p. 297-298). Todavia, é inegável o papel assumido pelo instituto com a promulgação da lei, frente as suas demais disposições, uma vez que se denota a “ênfase atribuída ao consentimento, seguindo a linha do regulamento europeu e das normas mais atuais sobre o tema, além de uma série de disposições que oferecem regramento específico para concretizar, orientar e reforçar o controle dos dados através do consentimento” (TEPEDINO; TEFFÉ, 2019, p. 298).

Para Danilo Doneda (2006, p. 377), a importância do instituto “reside na possibilidade de autodeterminação em relação aos dados pessoais, e que esta autodeterminação deve o elemento principal a ser levado em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos deste consentimento”. Entretanto, o mesmo autor adverte acerca de dois pontos a serem observados quando se está a analisar o consentimento: a utilização dele com o caráter meramente acessório, ligado a uma situação fundamental; e que seja ele um procedimento inócuo (DONEDA, 2019, p. 298-299). Diga-se que “o confronto com situações reais revela que, em tais situações, a alternativa a não revelação dos dados pessoais pelo seu titular costuma ser uma – por vezes, brutal – renúncia a determinados bens ou serviços” (DONEDA, 2019, p. 298), fazendo com que o titular deixe de ter acesso ao aplicativo, rede social, serviço, pelo simples fato de não ter concordado com a forma de operação dos dados pelo provedor¹⁰.

Nesse sentido é que se diz que o consentimento deve ser informado, ou seja, o titular dos dados deve ter ciência acerca daquilo que está consentindo sobre seus dados, bem como ser advertido sobre a negativa em fornecê-lo, sendo plenamente vedado o consentimento dado de maneira genérica, nos termos do artigo 8º, §4º¹¹. Essa necessidade de que ele seja informado serve “para evitar que seja inviabilizado pelos modelos de negócios em que se

¹⁰ Como bem já advertiu Rodotà (2008, p. 76), “o condicionamento deriva do fato de que a possibilidade de usufruir determinados serviços, essenciais ou importantes, ou tidos como tais, depende não somente do fornecimento de determinadas informações por parte do usuário do serviço, mas também do fato de que tais informações (eventualmente com base no consentimento do interessado) podem posteriormente ser submetidas a outras elaborações. Este é o caso de todos os serviços obtidos através das novas mídias interativas, cujos gestores, por evidentes razões de ordem econômica, estão prontos a exercer forte pressão sobre os usuários para que estes autorizem a elaboração (e a eventual transmissão a terceiros) de ‘perfis’ pessoais ou familiares baseados nas informações coletadas por ocasião do fornecimento dos serviços”.

¹¹ Conforme Lima e Ramiro (2020, p. 252) “a fim de corrigir tal assimetria, a LGPD determina que será nulo o consentimento manifestado de maneira genérica (art. 8º. §4º da LGPD), ou seja, o consentimento deve estar relacionado à uma finalidade específica do tratamento de dados pessoais inclusive por que assim estabelecem os princípios da finalidade, adequação e necessidade (art. 6º, inc. I, II e III da LGPD). Além disso, o consentimento fornecido por escrito deve constar de cláusulas destacadas das demais (art. 8º, §1º da LGPD)”.

pretende impor o consentimento sem dar o efetivo conhecimento ao titular dos dados pessoais” (LIMA; RAMIRO, 2020, p. 252). Veja-se que “para diminuir a assimetria técnica e informacional existente entre as partes, exige a lei que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados” (TEPEDINO; TEFFÉ, 2019, p. 301).

Todavia, importante lembrar que o consentimento não é o único meio que permite o tratamento de dados pessoais. A Lei Geral arrola dez hipóteses em seu artigo 7º que possibilitam que os agentes de tratamento operem com dados, podendo-se citar, dentre eles, o próprio consentimento, a proteção do crédito, cumprimento de obrigação legal pelo controlador, execução contratual, entre outros (BRASIL, 2018). Aqui, no presente estudo, ganha relevo a hipótese atinente ao tratamento de dados para execução contratual, prevista no inciso V do artigo 7º (BRASIL, 2018), tendo em vista que diz respeito a todas aquelas informações inerentes para que o ajuste realizado entre controlador e titular dos dados possa adequadamente dar continuidade, englobando dados como CPF, algumas informações bancárias, entre outros.

Como bem adverte Marcacini, “aqui, os dados são de algum modo essenciais ao contrato de que o seu titular é parte, e por isso hão de ser fornecidos ao outro contratante que, com certos limites, fará seu tratamento” (MARCACINI, 2020, p. 145), ou seja, apenas deverão ser tratados aqueles necessários para o contrato. Importa ressaltar que o tratamento dos dados não abrangidos por essa previsão – execução contratual, ou seja, que excedem o mínimo, não contam com essa autorização, sendo necessária a sua permissão por outras possibilidades previstas no artigo 7º, como, por exemplo, o consentimento do usuário.

Essas hipóteses de tratamento – especialmente o consentimento e a execução contratual - devem observar e ser lidas em conjunto com outros pontos fulcrais da LGPD, quais sejam os princípios da finalidade, adequação, necessidade e transparência do tratamento dos dados pessoais, que balizam a interpretação e as operações dessas informações. Como se pode observar, esses princípios estão dispostos no artigo 6º, juntamente com os outros princípios do livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização, pautando a forma de tratamento de dados pessoais (BRASIL, 2018).

Acerca do princípio da finalidade, é importante a lição de Rodotà, para quem o princípio assume “particular intensidade quando os dados pessoais do usuário do serviço não são solicitados por quem oferece o serviço, mas são uma consequência quase ‘natural’ do fornecimento do próprio serviço” (RODOTÀ, 2008, p. 204). Ainda, segundo o autor, “torna-se essencial para determinar a legitimidade do uso dos dados coletados, seu tempo de

conservação, a admissibilidade de sua interconexão com informações contidas em outros bancos de dados” (RODOTÀ, 2008, p. 204).

Segundo a própria LGPD, a finalidade diz respeito à “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), não se podendo utilizar de finalidades genéricas ou imprecisas para tratamento dos dados. Nesse sentido, “os provedores de aplicações de internet não podem guardar dados pessoais que excedam a finalidade pela qual o usuário titular consentiu que armazenassem, salvo em casos específicos previstos em Lei” (FLUMIGNAN; FLUMIGNAN, 2020, p. 129). Correlacionando com o papel do consentimento, deve o titular consentir com esta finalidade informada pelo controlador, jamais devendo estar a finalidade descolada do consentimento a ela permitido.

Em sentido semelhante é previsto o princípio da adequação. Conforme a própria definição legal, a adequação é “a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (BRASIL, 2018). Apesar da semelhança com a finalidade, a adequação se encontra em uma dimensão mais objetiva, exigindo a compatibilidade do serviço ou produto com as informações coletadas (FLUMIGNAN; FLUMIGNAN, 2020, p. 130).

Por sua vez, a necessidade vem estampada pela restrição dos dados coletados a apenas aqueles necessários para a finalidade informada (OLIVEIRA; LOPES, 2019, p. 75). Conforme a definição dada pela LGPD, o princípio da necessidade diz respeito a “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” (BRASIL, 2018). Também há que se conferir o destaque ao princípio da transparência, que é a “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” (BRASIL, 2018). Por esse princípio, exemplificativamente:

[...] pode-se citar o fato de que não é possível o compartilhamento de dados pessoais com terceiros de forma oculta. Caso quem efetue o tratamento de dados pessoais deseje repassá-los a terceiros, inclusive para operadores que sejam essenciais à execução do serviço, é necessário informar e obter o consentimento do titular dos dados pessoais (FLUMIGNAN; FLUMIGNAN, 2020, p. 130).

Por esses motivos que tal princípio é um dos mais presentes na LGPD, dado que não se encontra apenas no momento da coleta, mas por toda a operação de dados (OLIVEIRA; LOPES, 2019, p. 76), podendo estar presente inclusive após todo o tratamento das informações. Se somados todos os fatores previstos na legislação, além da importância elevada da proteção dos dados, do consentimento, da finalidade, adequação, necessidade e transparência do tratamento, verifica-se farto arcabouço protetivo do internauta no que toca às suas informações concedidas.

Nesse contexto, há a crucial necessidade de adequação das políticas de privacidade de empresas, provedores de conexão e aplicação, a essas previsões normativas, tendo em vista que, em razão da coleta dos dados pessoais, os usuários, pelas informações por ele fornecidas, são rotineiramente identificados pelos provedores, demonstrando os indicativos de sua personalidade (DONEDA, 2019, p. 23). Como já dito, essas informações concedidas pelos internautas e coletadas pelos provedores devem ser protegidas, evitando-se qualquer violação dos direitos dos usuários, cuja forma de utilização pelo controlador/provedor é prevista nos termos e condições de uso e dos documentos relativos às políticas de privacidade do *software*, *site*, aplicativo, etc.

Dessa maneira, já assentadas as premissas teóricas para subsidiar o presente estudo, angariando informações e elementos necessários para a análise pretendida, importa agora adentrar na temática acerca do aplicativo de *streaming Netflix*, situando o caso concreto em análise, especialmente o modo de funcionamento, políticas de privacidade, sistemas de recomendação, modo de tratamento de dados pessoais, etc, para, então, se verificar se o tratamento realizado pelo provedor é regular e adequado diante do que foi até agora exposto, com destaque ao previsto pela Lei Geral.

2 A ASCENSÃO DO *STREAMING*: *NETFLIX* E O SISTEMA DE RECOMENDAÇÃO DE CONTEÚDO BASEADO NA TÉCNICA DO *PROFILING*

Como já destacado, a internet possibilitou ampliar os meios de comunicação entre a população, além de facilitar o acesso a diversos bens culturais, anteriormente de difícil ou impossível acesso para grande maioria das pessoas. Aduz Castells (2016, p. 437) que “hoje existem milhões de usuários de redes no mundo inteiro, cobrindo todo o espectro da comunicação humana, da política e da religião ao sexo e à pesquisa – com o comércio eletrônico como atração principal da internet contemporânea”.

Essa massificação da rede corroborou para o aumento do acesso a determinadas plataformas, *sites* e diversos meios de comunicação, uma vez que “o que caracteriza o novo sistema de comunicação, baseado na integração em rede digitalizada de múltiplos modos de comunicação, é sua capacidade de inclusão e abrangência de todas as expressões culturais” (CASTELLS, 2016, p. 456). Da música à poesia, dos filmes às séries, da arte às diversas formas de expressão humana, a internet fez emergir usuários e serviços diversos que ofertassem esses bens culturais à disposição na rede.

Nesse sentido é que se destaca a crescente utilização pelos usuários de provedores de aplicação que fornecem determinados tipos de conteúdo *on line*, a exemplo de músicas, filmes e séries, por meio de plataforma denominada de *streaming*. Manuel Castells, ainda em 2003, já trazia a popularidade desse novo meio transmissão de conteúdo, especialmente pelo aumento do consumo de músicas na rede (CASTELLS, 2003, p. 161). Essa plataforma, citando-se como exemplo o consumo de músicas, “é uma forma de distribuição digital que dá acesso *online* a um catálogo ‘ilimitado’ de músicas gravadas, instantaneamente, em qualquer hora e local.” (MOSCHETTA; VIEIRA, 2018, p. 259) [grifo do autor]. Contudo, com a criação do *streaming*, “ao contrário de redes *peer-to-peer*, não exige o *download* antecipado das músicas, que são armazenadas em um servidor remoto e acessadas sob demanda a partir de qualquer dispositivo ligado à rede [...]” (MOSCHETTA; VIEIRA, 2018, p. 259) [grifo do autor].

Anteriormente, o internauta deveria realizar o armazenamento do arquivo, que se encontrava em outro servidor em lugar diverso, em seu dispositivo informático, para, então, poder ter acesso àquela mídia desejada. Com o *streaming*, não é necessário realizar o armazenamento, bastando que o usuário acesse a plataforma de modo *online* e usufrua dos serviços oferecidos pelo provedor. Em síntese, não há a necessidade de realizar a transferência do arquivo, possibilitando a utilização em tempo real, mediante fluxo contínuo de dados disponibilizado pelo provedor.

Dentre os aplicativos que se utilizam dessa forma de plataforma, vem ganhando popularidade pelos internautas e usuários o aplicativo de *streaming* da empresa *Netflix*¹², se sobressaindo no que toca à veiculação de mídias de vídeo, como filmes, séries, documentários, etc. Destaca-se que “inicialmente, ela se voltava para serviços de locação online de DVDs via correio por meio de seu site. Em 2007, adotou a tecnologia de *streaming*,

¹² Para os efeitos do presente estudo, considera-se o aplicativo *Netflix* como agente de tratamento de dados pessoais, tendo em vista que tanto é responsável pela decisão referente ao tratamento, como é quem realiza essa operação.

disponibilizando diversos conteúdos via internet” (ALZAMORA; SALGADO; MIRANDA, 2017, p. 43). Esse grande crescimento de mercado do aplicativo se deu principalmente nas democracias emergentes, a partir da segunda década do século XXI, a exemplo do Brasil, México e Coreia do Sul, sendo que, em janeiro de 2020, a empresa dispunha de 177 milhões de assinantes pelo mundo (MEIMARIDIS; MAZUR; RIOS, 2020, p. 6), passando a ganhar notoriedade ainda maior a partir da produção da série *House of Cards*.

De locadora de vídeos à plataforma digital, o modo atual de operação de “*Netflix* singulariza experiências contemporâneas de distribuição, circulação e produção de conteúdo audiovisual por operar na interseção entre referências audiovisuais provenientes de tradicionais meios de comunicação de massa” (MIRANDA, 2017, p. 19) [grifo do autor]. Dentro desse contexto de crescimento no meio digital, tem-se que a utilização do *streaming* foi fundamental para o aprimoramento do aplicativo, possibilitando sua ampliação e crescimento dos conteúdos fornecidos, que podem ser acessados de qualquer local e de qualquer aparelho conectado à rede (MIRANDA, 2017, p. 25).

O sucesso desse mercado se deve a uma das principais técnicas utilizadas por *Netflix*, que é o seu sistema de recomendação de conteúdo aos usuários a partir de mecanismos envolvendo algoritmos¹³. Diga-se que “esses mecanismos fazem parte das dinâmicas midiáticas de circulação e consumo em *Netflix* desde seus primeiros anos, por meio do *software CineMatch*, lançado em 2000” (MIRANDA, 2017, p. 47) [grifo do autor], sendo que com essa técnica de recomendação são utilizados instrumentos de perfilamento, ou *profiling*, objetivando inferir gostos, hábitos, etc., a partir das informações pessoais concedidas pelo próprio usuário. Acerca do tema, Danilo Doneda expõe que:

Esta técnica, conhecida como *profiling*, pode ser aplicada a indivíduos, bem como estendida a grupos. Com ela, os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma ‘metainformação’, que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo (DONEDA, 2019, p. 151) [grifo do autor].

Contudo, quando se trata da plataforma em análise, é desconhecido o modo interno de seu funcionamento, apenas sendo observáveis alguns aspectos externos de como é utilizado

¹³ A título de contextualização, os algoritmos “são um conjunto de comandos (protocolos) que servem de base para qualquer sistema computacional” (ALZAMORA; SALGADO; MIRANDA, 2017, p. 44-45), que, por sua vez, são “cálculos matemáticos (logaritmos), funções, fórmulas, códigos ou *softwares* programados por humanos que visam realizar uma tarefa por meio da resolução de algum problema e que reconhecem informações e produzem outras” (ALZAMORA; SALGADO; MIRANDA, 2017, p. 45) [grifo do autor].

o sistema de recomendação (MIRANDA, 2017, p. 48), como “no momento do cadastro de um novo assinante, por exemplo, *Netflix* solicita que o usuário selecione produtos que já assistiu ou que pretende ver” (MIRANDA, 2017, p. 48) [grifo do autor]. Após isso, “o usuário é convidado a pontuar de uma a cinco estrelas os títulos que sinalizou ter assistido – essa ação não é obrigatória. Depois, ele é direcionado para a página central do acervo da plataforma, indicando alguns conteúdos que poderiam ser de seu interesse” (ALZAMORA; SALGADO; MIRANDA, 2017, p. 46) [grifo do autor].

É dessa análise inicial, aliada as posteriores que são realizadas durante a utilização dos serviços do aplicativo, que a empresa pode mapear os gostos e interesses do usuário, propondo outros títulos de filmes e séries, que poderiam ser de seu interesse. Além disso, “os sistemas de recomendação ainda atuam como relevante ferramenta de interpretação de hábitos culturais para *Netflix*, auxiliando no ramo de suas produções exclusivas e ações de *marketing*, além de atuarem nas dinâmicas de circulação e consumo” [...] (MIRANDA, 2017, p. 50) [grifo do autor]. Dessa maneira, os algoritmos, além de recomendarem¹⁴ determinadas mídias ao usuário a partir do perfilamento realizado, também auxiliam a empresa a produzir novos filmes e séries baseados, justamente, nos gostos e interesses do grande grupo de assinantes¹⁵. Nesse sentido, observa-se que

Por meio desses mecanismos, *Netflix* pôde prever preferências de consumo de seus usuários e lançar produtos como a série *House Of Cards*. [...] O emprego de dados no auxílio à produção de séries originais de *Netflix* se relaciona aos sistemas de recomendação e, desse modo, remete à adoção de lógica algorítmica no processo criativo humano. De maneira correlata, os sistemas de recomendação algorítmica de plataformas midiáticas online operam na formação de públicos (ALZAMORA; SALGADO; MIRANDA, 2017, p. 48) [grifo do autor].

Em síntese, o sistema de recomendação utilizado por *Netflix* é o ponto central e fundamental de seu funcionamento, responsável pelo grande sucesso mundial. Contudo, “*Netflix* também lança mão de contas oficiais em redes sociais on-line, como *Facebook* e *Twitter*, que atuam como alicerces adjacentes das dinâmicas de circulação dos conteúdos ofertados pela companhia” (MIRANDA, 2017, p. 15-16) [grifo do autor].

¹⁴ Destaca-se, inclusive, que além do aplicativo fornecer sugestões baseadas nos dados fornecidos pelo usuário, também oferece sugestões baseadas em técnicas de georreferenciamento, a exemplo de filmes e séries que estariam sendo assistidas na região de residência do assinante, como se extrai da sua declaração de privacidade, que será adiante abordada, quando refere ao uso dos dados para “determinar sua localização geográfica aproximada, oferecer conteúdo localizado, oferecer recomendações personalizadas e customizadas de filmes e séries que, na nossa avaliação, poderiam ser do seu interesse” (NETFLIX, 2019).

¹⁵ Diversos são os estudos realizados para analisar o funcionamento desses sistemas e o modo como a empresa explora os interesses dos usuários. Nesse sentido, cite-se interessante estudo de *Netflix* explorando a nostalgia e interesse dos usuários a partir de produções anteriores com a série *Stranger Things* (ALZAMORA; SALGADO; MIRANDA, 2017, p. 38-59).

Toda essa sistemática de recomendação é baseada na coleta e tratamento dos dados pessoais do assinante do serviço do aplicativo por intermédio dessa prática do *profiling*, pelo qual “se torna possível não só um controle mais direto do comportamento dos usuários, como também a identificação precisa e atualizada de certos hábitos, inclinações, interesses, preferências” (RODOTÀ, 2008, p. 62). Conforme lição de Rodotà, essas informações seriam a possibilidade de uma nova mercadoria capaz de alterar as relações de consumo, diminuindo, contudo, a autonomia do consumidor (RODOTÀ, 2008, p. 62).

Esse novo mercado envolvendo informações pessoais dos usuários não é novidade no cenário mundial envolvendo a sociedade em rede. Citando o exemplo das empresas *Facebook, Amazon, Google, Microsoft e Apple*, acentuam Terra e Mulholland que o modo de se fazer mercado dessas empresas é baseado na coleta de dados para proporcionar ao seu usuário conteúdos, informações e serviços personalizados a ele, sob o argumento de otimizar a atividade ou o produto (TERRA; MULHOLLAND, 2019, p. 616). Doneda, por sua vez, adverte a necessidade de mediar a utilização desse tipo de segmento mercadológico, envolvendo a operação de informações de seus usuários, típico da atual era, com a adequada proteção de dados pessoais e as legislações vigentes que os protegem de práticas abusivas envolvendo os dados:

O cerne do problema reside, portanto, justamente em se conciliar os imperativos inafastáveis deste modelo de negócios com as diversas normativas de proteção de dados que abordam justamente as modalidades de tratamento de dados, bem como com as legítimas expectativas dos seus próprios usuários de divulgação de informações pessoais. (DONEDA, 2012, p. 12).

Nesse sentido, considerando as disposições normativas acerca do tratamento de dados, as práticas dos aplicativos devem ser de conhecimento do usuário, que concordará ou não com essas operações de suas informações pessoais. Essas operações se encontram destacadas em documentos disponibilizados pelo provedor de aplicação, normalmente denominadas de termos e condições de uso e declaração de privacidade, expondo o modo de coleta, tratamento e demais disposições acerca do tratamento de dados, além das condições de utilização do provedor contratado, bem como os possíveis direitos que os usuários possuem. É sobre esse tema que versará o próximo tópico.

3 NETFLIX E PROTEÇÃO DE DADOS PESSOAIS: É POSSÍVEL SE FALAR EM USUÁRIO SUFICIENTEMENTE PROTEGIDO FRENTE AOS TERMOS DE USO E DECLARAÇÃO DE PRIVACIDADE?

Necessário investigar, diante do que foi até agora exposto, se os termos de uso e a respectiva declaração da privacidade do aplicativo *Netflix* se encontram suficientes frente à legislação brasileira, conferindo a adequada proteção de dados de seus usuários, especialmente frente aos princípios da LGPD e as hipóteses de tratamento de dados. Para a base da presente análise, utilizaram-se os termos de uso com a última atualização datada de 31 de dezembro de 2019 e a declaração de privacidade com a última atualização realizada em 31 de julho de 2020, sendo que ambas estão disponíveis no *site* da plataforma¹⁶.

Um esclarecimento inicial é o de diferenciar termos de uso de declaração de privacidade. Apesar de os documentos serem semelhantes, dispostos, normalmente, nas mesmas abas de acesso de sítios e aplicativos da internet, ambos possuem diferentes âmbitos de proteção, pois,

[...] de modo geral, o termo de uso descreve como é a aplicação, além de informar as “regras internas” que devem ser obedecidas durante seu funcionamento. Enquanto que a política de privacidade informa ao usuário questões relacionadas à privacidade de seus dados, por exemplo, informações a respeito da coleta e tratamento dos dados e localização dos servidores (YAMAUCHI; SOUZA; SILVA JÚNIOR, 2016, p. 03).

Nesse sentido, tem-se que para o tratamento de qualquer dado pessoal, a Lei Geral de Proteção de Dados Pessoais impõe dez bases legais, com especial atenção aqui ao consentimento do usuário de modo livre, inequívoco e informado (BRASIL, 2018), bem como o tratamento de dados para a execução contratual, conforme anteriormente visto.

É preciso lembrar que o consentimento “compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade” (DONEDA, 2019, p. 298). É ele um instituto fundamental, pois é “o consentimento para o tratamento de dados pessoais toca diretamente em uma série de elementos da própria personalidade, ainda que não no sentido exato da disposição desses elementos” (DONEDA, 2019, p. 302), eis que autoriza o tratamento de dados pessoais da pessoa. Em sendo dados pessoais sensíveis, há a obrigatoriedade de que esse consentimento seja dado de modo específico e para finalidade

¹⁶ Interessante destacar aqui que a publicidade desses documentos não se deve apenas em decorrência das disposições da relação de consumo, mas também de um direito do internauta expressamente previsto no Marco Civil da Internet, no inciso XI do artigo 7º, que preceitua o direito de “publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet” (BRASIL, 2014), bem como no disposto no §3º do artigo 10 da mesma lei. Ainda, há que se destacar o artigo 16 do Decreto nº. 8.771 de 2016, que regulamenta o Marco Civil da Internet, no qual aduz que “as informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais” (BRASIL, 2016). Em síntese, observa-se que a divulgação desses meios decorre de um dever de transparência entre provedor e usuário imposto pela legislação brasileira.

determinada, da qual o usuário seja previamente conhecedor, ou seja, esteja informado do objetivo do controlador no que toca àquela operação envolvendo os seus dados (BRASIL, 2018).

Além disso, a questão do tratamento de dados para a execução de contratos, com a ampliação dos serviços de *streaming* na internet passa a ter maiores contornos. Relembre-se que essa operação deve apenas se limitar ao mínimo de dados necessários para que o contrato seja adequadamente executado, sendo essa coleta implícita ao próprio contrato. Todavia, caso haja a coleta de dados superiores aos necessários para a execução, o tratamento dependerá da manifestação expressa do titular, que é o consentimento para tal ampliação do tratamento, objetivando que não haja violação dos direitos do usuário. É esse o entendimento de Marcacini, quando afirma que “o fornecimento de dados não necessários ao negócio teria seu quadro normativo no inc. I, do mesmo art. 7º, e as demais regras aplicáveis à espécie” (MARCACINI, 2020, p. 146).

Para a contratação dos serviços fornecidos por *Netflix*, o usuário adere aos seus termos de uso e a forma de tratamento de dados constante na declaração de privacidade, documentos que norteiam tanto a relação entre o usuário e a empresa, como o modo com que serão coletados, armazenados e utilizados os dados pessoais à disposição dela. Como ocorre em outros *sites*, aplicativos e demais serviços da internet, não é possível qualquer discussão acerca de eventuais cláusulas com a qual o usuário possa discordar, mostrando-se impositiva a aceitação e adesão às previsões. Ao se inscrever no aplicativo *Netflix*, conclui-se que o usuário concorda com o modo das políticas de uso do aplicativo, além das imposições de cláusulas para as quais não há margem à discussão, sem que se demonstre suficiente clareza nelas, especialmente sobre o uso de dados pessoais (ALZAMORA; SALGADO; MIRANDA, 2017, p. 49-50).

Da análise concreta da declaração de privacidade, é possível dividir a previsão de tratamento de dados em três tópicos, quais sejam a coleta de dados (fornecidos pelo usuário; coletados automaticamente; obtidos com parceiros; obtidos de outras fontes), uso de dados e divulgação de dados (família *Netflix* de empresas; prestadores de serviços; parceiros; ofertas promocionais), que, apesar de divididas, podem também ser lidas conjuntamente. Além disso, o documento conta com previsões sobre acesso a perfis, direitos do usuário, bem como disposições sobre *cookies*, o que também será brevemente abordado na presente pesquisa.

No que toca a coleta de dados, observa-se que o usuário consente com o recebimento e armazenamento de suas informações, que são fornecidas pelo assinante (nome, *email*, endereço, número, dados bancários), classificação de títulos, preferências pessoais

(NETFLIX, 2020). No momento do cadastro, são coletadas essas informações fornecidas pelo próprio usuário, a exemplo do nome, CPF, dados bancários, etc., que ficam armazenados e são tratados durante todo o período da contratação do aplicativo. As preferências pessoais são obtidas a partir dos sistemas de recomendação algorítmica, mediante os gostos anteriormente mapeados no momento do cadastro e da utilização.

São coletados automaticamente informações sobre as atividades no provedor, interações com a empresa, aparelhos conectados, dados sobre a conexão e também coletados por *cookies* (NETFLIX, 2020). Segundo a própria *Netflix*, *cookies* “são pequenos arquivos de dados, armazenados normalmente no seu aparelho enquanto você navega e utiliza sites e serviços online” (NETFLIX, 2020). A doutrina traz a definição de que são “dados digitais sobre as ações dos usuários em plataformas online” (ALZAMORA; SALGADO; MIRANDA, 2017, p. 50), podendo-se dizer, em síntese, que são rastros deixados pelo usuário daquilo que foi anteriormente visualizado, inclusive com os diversos aparelhos conectados a uma mesma conta, dada a sincronização existente. Os rastros digitais permitem que se recupere a visualização pretérita do usuário, reafirmando a possibilidade de oferecimento de conteúdo direcionado a partir dos sistemas de recomendação.

Ainda, há a coleta de dados obtidos com parceiros, os quais não são previamente declarados, limitando-se a informar o provedor de TV ou internet, operadores de telefonia, assistente de voz, outros provedores de aparelhos de *streaming* (NETFLIX, 2020), sendo que, dentre esses dados, são obtidos consultas e comandos, dados de ativação de serviços e endereço de IP (NETFLIX, 2020). Também aqui se destaca a obtenção de dados de outras fontes, limitando-se a informar que seriam prestadores de serviços de localização, serviços de pagamento e segurança, além das fontes publicamente disponíveis (NETFLIX, 2020). Veja-se que, apesar da aceitação dessas condições, dado que não são informações inerentes à execução do contrato, o usuário não possui a clareza e certeza de onde provêm os demais dados coletados pelo *Netflix*, apenas contando com a informação de que seriam com outros parceiros. Essa circunstância demonstra a vagueza da declaração de privacidade, dado que não há informação de quem são tais provedores, não havendo especificação da origem concreta, quais dados são recebidos e qual a finalidade de operar com esses dados, utilizados de forma síncrona entre *Netflix* e outra empresa. A ausência de transparência nesse momento da operação dificulta que o usuário possa, de fato, compreender o alcance das informações concedidas e ter o mínimo controle sobre elas.

Rememore-se que a criação de instrumentos legislativos, como a Lei Geral de Proteção de Dados, é destinada para assegurar ao usuário sua adequada proteção diante de

práticas que dificultem ele ter o conhecimento do que é realizado com as suas informações, as quais, por vezes, como é o caso, sequer possui a possibilidade de saber de onde são obtidos. Os instrumentos justamente servem “para evitar que seja inviabilizado pelos modelos de negócios em que se pretende impor o consentimento sem dar o efetivo conhecimento ao titular dos dados pessoais” (LIMA; RAMIRO, 2020, p. 252), além de fazer reduzir a diferença técnica e de informação existente entre a empresa e seu assinante.

Por sua vez, a empresa utiliza os dados para “oferecer, analisar, administrar, aprimorar e personalizar”¹⁷ (NETFLIX, 2020), os seus serviços, mediante a determinação de localização geográfica, coordenar com parceiros a disponibilização de seus serviços, proteger seus sistemas, atuar de modo a coibir atividades fraudulentas, entender seu público e comunicar novidades (NETFLIX, 2020). No ponto, a questão atinente ao georreferenciamento deve ser analisada detidamente, pois são utilizadas as informações coletadas da localização do usuário com o fim de “oferecer conteúdo localizado, oferecer recomendações personalizadas” (NETFLIX, 2020). Essa disposição também se observa nos termos de uso, informando que “o conteúdo que pode estar disponível irá variar segundo a sua localização geográfica e será alterado periodicamente” (NETFLIX, 2019). Em que pese a alegação de que são utilizados apenas para o oferecimento de conteúdo por parte do aplicativo, essa utilização deve ser vista com ressalvas, dado que a localização pode permitir a inferência se o usuário habita regiões mais populosas, em locais de vulnerabilidade social ou de condições mais abastadas, inclusive permitindo a diferenciação de conteúdo ofertado ao usuário.¹⁸

Além disso, há a previsão da divulgação de dados do usuário para as empresas que compõem o conglomerado empresarial *Netflix* – que o consumidor não sabe claramente quem integra - prestadores de serviços (marketing, publicidade, comunicação, segurança, infraestrutura e serviços de TI, segundo a empresa), utilizados para visualização de contas bancárias (tendo em vista que *Netflix* também permite o débito bancário para pagamento dos serviços), parceiros (utilizados para coordenar a prestação do serviço, como operação de assistente de voz, facilitar promoções pré-pagas, sugerir conteúdo), além de ofertas promocionais. Aqui, importa lembrar o que já visto acerca dos princípios da Lei Geral e do consentimento do usuário, pois necessário averiguar qual a real finalidade e objetivo de se

¹⁷ Essas são funções que estão previstas nos documentos em análise. Todavia, dado o caráter vago das previsões, não se podem descartar outras utilizações subterrâneas dos dados pessoais.

¹⁸ Uma diferenciação por questões econômicas, a partir das informações de georreferenciamento, não é novidade no Brasil. Com base nas disposições do Código do Consumidor, o Departamento de Proteção e Defesa do Consumidor, vinculado ao Ministério da Justiça, condenou a empresa Decolar.com por fazer a diferenciação de valores oferecidos com base na localização geográfica, o que faz emergir uma cautela redobrada quando se fala da utilização do georreferenciamento por empresas de grande porte (TERRA; MULLHOLLAND, 2019, p. 602)

utilizar todas essas informações consentidas pelo assinante. Do contrário, está a se verificar o pleno caráter inócuo do consentimento e de sua utilização apenas como caráter formal e acessório que, caso não concedido, importa a não utilização do serviço.

O conjunto de todas essas informações, registros prévios, preferências, *cookies*, georreferenciamento, entre outras, permite que a empresa consiga mapear o integral perfil de seu usuário e até mesmo prever os títulos que ele buscará assistir, formando, verdadeiramente, aquilo uma personalidade eletrônica do indivíduo. Nesse sentido, a tutela desses dados é elemento primordial da personalidade da pessoa e não deve ser polarizada entre ganhador e perdedor, dada sua importância para a esfera privada (RODOTÀ, 2008, p. 137).

É a partir desse conjunto de dados coletados, armazenados e repassados para terceiros, aliado os procedimentos vinculados à recomendação algorítmica que há potencial de que *Netflix* trabalhe com dados pessoais sensíveis, para os quais a lei impõe maiores requisitos para tratamento. Com o conjunto de dados, facilmente o sistema utilizado pode inferir informações pessoais referentes à religião, sexualidade, raça, entre outros, gerando sérios riscos à esfera da pessoa que o utiliza. Veja-se, por exemplo, o usuário que utiliza o aplicativo para consumir mídias sobre determinada religião com assiduidade. Dado o avanço do *software*, o sistema facilmente pode fazer a inferência e concluir que o assinante possui preferências sobre aquela programação religiosa e, a partir disso, passar a lhe fornecer conteúdo direcionado, o que implica realizar toda a operação com dados sensíveis ligados à religião da pessoa, criando uma verdadeira bolha que apenas fortalece o movimento de fechamento da pessoa para outras informações e bens culturais. O mesmo raciocínio é aplicável ao usuário com determinada opinião política que utilizaria o aplicativo para assistir determinadas mídias nesse viés. Contudo, todas as informações previstas nos documentos são vagas e não trazem uma concreta confiança de que haja o adequado tratamento e menos ainda o consentimento específico para tal.

Em síntese, quando se está a analisar os documentos que norteiam o tratamento de dados de *Netflix* se percebe que não se “explicita pormenores de como dados de hábitos de uso de seus usuários são coletados. [...] não aclara de quais maneiras seu sistema de recomendação algorítmica opera ou em que medida há um limite de sua operação” (ALZAMORA; SALGADO; MIRANDA, 2017, p. 50). Em outras palavras, não se observa que são esmiuçados em detalhes o modo de operação do aplicativo (ALZAMORA; SALGADO; MIRANDA, 2017, p. 50). É nesse contexto que também se verifica que o aplicativo *Netflix* não permite discussão a respeito de suas condições de uso ou mesmo de sua política de privacidade. Não se olvida que, quando o tratamento de dados pessoais for

condição para o serviço, o usuário deve ser especificamente informado dessas questões, o que não se verifica do disposto nos documentos de *Netflix*.

Entretanto, há a ressalva na própria declaração de privacidade sobre a possibilidade de retificar dados, se opor ao uso de dados, solicitar portabilidade, retirada de consentimento, informação de dados usados de forma compartilhada (cujo item remete para o tópico de divulgação de dados, já analisado), reclamação junto a Autoridade Nacional de Proteção de Dados (NETFLIX, 2020), o que não deixa de representar um ponto favorável ao usuário. Contudo, essa previsão sequer não poderia constar no documento, tendo em vista ser expresso direito do usuário assegurado em alguns incisos do artigo 18 da Lei Geral (BRASIL, 2018).

É possível exsurgir a alegação de existência do direito de confidencialidade em relação aos segredos empresariais referentes ao *software* utilizado, que também é amparado pela legislação. Contudo, os deveres de transparência, aliados às questões referentes ao consentimento devem sobressair na análise, tendo em vista a vulnerabilidade do usuário frente às possibilidades da empresa na utilização dos dados. Questões simples como informar os parceiros de onde provêm alguns dados e aclarar o uso deles não envolvem informações sigilosas da atividade empresária, constituindo direitos do usuário/assinante, especialmente frente ao papel que assume a informação adequada ao usuário.

Ainda, chama-se atenção para que, aliado ao fato do sistema algorítmico, as constantes alterações das políticas de privacidade podem tornar mais difícil o acesso do usuário para as formas com que a companhia utiliza os dados pessoais de seus clientes (ALZAMORA; SALGADO; MIRANDA, 2017, p. 56). A importância de uma necessária adequação e proteção decorre do fato de que “os assinantes, ao utilizarem o serviço que contrataram, produzem rastros digitais que são armazenados em bancos de dados e recuperados por Netflix” (ALZAMORA; SALGADO; MIRANDA, 2017, p. 49), cujos procedimentos, se não corretamente realizados, podem acarretar violações a direitos de seus usuários. Nesse contexto, é possível afirmar que

Apesar de os Termos de Uso de Netflix serem disponibilizados no site dessa companhia, não fica claro como eles são de fato utilizados por ela e até que ponto eles são disponibilizados a outras empresas e comercializados a elas. A grande questão que se coloca aos usuários e pesquisadores, portanto, é o grau de transparência no uso dos dados pessoais coletados, bem como a não negociação possível do contrato estabelecido entre a prestadora de serviços Netflix e os usuários contratantes destes. (ALZAMORA; SALGADO; MIRANDA, 2017, p. 56).

Vale destacar que a proteção de dados pessoais, frente ao crescente aumento na utilização de aplicativos lado a lado à sofisticação deles, prevista nas políticas de privacidade,

não pode constituir apenas um caráter formalizante de uma relação contratual entre usuário e empresa, mas um verdadeiro instrumento de salvaguarda de direitos (inclusive fundamentais) da pessoa. Dessa maneira, no que toca a proteção conferida pelo aplicativo *Netflix*, observa-se que, mesmo prevendo os dados que são coletados, o armazenamento, o compartilhamento, carece de maiores explicitações acerca das operações envolvendo as informações, em respeito aos ditames do consentimento e dos princípios norteadores da Lei Geral de Proteção de Dados Pessoais.

CONSIDERAÇÕES FINAIS

Com os avanços emergidos da era da sociedade em rede, surgiram inúmeras situações jurídicas novas, a ensejar o aprimoramento das legislações. Dentre essas situações, a proteção de dados pessoais se sobressai, especialmente com o crescimento da utilização de provedores de aplicação na modalidade *streaming*, destinados ao consumo de mídias na rede, com especial ênfase ao aplicativo *Netflix*. Nesse sentido, o problema de pesquisa norteou-se por investigar se é possível afirmar que o aplicativo de *streaming Netflix*, considerado provedor de aplicação e controlador de dados, adequou suas políticas de proteção de dados e respectivos termos de uso com a legislação brasileira. Para tal problemática foi aplicado o método de abordagem de dedutivo e de procedimento o estudo de caso, chegando-se a algumas conclusões que passam a ser descritas.

O primeiro tópico da pesquisa demonstrou a evolução legislativa no que se refere à regulação da internet, a exemplo do Marco Civil da Internet, além do especial destaque na proteção de dados pessoais com o advento da Lei Geral de Proteção de Dados Pessoais Brasileira. Verificou-se também que a lei brasileira, fortemente inspirada no Regulamento Geral de Proteção de Dados Europeu, recepcionou diversos institutos protetivos, como o consentimento expresso, informado e inequívoco do usuário, bem como de inúmeros princípios. Nesse sentido, abordou-se com ênfase os princípios da finalidade, adequação, necessidade e transparência do tratamento dos dados pessoais, verificando-se que são essenciais para a interpretação e análise das situações envolvendo as informações pessoais.

O segundo ponto buscou abordar a ascensão das plataformas de *streaming* diante do crescimento dos usuários que utilizam a internet para o consumo de mídias diversas. Nesse ponto, verificou-se que *Netflix* se sobressai nesse mercado, comercializando assinaturas mensais para os usuários para que possam utilizar desse tipo de serviço, permitindo a visualização de filmes, séries e diversas mídias audiovisuais. Além disso, observou-se que o

sucesso de *Netflix* se deve ao seu sofisticado sistema de recomendação, cujas bases são técnicas de *profiling*, mapeando gostos, hábitos e preferências de filmes, que fundamentam tanto as mídias que serão oferecidas, como a criação e filmagem de novas produções.

Por sua vez, o terceiro tópico estudou a declaração de privacidade e os termos de uso de *Netflix*, averiguando se são adequados à luz da legislação brasileira e dos conteúdos delineados no primeiro tópico. Desse contexto, a assinatura de *Netflix* implica a concordância com a forma com que são coletados, armazenados e utilizados os dados pessoais por parte do provedor de aplicação, não havendo margem para discussão das cláusulas. Nesse sentido, além dos dados informados pelo próprio assinante, a empresa também obtém diversas informações a partir das suas preferências e hábitos, inclusive as da região onde reside, dados obtidos com parceiros e com outras plataformas de *streaming*, *cookies*, aparelhos conectados, entre outros, podendo-se afirmar haver ampla gama de informações coletadas, inclusive que elas são de caráter sensível, permitindo um verdadeiro mapeamento do usuário.

Diante disso, observou-se que o provedor de aplicação efetivamente prevê determinadas regras no que tange à proteção de dados do usuário, especificando a forma de coleta, uso e tratamento de informações coletadas. Há que se destacar também que *Netflix* enuncia a possibilidade de solicitação dos dados pessoais da empresa, além de referir que o usuário pode contestar a forma com que ocorre o tratamento dos dados em poder da empresa, além de solicitar a sua exclusão, da qual o usuário nunca terá certeza se efetivamente foram excluídos, ferindo o princípio da transparência. Entretanto, necessário fazer a ressalva que não se observa que é possível afirmar que o usuário tenha sido amplamente informado, especialmente ante as questões envolvendo o consentimento e as bases principiológicas da legislação. Se contrastadas as disposições dos documentos com a legislação, observa-se que os dados operados excedem – e muito – aos essenciais para a execução do contrato firmado entre o usuário e a empresa. Com isso, a empresa busca obter o consentimento do assinante para a operação com demais dados pessoais e formas de tratamento não adequadamente informadas ao titular. Isso porque, pegando-se como exemplo os dados coletados com parceiros, tem-se que não se demonstra a finalidade para qual é realizada essa coleta, nem mesmo havendo informação específica sobre os parceiros, aumentando ainda mais a já existente vulnerabilidade digital do usuário frente aos provedores, se analisados diante dos princípios fundamentais da legislação.

Além disso, denota-se que carece de maior transparência acerca do modo como ocorre esse compartilhamento de dados e da inteira finalidade de sua utilização, dado que a empresa se limita a exemplificar que são utilizados para sugestão de conteúdos e

aprimoramento dos serviços prestados, buscando coletar e operar com o máximo de dados pessoais possível. Em síntese, a base de princípios que dá sustentáculo hermenêutico às regras previstas na Lei Geral de Proteção de Dados Pessoais permite afirmar a existência de deficiência nas informações prestadas por *Netflix* em sua política de privacidade e termos de uso, especialmente se tomado o usuário como a parte vulnerável da relação jurídica estabelecida, eis que excedem aos dados coletados para que o contrato firmado seja executado, além de que essas informações excedentes não são obtidas com o consentimento informado e inequívoco, destoando dos princípios norteadores da legislação, com ênfase à finalidade, transparência e adequação.

REFERÊNCIAS

ALZAMORA, Geane Carvalho; SALGADO, Tiago Barcelos Pereira; MIRANDA, Emmanuelle C. Dias. Estranhar os algoritmos: Stranger Things e os públicos de Netflix. **Revista GEMInIS**, São Carlos, UFSCar, v. 8, n. 1, p.38-59, jan./abr. 2017. Disponível em: <http://www.revistageminis.ufscar.br/index.php/geminis/article/view/280/251>. Acesso em: 05 mai. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 05 mai. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 05 mai. 2020.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 30 set. 2020.

BUCHAIN, Luiz Carlos. A Lei Geral de Proteção de Dados: noções gerais. **Revista dos Tribunais**, São Paulo, v. 1010, p. 209-229, dez. 2019.

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

CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Privado**, São Paulo, v. 98, p. 161-186, mar./abr. 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters, 2019.

DONEDA, Danilo. Reflexões sobre a proteção de dados pessoais em redes sociais. **Revista de la Red Académica Internacional de Protección de Datos Personales**. n. 1, jul./dic. 2012. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Danilo-Doneda_FINAL.pdf. Acesso em: 30 set. 2020.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Lumen Juris, 2016.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Brasileira**, Florianópolis, v. 23, n. 9, p. 284-301, fev. 2020. ISSN 2358-1352. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343>. Acesso em: 05 set. 2020.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que Regem o Tratamento de Dados no Brasil. *In*: LIMA, Cíntia Rosa Pereira de. **Comentários à lei geral de proteção de dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019, São Paulo: Thomson Almedina, 2020. p. 123-140.

JESUS, Damásio de; MILAGRE, José Antônio. **Marco Civil da Internet**: comentários à Lei n. 12.965 de 23 de abril de 2014. São Paulo: Saraiva, 2014.

LIMA, Cíntia Rosa Pereira de; RAMIRO, Livia Froner Moreno. Direitos do Titular dos Dados Pessoais. *In*: LIMA, Cíntia Rosa Pereira de. **Comentários à lei geral de proteção de dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019, São Paulo: Thomson Almedina, 2020. p. 249-277.

MARCACINI, Augusto Tavares Rosa. Regras Aplicadas ao Tratamento de Dados Pessoais. *In*: LIMA, Cíntia Rosa Pereira de. **Comentários à lei geral de proteção de dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019, São Paulo: Thomson Almedina, 2020. p. 141-161.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 106, p. 37-69, jul./ago. 2016.

MEIMARIDIS, Melina; MAZUR, Daniela; RIOS, Daniel. A Empreitada Global da Netflix: uma análise das estratégias da empresa em mercados periféricos. **Revista GEMInIS**, v. 11, n. 1, p. 4-30, 11 jun. 2020. Disponível em: <http://www.revistageminis.ufscar.br/index.php/geminis/article/view/492>. Acesso em: 15 set. 2020.

MIRANDA, Emanuelle Cristine Dias. **Dinâmicas de distribuição e circulação de séries originais Netflix**: um estudo de caso de House of Cards. 2017. Dissertação (Mestrado em Comunicação Social) – Faculdade de Filosofia e Ciências Humanas, Universidade Federal de Minas Gerais, Belo Horizonte, 2017. Disponível em:

https://repositorio.ufmg.br/bitstream/1843/30089/1/Disserta%20c3%a7%20a3o_Emanuelle%20C.%20Dias%20Miranda.pdf. Acesso em: 14 set. 2020.

MOSCHETTA, Pedro Henrique; VIEIRA, Jorge. Música na era do streaming: curadoria e descoberta musical no Spotify. **Sociologias**, Porto Alegre, v. 20, n. 49, p. 258-292, dez. 2018. Disponível em:

http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-45222018000300258&lng=en&nrm=iso. Acesso em: 06 mai. 2020.

NETFLIX. **Termos de uso**, 2019. Disponível em: <https://help.netflix.com/legal/termsfuse>. Acesso em: 15 set. 2020.

NETFLIX. **Declaração de privacidade**, 2020. Disponível em: <https://help.netflix.com/pt/legal/privacy>. Acesso em: 15 set. 2020.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters Brasil, 2019. p. 53-83.

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

RUARO, Regina Linden; GLITZ, Gabriela Pandolfo Coelho. Panorama Geral da Lei Geral de Proteção de Dados Pessoais no Brasil e a inspiração no Regulamento Geral de Proteção de Dados Pessoais europeu. **Revista de Estudos e Pesquisas Avançadas do Terceiro Setor**, Brasília, v. 6, n. 2, p. 340-356, jul./dez. 2019. Disponível em: <https://portalrevistas.ucb.br/index.php/REPATS/article/view/11545/pdf>. Acesso em: 03 set. 2020.

SARLET, Gabrielle Bezerra Sales; 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. **Civilistica.com**. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: <http://civilistica.com/o-consentimento-informado-e-a-protecao/>. Acesso em: 03 set. 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters Brasil, 2019. p. 287-322.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores *on-line* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas**

repercussões no direito brasileiro, São Paulo: Thomson Reuters Brasil, 2019. p. 601-619.

YAMAUCHI, Eduardo Akimitsu; SOUZA, Patrícia C; SILVA JUNIOR, Deógenes. Pereira. Questões Proeminentes para o Estabelecimento da Privacidade em Políticas de Privacidade de App Móveis. In: XV Simpósio sobre Fatores Humanos em Sistemas Computacionais (IHC 2016), 2016, São Paulo. **Anais do XV Simpósio sobre Fatores Humanos em Sistemas Computacionais (IHC 2016)**, 2016.