UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO
ELORA RAAD FERNANDES

A PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES NO BRASIL: um estudo de caso do *YouTube*

Juiz de Fora
2019

ELORA RAAD FERNANDES

A PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES NO BRASIL: um estudo de caso do *YouTube*

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestra no Mestrado em Direito e Inovação, sob orientação do Prof. Dr. Sergio Marcos Carvalho de Ávila Negri.

Juiz de Fora
2019

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Fernandes, Elora Raad.
A proteção de dados de crianças e adolescentes no Brasil : um estudo de caso do YouTube / Elora Raad Fernandes. -- 2019.
97 p.

Orientador: Sergio Marcos Carvalho de Ávila Negri
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2019.

1. Proteção de dados. 2. Privacidade. 3. Crianças e adolescentes. 4. YouTube. 5. Pesquisa empírica em Direito. I. Negri, Sergio Marcos Carvalho de Ávila, orient. II. Título.

FOLHA DE APROVAÇÃO

ELORA RAAD FERNANDES

A PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES NO BRASIL: um estudo de caso do *YouTube*

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestra no Mestrado em Direito e Inovação, submetida à Banca Examinadora composta pelos membros:

Orientador: Prof. Dr. Sergio Marcos Carvalho de Ávila Negri
Universidade Federal de Juiz de Fora

Prof. Dr. Sergio Vieira Branco Júnior
Grupo Ibmec

Prof. Dr. Marcos Vinício Chein Feres
Universidade Federal de Juiz de Fora

PARECER DA BANCA

( ) APROVADA

( ) REPROVADA

Juiz de Fora, 30 de novembro de 2018

AGRADECIMENTOS

Agradeço, primeiramente, a toda minha família, em especial ao meu pai, à minha mãe e à Lara, por todo o apoio e amor incondicionais, elementos imprescindíveis nesta caminhada.

Agradeço ao meu companheiro de vida, Alan, pelo carinho, pelas discussões enriquecedoras e pelos ensinamentos diários.

Agradeço ao meu orientador, Sergio Negri, por todos os aprendizados compartilhados durante minha jornada acadêmica.

Agradeço à Universidade Federal de Juiz de Fora (UFJF), à Faculdade de Direito da UFJF, ao Programa de Pós-graduação *Stricto Sensu* em Direito e Inovação da UFJF e à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Sem a existência e o apoio dessas instituições em vários momentos de minha formação acadêmica, certamente não seria possível a conclusão de mais esta etapa.

Por último, mas não menos importante, agradeço a tod@s aquel@s que passaram por meu caminho, acadêmica ou pessoalmente, e também àquel@s que não passaram, mas cujos esforços foram indispensáveis para que meus sonhos se tornassem realidade e eu me transformasse na pessoa que sou hoje.

"*Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say*".

Edward Snowden

RESUMO

As grandes mudanças na área das Tecnologias de Informação e Comunicação (TIC), principalmente através da internet, representaram um grande avanço social e possibilitaram que diversos direitos fossem concretizados. Em contrapartida, essas mesmas tecnologias apresentam diversos desafios ao Direito, especialmente no que concerne à privacidade e à proteção de dados pessoais. O novo modelo de negócios da internet, baseado na economia da atenção e financiado por publicidade utiliza dados de seus usuários para a criação de perfis individuais, que são utilizados para técnicas de *targeting* e *profiling*, bem como para a manipulação social. Isso é especialmente perigoso no que toca às crianças e aos adolescentes, pessoas vulneráveis e em desenvolvimento que, dada essa condição, são as mais afetadas por essas condutas. Com o objetivo de contribuir com essa discussão, o presente estudo busca compreender como os dados de crianças e de adolescentes têm sido tratados (coletados e processados) pelo *YouTube*. Como referencial teórico, parte-se do conceito de privacidade cunhado por Stefano Rodotà, segundo o qual, a privacidade é o direito de se manter o controle sobre suas próprias informações e de se determinar a maneira de construir sua própria esfera particular. Complementarmente, adota-se a interpretação ontológica da privacidade informacional, formulada por Luciano Floridi. Metodologicamente, utiliza-se a pesquisa empírica, baseada nas regras de inferência de Lee Epstein e Gary King, a técnica de estudo de caso, de Robert Yin, e a técnica de análise documental, a partir de André Cellard. Conclui-se a presente investigação ao se corroborar a hipótese inicial de que o *YouTube* tem tratado os dados de crianças e de adolescentes de maneira proprietária e desconsiderado a necessidade de se reforçar estruturas que permitam aos usuários moldarem suas identidades como agentes informacionais.

Palavras-chave: Proteção de dados. Privacidade. Crianças e Adolescentes. *YouTube*. Pesquisa Empírica em Direito.

ABSTRACT

The great changes in the area of Information and Communication Technologies (ICT), mainly through the internet, represented a great social advance and enabled several rights to be fulfilled. Nonetheless, these same technologies present several challenges to the Law, especially regarding privacy and the protection of personal data. The new business model of the internet, based on the economy of attention and financed by advertising, uses data from its users to create individual profiles that are used for targeting and profiling techniques as well as for social manipulation. This is especially dangerous for children and adolescents, developing and vulnerable people who, given this condition, are most affected by these behaviors. In order to contribute to this discussion, this study seeks to understand how the data of children and adolescents have been treated (collected and processed) by YouTube. As a theoretical reference, it adopts the concept of privacy coined by Stefano Rodotà, according to which, privacy is the right to maintain control over your own information and to determine the way your own particular sphere is built. Complementarily, it adopts the ontological interpretation of informational privacy, formulated by Luciano Floridi. Methodologically, the empirical research is used, based on the rules of inference developed by Lee Epstein and Gary King, as well as the Robert Yin's case study technique and the document analysis technique, from André Cellard. The investigation is concluded by corroborating the initial hypothesis that YouTube is treating data from children and adolescents in a proprietary manner and it is disregarding the need to reinforce structures that allow users to shape their identities as information agents.

Keywords: *Data protection. Privacy. Children and Adolescents. YouTube. Empirical Legal Research.*

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

APYK	Aviso de Privacidade do *YouTube Kids*
Art.	Artigo
CDC	Código de Defesa do Consumidor
COPPA	*Children's Online Privacy Protection Act*
CTS/RJ	Centro de Tecnologia e Sociedade da Faculdade de Direito da Fundação Getúlio Vargas do Rio de Janeiro
CRFB	Constituição da República Federativa do Brasil
ECA	Estatuto da Criança e do Adolescente
EULA	*End User License Agreement*
GDPR	*General Data Protection Regulation*
ICS	*Irish Computer Society*
IBM	*International Business Machines*
LGPD	Lei Geral de Proteção de Dados
MPDFT	Ministério Público do Distrito Federal e Territórios
n.º	Número
NSA	*National Secutiry Agency*
NIC.BR	Núcleo de Informação e Coordenação do Ponto BR
ODS	Objetivos de Desenvolvimento Sustentável
p.	Página
PET	*Privacy Enhancing Technologies*
PP	Política de Privacidade do *Google*
RGPD	Regulamento Geral de Proteção de Dados
TIC	Tecnologias da Informação e Comunicação
TS	Termos de Serviço
UNICEF	*United Nations Children's Fund* / Fundo das Nações Unidas para a Infância

LISTA DE SÍMBOLOS

§	Parágrafo
%	Porcentagem

SUMÁRIO

1 INTRODUÇÃO

As novas Tecnologias de Informação e Comunicação (TIC), principalmente por meio da internet, de fato, representam um grande avanço social. Seus efeitos exponenciais podem ser encontrados em todas as áreas da vida e foram capazes de mudar o que a humanidade acreditava ser possível. No ciberespaço, as pessoas podem se comunicar com mais facilidade, expressar suas opiniões em espaços políticos, compartilhar conhecimento e participar de atividades culturais e sociais. As fronteiras físicas se tornaram mais maleáveis e a relação espaço-tempo foi ressignificada, sendo hoje possível visitar outros países ou mesmo comprar produtos de outro continente sem sair de casa. As fronteiras mentais e históricas da humanidade também foram desafiadas ao se vivenciar a expansão quase infinita da memória e da capacidade de processamento da chamada inteligência artificial. Além disso, a própria noção de identidade passou a ser rediscutida, principalmente a partir da importância dos perfis digitais nas redes sociais.

Esse cenário não é diferente em relação às crianças e aos adolescentes. A internet e as TIC podem potencializar direitos, como o direito à informação, à cultura, ao lazer e a serviços que respeitem sua condição peculiar de pessoa em desenvolvimento (BRASIL, 1990a). Elas podem abrir portas para um futuro melhor e quebrar ciclos intergeracionais de privação e pobreza, oferecendo acesso à aprendizagem, a comunidades de interesse, a mercados, a serviços e a outros benefícios que ajudam a realizar o potencial existente em cada criança e adolescente (UNITED NATIONS CHILDREN'S FUND, 2018). Na medida em que se trabalha para realizar os Objetivos de Desenvolvimento Sustentável (ODS), as TIC e a internet podem ser facilitadores poderosos, ajudando a concretizar a promessa desses objetivos de não deixar ninguém para trás (UNICEF, 2017).

Entretanto, a ação de cada uma das partes interessadas, como governos, sociedade civil e academia, deve corresponder ao ritmo dessa mudança. A falta de conhecimento acerca dos perigos advindos da coleta de dados, a vigilância *online* por órgãos governamentais, o *cyberbullying* e a propaganda direcionada ao público infantil são apenas alguns dos desafios a serem enfrentados (VIOLA, 2017). Em síntese, a *Web 3.0*[1] traz consigo situações nunca antes

[1] Costuma-se dividir as gerações da internet em três, até o momento: a primeira geração é marcada pelos motores de busca simplistas e pelos *e-mails*, o que já era bastante revolucionário para a época de seu surgimento; a segunda geração é marcada pelas redes sociais e pelas compras *online*, pelas conversas em tempo real, pelo cruzamento de informações, pelas contribuições para a Wikipédia e pelos mundos virtuais (RIBEIRO, 2009). A *web 3.0*, por outro lado, é marcada pela inteligência artificial e pelos algoritmos utilizados para a personalização do conteúdo (RIBEIRO, 2009). Em síntese, "a diferença entre a *Web 2.0* e a *Web 3.0* é a diferença entre obter

experimentadas, desagradáveis ou até mesmo perigosas, que devem estar na pauta de discussão.

Especialmente no que concerne à privacidade e à proteção de dados, os dados em nossa sociedade se tornaram o novo petróleo (THE ECONOMIST, 2017) e ser pessoa passou a se confundir com ter dados. Rodotà (2004, p. 97) alerta que, "se parece reducionista e perigosa uma formulação que leve a concluir que 'nós somos os nossos dados', é porém indubitável que o nexo entre corpo, informações pessoais e controle social pode assumir contornos dramáticos". Assim, ao se transformar a informação em mercadoria, a pessoa se torna matéria prima (SCHULMAN, 2016) e perde sua condição de pessoa para a posição de consumidor, destinatário de produtos (RODOTÀ, 2007 apud SCHULMAN, 2016).

Nesse novo modelo de negócios da internet, o *Big Data* e seus "4 Vs" [2] tem se tornando alvo de extrema preocupação. Com o aumento da coleta e da capacidade de processamento de informações, garantir a segurança dos dados pessoais e proteger a privacidade dos indivíduos é uma tarefa cada vez mais difícil. As informações fornecidas a empresas a fim de se conseguir certo serviço propiciam seu uso secundário, principalmente na forma de novos produtos: os perfis de consumo individual ou familiar, análises de preferência etc., que interessam a outros parceiros comerciais (RODOTÀ, 2008). Isso é problemático mesmo em relação às informações anônimas, pois já se demonstrou que essas podem ser reidentificadas e atribuídas a indivíduos específicos (TENE; POLONETSKY, 2012). Esse uso por entes privados de quantidades enormes de informações, algo relativamente recente, gera efeitos quantitativos e qualitativos, pois estruturas de poder vinculadas a essa nova arquitetura informacional são modificadas (DONEDA, 2006).

Nesse sentido, pode-se citar o exemplo bastante atual do escândalo envolvendo a *Cambridge Analytica* e o *Facebook*, revelado pelo *The Guardian* em março de 2018. Neste caso, Wylie (o delator do caso) relata ao periódico que a empresa *Cambridge Analytica*, através de "operações psicológicas", como ele mesmo define, tinha o objetivo de moldar a opinião pública americana nas últimas eleições presidenciais dos Estados Unidos

---

uma lista de respostas e uma solução concreta e personalizada para uma pergunta. É a diferença entre a sintaxe e a semântica" (RIBEIRO, 2009, grifo nosso).

[2] Para que a formação do *Big Data* fosse possível, três fatores foram essenciais: 1) o volume, que está ligado à escala de dados produzidos hoje no mundo; 2) a velocidade com que esses dados podem ser processados pelas tecnologias atuais e 3) a variedade de dados produzidos, que, quando interligados, podem ser utilizados por algoritmos a fim de gerar perfis, por exemplo (INTERNATIONAL BUSINESS MACHINES, 2018b). Por fim, um quarto fator envolvendo o *Big Data* também deve ser considerado, qual seja, 4) a veracidade dos dados utilizados, o que pode gerar distorções no resultado final de sua análise (IBM, 2018b). Há aqueles que dizem que um quinto "V" ainda deve ser discutido, que é o valor dos dados, ou seja, diz respeito ao valor das inferências que se pode extrair de sua análise (IBM, 2018a).

(CADWALLADR; GRAHAM-HARRISON, 2018). Para tal, a empresa se associou a outra, chamada *Global Science Research*, de Aleksandr Kogan, um pesquisador do departamento de psicologia da Universidade de Cambridge. Kogan havia desenvolvido um aplicativo ("*my digital life"*) através do *Facebook* para coletar dados e traçar perfis, tanto das pessoas que o utilizavam quanto de sua rede de amigos, sendo que estes últimos não teriam fornecido consentimento para tanto. Ao desenvolver perfis tão refinados, uma vez que a quantidade de dados coletada é muito maior do que a efetivamente necessária para o funcionamento do aplicativo, seria possível enviar às pessoas propaganda política de maneira extremamente personalizada (CADWALLADR; GRAHAM-HARRISON, 2018).

Esse escândalo revela o quão frágil é a proteção de informações pessoais e a privacidade dentro do mundo digital. Isso é verdadeiro tanto em relação aos entes privados quanto aos governos, bastando recordar do caso envolvendo a *National Security Agency* (*NSA*), que controlava um programa de vigilância desenvolvido pelos Estados Unidos após o episódio do 11 de setembro de 2001, o que foi denunciado por Edward Snowden, em 2013. Outro exemplo emblemático a ser citado, que também foi colocado em voga após o escândalo da *Cambridge Analytica*, foi o referente ao aplicativo de *Facebook* chamado *Cow Clicker*, que demonstrou como os aplicativos mais simples são capazes de coletar quantidades gigantescas de dados. Nesse jogo, o único objetivo era o de clicar em uma vaca, o que poderia ser feito pelo usuário novamente apenas 6 horas mais tarde. Seu desenvolvedor, Ian Bagost, o fez com o objetivo de satirizar o vício de pessoas em aplicativos do *Facebook*, como o *Farmville*, à época (BAGOST, 2018). Mesmo após o cancelamento do aplicativo, os dados coletados das cerca de 180.000 pessoas que o utilizaram ainda estão à disposição de seu desenvolvedor, dados estes não necessariamente relacionados à função e à finalidade do aplicativo.

Assim, percebe-se, através desses episódios, que mesmo os espaços que pareciam seguros se provaram perigosos. Se em um jogo tão simples como o *Cow Clicker*, que facilmente poderia ser utilizado por crianças e adolescentes, foi possível coletar dados suficientes para a criação de perfis tão sofisticados (BAGOST, 2018), o que é capaz de fazer o *Big Data* ao longo da vida daqueles que tiveram, desde o berço, seus dados coletados?

O fato de o Direito estar sempre um passo atrás no que concerne à proteção de dados de crianças e adolescentes, atualmente, deixa livre o caminho para que direitos fundamentais sejam violados. O conhecimento a fundo de cada indivíduo, de suas preferências e de seus dados sensíveis possibilita a predição[3] e a manipulação de comportamentos (através de

[3] Nesse sentido, em um estudo realizado por Youyou, Kosinski e Stillwell (2015), verificou-se que julgamentos de personalidade feitos por inteligência artificial, a partir de *likes* do *Facebook* de voluntários, eram mais

técnicas como o *targeting* e o *profiling*), o que é bastante perigoso à democracia. Além disso, a criação de estereótipos a partir dessas informações pode engessar o desenvolvimento social (RODOTÀ, 2008). Considerando crianças e adolescentes como pessoas em desenvolvimento, há ainda o problema da bolha dos filtros presente na internet, advinda da extrema personalização do conteúdo por meio de algoritmos, que pode ter efeitos geracionais nunca antes imaginados, uma vez que nenhuma tecnologia é neutra. Nessa bolha, há cada vez menos espaço para encontros aleatórios e cada vez menos espaços de discussão através da colisão de ideias diferentes (PARISER, 2012).

Tendo em vista que o tempo passado por crianças e adolescentes na *web* apenas cresce[4] e todas as adversidades acima expostas, discutir quais dados têm sido coletados deste público e como eles têm sido processados é imperativo. O argumento de que os nativos digitais[5] compartilham em excesso sua vida e de que não se importam com a privacidade é algo comum hoje em dia, fazendo com que os esforços desses usuários em prol de sua privacidade sejam frequentemente esquecidos, legitimando tomadas de decisões de diversas redes sociais que, na verdade, as tomam em prol de seu modelo de negócios (BOYD, 2014). Boyd (2014) argumenta que principalmente os adolescentes, ao contrário de adultos mais conscientes politicamente, não estão preocupados com empresas ou com governos, mas com a vigilância de pessoas com algum grau de autoridade, como pais e professores, que usam da desculpa da segurança e da proteção para monitorarem suas vidas. Exemplo disso é o que a autora chama de "falar por códigos", isto é, adolescentes costumam utilizar uma linguagem que essas pessoas não entenderiam (BOYD, 2014). Destaca-se que, no Brasil, 67% dos adolescentes afirmaram em pesquisa saber mudar as configurações de privacidade em redes sociais (NIC.BR, 2017).

Assim sendo, crianças e adolescentes estão, sim, preocupados com sua privacidade, todavia, não têm ainda compreensão suficiente da gravidade do compartilhamento de dados, principalmente no que se refere às empresas e aos governos. Isso não quer dizer, porém, que eles não lamentem o fato de não terem escolha quando elas mesmas têm de "aceitar" termos de consentimento, o que se traduz em uma desconfiança geral das empresas que abrigam os sítios eletrônicos que visitam, como asseverado por Marx e Steeves (2010). Assim, o

---

acurados que aqueles realizados por humanos amigos ou parentes do mesmo voluntário, exceto em relação a seus cônjuges.

[4] Segundo o Núcleo de Informação e Coordenação do Ponto BR (2017), enquanto em 2012 47% dos jovens usuários de internet acessavam a rede todos os dias ou quase todos os dias, essa proporção atingiu 81% em 2014 e, em 2016, 84%. Ademais, cerca de sete em cada dez desses usuários acessam a rede todos os dias, segundo o último censo (NIC.BR, 2017).

[5] Segundo Prensky (2001), os nativos digitais são uma geração caracterizada por ter nascido imersa no desenvolvimento das novas tecnologias, sendo estas partes integrantes de sua vida.

comportamento das redes sociais em relação a esse tratamento dos dados é muito importante e não pode ser relevado, ao se terceirizar a culpa para aqueles que mais precisam de proteção jurídica.

Esse comportamento encontra tutela em contratos eletrônicos entre as empresas e seus usuários. Estes contratos são denominados, geralmente, Termos de Serviço ou Termos de Uso e são acompanhados de Políticas de Privacidade, dentre outros documentos, que detalham os pormenores dessa relação jurídica. De maneira geral, esses documentos possuem fonte pequena e conteúdo extenso, linguagem jurídica e de difícil compreensão para a maioria da população, de maneira que dificilmente serão lidos e entendidos pelos pais ou responsáveis do menor e, muito menos, por este.

Com o objetivo de contribuir com essa discussão e verificar a situação de maneira empírica, a partir de um estudo de caso, o presente trabalho busca compreender como os dados de crianças e de adolescentes têm sido tratados (coletados e processados) pelo *YouTube*. Como hipótese a esta pergunta de pesquisa, tem-se que, ao se considerar a privacidade como o direito de se manter o controle sobre suas próprias informações e de se determinar a maneira de construir sua própria esfera particular, segundo Rodotà (2008), e a interpretação ontológica da privacidade informacional, a partir de Floridi (2005, 2006, 2014), é possível afirmar que o *YouTube* tem tratado os dados de crianças e adolescentes de maneira proprietária e desconsiderado a necessidade de se reforçar estruturas que permitam aos usuários moldarem suas identidades como agentes informacionais.

Para tanto, após esta introdução, no capítulo 2 deste trabalho apresenta-se as bases teóricas assumidas nas discussões que aqui serão empreendidas. Serão discutidas, principalmente, a ampliação e releitura do Direito Civil a partir dos acontecimentos do séc. XX, o que fez com que o ordenamento jurídico se convergisse na pessoa, dando origem aos direitos de personalidade; a expansão do conceito de privacidade, a partir da contribuição de Stefano Rodotà e a interpretação ontológica e autoconstituinte de privacidade informacional de Luciano Floridi. Por fim, ao final deste capítulo, será abordada a situação legislativa atual no Brasil quanto ao tema.

O capítulo 3, por sua vez, versa sobre a metodologia utilizada para a condução desta investigação. Inicialmente, discute-se a pesquisa empírica e sua importância para balizar a subjetividade da pesquisadora e para proporcionar transparência, replicabilidade e validade nas pesquisas em Direito. Por conseguinte, explana-se o caráter empírico deste estudo e as técnicas utilizadas: o estudo de caso e a análise documental. Neste capítulo, ainda, se explicita a escolha pela rede social *YouTube*, dentre todas as outras, o procedimento de coleta de dados,

a fim de trazer replicabilidade à pesquisa e, por fim o modelo de análise criado para a análise dos documentos.

No capítulo 4 descreve-se como a coleta e o processamento de dados de crianças e de adolescentes é feito pela rede social *YouTube*. Em um primeiro momento, utiliza-se da técnica de análise de documento, a partir de Cellard (2008), para realizar uma análise preliminar dos documentos de consentimento obrigatório para uso do sítio eletrônico *YouTube* e do aplicativo *YouTube Kids*, em que são analisados diversos aspectos extrínsecos a estes. Nessa mesma fase, é feita a verificação de alguns elementos formais importantes, no que diz respeito à leitura de contratos eletrônicos na internet. Em um segundo momento, é feita uma análise de conteúdo destes documentos, a partir do modelo de análise esclarecido no capítulo 2.

O capítulo 5 desta investigação discute os resultados encontrados na pesquisa realizada e responde à pergunta de pesquisa proposta inicialmente. Neste mesmo capítulo busca-se controlar uma hipótese rival à hipótese inicial proposta neste trabalho, qual seja, a da necessidade do tratamento da privacidade como um direito de propriedade, juntamente com todas as benesses que isso traria à tutela deste direito. Ainda, após um diagnóstico da situação brasileira atual, no que se refere à privacidade e proteção de dados de crianças e adolescentes, debate-se acerca dos desdobramentos da conclusão traçada, a fim de se discutir governança para uma rede segura para essas pessoas. Por fim, no capítulo 6, conclui-se o trabalho com uma retomada de seu conteúdo e com a apresentação das considerações finais.

2 OS DIREITOS DE PERSONALIDADE E A PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL

Os acontecimentos específicos do séc. XX, apesar de não serem responsáveis pelo surgimento da ideia, aceleraram e moldaram a convergência do ordenamento jurídico na pessoa (DONEDA, 2006). Após o fim da segunda guerra, algumas tendências no Direito foram reforçadas, como a do estado social que, a partir da promoção de uma hierarquia de valores, privilegia a pessoa através de uma constituição que se torna o ponto central de todo o ordenamento (DONEDA, 2006). Além disso, o aumento da complexidade social faz com que o Código Civil não seja mais suficiente para enquadrar todas as situações demandadas pela sociedade, o que põe em xeque noções como a de sujeito de direito e a dicotomia clássica entre Direito Público e Direito Privado (DONEDA, 2006), o que traz consequências diretas aos direitos de personalidade.

O Direito Civil, que teve seu campo de atuação ampliado a partir dos valores constitucionais (TEPEDINO, 2016), passou a ser responsável pela tutela da pessoa em sentido amplo e o "instituto da personalidade era o que apresentava a mais forte vocação para se tornar o centro de irradiação, no Direito Privado, dessa nova dogmática voltada à proteção da pessoa" (DONEDA, 2006, p. 79-80). Porém, mesmo com a introdução destes direitos através da mudança de paradigmas advindas do pós-guerra, o instrumento disponível para a sua tutela continuava sendo a do direito subjetivo estruturado em torno da propriedade, herança dos códigos oitocentistas (DONEDA, 2006). Em sua conformação clássica,

> o direito subjetivo pressupõe a existência de um objeto, externo ao sujeito – assim como é o direito de propriedade, no qual os bens são separados da pessoa de seu proprietário[6]. O mesmo não ocorre com os direitos de personalidade, que recaem sobre aspectos indissociáveis de seu titular (DONEDA, 2006, p. 82).

A convergência do ordenamento na pessoa e o surgimento dos direitos de personalidade geraram, portanto, diversos questionamentos em relação ao sujeito de direito abstrato, classicamente idealizado no Direito Civil, que tinha o condão de neutralizar conflitos e, portanto, a realidade (TEPEDINO, 2016). Esse processo é chamado por Rodotà (2007 *apud*

[6] Especificamente no que concerne à privacidade, vale evidenciar que essa abordagem em termos proprietários foi se delineando também historicamente no ordenamento jurídico brasileiro: "no Brasil, a inviolabilidade do domicílio e da correspondência – nas quais se inclui o direito à privacidade – estão presentes em todas as Constituições brasileiras, desde a Constituição do Império, de 1824" (DONEDA, 2006, p. 117).

NEGRI, 2016, p. 2) de *expropriação da subjetividade*, isto é, "sob o pretexto de proteção do sujeito abstrato, usurpam-se, no plano concreto, direitos inerentes ao ser humano".

A partir dessa releitura do Direito Civil, o indivíduo, entendido como elemento neutro no Direito Civil codificado daria lugar à pessoa humana, para cuja promoção se volta a ordem jurídica como um todo. Todavia, a construção do sujeito é extremamente importante e, portanto, é necessário que ambas as construções - sujeito e pessoa - coexistam, pois o "primado da dignidade humana comporta o reconhecimento da pessoa a partir dos dados da realidade, realçando-lhe as diferenças, sempre que tal processo se revelar necessário à sua tutela integral" (TEPEDINO, 2016, p. 18). Por outra parte, a abstração do sujeito "assume grande relevância nas hipóteses em que a revelação do dado concreto possa gerar restrição à própria dignidade, ferindo a liberdade e a igualdade da pessoa" (TEPEDINO, 2016, p. 18). Em outras palavras, essa mediação deve ser levada a cabo entre a "igualdade formal do *sujeito* (libertadora de preconceitos) e a igualdade substancial da *pessoa* (protetora das vulnerabilidades)" (TEPEDINO, 2016, p. 23, grifos do autor).

Percebe-se, portanto, que a dignidade humana é a amalgama que possibilita a coexistência e a interligação entre o sujeito e a pessoa, entre o Direito Público e o Direito Privado. É nessa perspectiva, que as situações positivadas no Código Civil brasileiro sob a denominação de direitos de personalidade não devem ser lidas de maneira excludente, mas sim à luz da cláusula geral de proteção da personalidade presente na CRFB (DONEDA, 2006). A dignidade da pessoa humana como fundamento da república, se tornou, portanto, orientação axiológica constitucional e faz parte de um cenário[7] que confirma a existência, de maneira mais ampla, de uma cláusula geral de tutela e promoção da pessoa humana (TEPEDINO, 2004). É essa orientação axiológica que possibilitou uma multiplicação sem precedentes dos campos em que é realizada a tutela da dignidade humana e a privacidade pôde ser alçada a direito fundamental[8].

---

[7] Neste cenário, a dignidade humana está "associada ao objetivo fundamental de erradicação da pobreza e da marginalização, e de redução das desigualdades sociais, juntamente com a previsão do § 2º do art. 5º, no sentido da não exclusão de quaisquer direitos e garantias, mesmo que não expressos, desde que decorrentes dos princípios adotados pelo texto maior" (TEPEDINO, 2004, p. 50).

[8] Segundo Doneda (2006), o pós-guerra possibilitou o abrigo da privacidade nos ordenamentos jurídicos ao redor do mundo, sendo que a primeira menção de tutela da privacidade surgiu na Declaração Americana dos Direitos e Deveres do Homem, em 1948, vindo a aparecer logo após na Declaração Universal dos Direitos do Homem e do Cidadão e em diversas convenções que se seguiram. No Brasil, a Constituição da República Federativa do Brasil (CRFB) incluiu em seu art. 5º, X, a proteção da intimidade e da vida privada (juntamente com a honra e a imagem) (BRASIL, 1988). Doneda (2006) questiona se a utilização de dois termos pelo legislador faria com que se estivesse diante de duas hipóteses diversas que poderiam ser valoradas diferentemente. O autor responde que não, pois "(i) a ausência de uma clara determinação terminológica na doutrina e na jurisprudência, além do fato de ser a primeira vez que o tema ganha assento constitucional, podem ter sugerido ao legislador optar pelo excesso, até pelo temor de reduzir a aplicabilidade da norma; (ii) a discussão dogmática sobre os limites entre

A partir dessa conjuntura, é interessante destacar a discussão realizada por Floridi (2016) referente à relação entre dignidade humana e privacidade. Floridi defende que a proteção da privacidade deve ser dada diretamente pela dignidade humana e não indiretamente através de outros direitos. Segundo o autor, porém, a posição de cada um referente à antropologia filosófica influencia na definição adotada de dignidade humana e, consequentemente, na forma com que se baseia a privacidade (FLORIDI, 2016). As antropologias filosóficas, por sua vez, apesar de se diferenciarem significativamente entre elas, têm em comum a mesma estratégia: prover uma interpretação de dignidade humana através da defesa de algum tipo de excepcionalismo humano, isto é, de que a humanidade é essencialmente diferente das outras espécies e que merece especial consideração e respeito (FLORIDI, 2016).

Quatro são as principais teorias antropológicas filosóficas na história, segundo o autor: (i) na filosofia grega e romana, o excepcionalismo humano é baseado na habilidade natural e única do ser humano de exercer controle sobre si mesmo; (ii) na filosofia cristã, especialmente em Tomás de Aquino, o excepcionalismo humano é fundado na criação divina da humanidade, à imagem e semelhança de Deus; (iii) na filosofia moderna, especialmente depois do Iluminismo e de Kant, o excepcionalismo humano tem relação com a autonomia racional da humanidade e a habilidade de autodeterminação; (iv) na pós-modernidade, o excepcionalismo humano tem suas raízes no reconhecimento social da humanidade do valor do outro (FLORIDI, 2016).

Todas essas teorias, porém, são antropocêntricas e Floridi defende que, na verdade, seria necessária uma teoria excêntrica ("antropo-excêntrica"), que colocaria o papel especial da humanidade na periferia, significando estranho ao curso normal da natureza ao invés de superior (FLORIDI, 2016). Essa seria, portanto, uma abordagem altruísta (voltada ao paciente e não ao agente), essencial para a ética da informação. Nesse sentido, cada um dos indivíduos, como entidades cujas vidas são feitas de informação, teria a dignidade residindo em poder ser o mestre de sua própria jornada e manter suas identidades e suas escolhas abertas (FLORIDI, 2016).

---

ambos os conceitos, visto o alto grau de subjetividade que encerra, desviaria o foco do problema principal, que é a aplicação do direito fundamental da pessoa humana em questão, em sua emanação constitucional" (DONEDA, 2006, p. 110). A forma eleita pelo legislador, porém, não é das mais claras e os termos utilizados fazem menção específica a determinadas amplitudes do desenvolvimento da proteção da privacidade. Assim, aplicá-las à atual problemática dos dados pessoais poderia ser feita através de um raciocínio extensivo, de maneira que o autor prefere utilizar o termo privacidade. Vale ressaltar que, no ordenamento jurídico brasileiro atual, principalmente a partir do Marco Civil da Internet, a privacidade e a proteção de dados são tidas como princípios gerais. Estes princípios são apresentados de forma separada - art. 3º, II e III (BRASIL, 2014) - e possuem diferentes escopos, apesar de suas semelhanças (DONEDA, 2014; VIOLA, 2017).

Isso é visto mais claramente ao analisar-se uma situação em que a privacidade seja violada e, consequentemente a dignidade humana. Apenas a partir de uma filosofia da informação que enxerga a natureza humana como constituída por padrões informacionais, as violações da privacidade têm um impacto ontológico. Ao se basear o excepcionalismo em um

> caráter antropo-excêntrico do status peculiar dos seres humanos como organismos informacionais que carecem intrinsecamente de um equilíbrio permanente, mas constantemente se tornando eles mesmos, como obras informativas em andamento, então uma completa falta de privacidade é de fato desumanizadora[9] (FLORIDI, 2016, p. 5, tradução nossa).

Na sociedade hiperconectada de hoje, concluir que *nós somos os nossos dados* pode parecer reducionista e perigoso, porém é "indubitável que o nexo entre corpo, informações pessoais e controle social pode assumir contornos dramáticos, a ponto de fazer evocar imediatamente o respeito da dignidade da pessoa" (RODOTÀ, 2004, p. 6). A dignidade da pessoa deve ser interpretada, portanto, de maneira rigorosa, a partir do princípio de estrita necessidade na coleta e no tratamento de informações, isto é, de que só se pode recorrer a dados que possam identificar um sujeito quando não há outra saída (RODOTÀ, 2004).

O Direito Civil possui nas mãos, portanto, uma ótima oportunidade de se reinventar e se oxigenar a partir das novas tecnologias. Elas fizeram com que os civilistas se dessem conta de que uma nova área carente de regulação surgia e que esta afeta a vida de todos, necessitando de um outro tipo de disciplina jurídica, nunca antes pensada (RODOTÀ, 2002). Essa disciplina, porém, deve sempre ter em conta aquilo que dá razão a todo esse sistema: a pessoa humana.

2.1 Privacidade e proteção e dados pessoais

Desde a discussão histórica feita por Warren e Brandeis (1890), em que se retoma a definição de privacidade de Judge Cooley como sendo este o direito a ser deixado só (*right to be let alone*), pode-se afirmar que a privacidade sofreu um verdadeiro processo de reinvenção e, neste trabalho, será entendida como "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (RODOTÀ, 2008, p. 15).

[9] No original: "*If human exceptionalism is anthropo-eccentrically based on the peculiar status of human beings as informational organisms intrinsically lacking a permanent balance but constantly becoming themselves, like informational works in progress, then a complete lack of privacy is indeed dehumanizing*" (FLORIDI, 2016, p. 5).

Segundo Rodotà (2008), o nascimento da privacidade retrata um privilégio da burguesia, que, com a degradação da sociedade feudal e as transformações socioeconômicas advindas da revolução industrial, possuía meios econômicos de reproduzir o isolamento que, na época, era disfrutado apenas por monges, místicos etc. Assim, o nascimento da privacidade não surge de uma demanda natural de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo, o que o imbui de um caráter individualista e faz com que ele seja tutelado como um direito burguês por excelência: a propriedade (RODOTÀ, 2008). É esta noção de privacidade que se argui quando se resiste a ceder à autoridade pública informações relevantes à elaboração de programas sociais, caso em que, por trás da defesa da privacidade, se encontra uma "hostilidade em relação a uma pressão fiscal mais acentuada e a uma política de diminuição da diferença social" (RODOTÀ, 2008, p. 29).

Outro significado adquire, porém, a reação contra a coleta de informações relacionadas ao controle do comportamento político, o que caracteriza uma defesa mais progressista da privacidade e é utilizada para reagir contra autoritarismos e discriminações (RODOTÀ, 2008). A mudança na tendência burguesa do tratamento da privacidade se deu, principalmente, a partir da década de 1960, com a contribuição de várias frentes como o desenvolvimento do *welfare state*, a mudança de relacionamento entre o cidadão e o Estado, a importância dos movimentos sociais e a maior demanda por informações advinda das novas tecnologias (DONEDA, 2006). As informações individuais das massas passaram, portanto, a adquirir importância. A partir dessa diferenciação de significados das demandas por privacidade, Rodotà (2008) defende a garantia máxima de opacidade em relação a informações suscetíveis de gerar práticas discriminatórias (dados sensíveis)[10] e a máxima transparência em relação às informações relativas à esfera econômica dos sujeitos.

Segundo Doneda (2006), inicialmente, dois fatores são utilizados para justificar o uso de informações pessoais: o controle e a eficiência. Inicialmente, o Estado teria sido o grande utilizador dos dados pessoais, como afirmado acima por Rodotà, a fim de conhecer a população e desenvolver programas sociais (e isso ocorreu tanto em relação ao desenvolvimento do *welfare state* quanto de autoritarismos, já que ambos necessitam de informações para a implementação de seus programas). Todavia, as novas tecnologias propiciam um meio acessível de coleta e processamento de informações, tornando possível o

[10] Segundo a clássica definição de Bodin de Moraes (2008, p. 371), "dados sensíveis são os dados pessoais que dizem respeito à saúde, opiniões políticas ou religiosas, hábitos sexuais etc. aptos a gerar situações de discriminação e desigualdade". Na Lei Geral de Proteção de Dados (LGPD), que entrará em vigor em fevereiro de 2020, dado sensível é todo "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).

uso das informações por entes privados. Essa mudança, inicialmente quantitativa, gera efeitos qualitativos, pois mudam as estruturas de poder que estão vinculadas a essa nova arquitetura informacional (DONEDA, 2006).

A quantidade e a qualidade das informações fornecidas a empresas a fim de conseguir certo serviço propiciam seu uso secundário, principalmente na forma de novos produtos: os perfis de consumo individual ou familiar, análises de preferência etc. que interessam a outros parceiros comerciais (RODOTÀ, 2008). A informação é, portanto, uma mercadoria e, uma vez que as regras de circulação de informações criadas a partir disso são destinadas a incidir sobre a distribuição de poder na sociedade, é especialmente importante que isso seja tratado no âmbito coletivo (RODOTÀ, 2008).

Para que isso ocorra, portanto, é necessário lidar com a privacidade através do controle e não do sigilo, pois, dessa maneira, é possível conjugá-la com a publicidade das informações (RODOTÀ, 2008). De fato, não é mais possível enxergar pessoas como meras fornecedoras de dados pessoais para que sejam beneficiadas com serviços, vez que o acúmulo de informações, como já mencionado, cria bolhas de poder e, diante disso, os cidadãos devem ter o direito de pretender exercer um controle sobre os sujeitos detentores desses bancos de dados (RODOTÀ, 2008). A privacidade, portanto, não se estrutura mais em torno do eixo "pessoa-informação-sigilo", mas sim do eixo "pessoa-informação-circulação-controle" (RODOTÀ, 2008, p. 93).

A mudança no cenário tecnológico, que, principalmente no séc. XIX, era vista como progresso (DONEDA, 2006) e, nos dias de hoje, como instigadora de distopias, gera, portanto, um desafio para a seara jurídica. Apesar disso, o Direito também sofre mudanças: passada a discussão, da qual o cerne era a privacidade, passa-se a uma noção mais completa de proteção de dados, "a qual extrapola os problemas ligados à tutela da intimidade individual" [11] (RODOTÀ, 2008, p. 44). Nesse seguimento, a privacidade vai ao encontro da própria evolução da teoria dos direitos de personalidade e se expande para um "elemento que, antes de garantir o isolamento ou a tranquilidade, proporcione ao indivíduo os meios

[11] Floridi (2014), cuja teoria será abordada na próxima seção, aborda a proteção de dados como parte do que ele denomina de privacidade informacional, ou seja, a liberdade contra interferência informacional, alcançada através de uma restrição sobre fatos sobre ela que são desconhecidos ou incognoscíveis. Nesta perspectiva, a definição de privacidade para Floridi vai ao encontro da definição de privacidade por Rodotà: "privacidade é o direito dos indivíduos (sejam esses pessoas individuais, grupos ou instituições) de controlar o ciclo de vida (especialmente a geração, acesso, registro e uso) de suas informações e determinar quando, como e até que ponto suas informações são processadas por outras" (FLORIDI, 2014, p. 151, tradução nossa). No original: "*privacy is the right of individuals (be these single persons, groups, or institutions) to control the life cycle (especially the generation, access, recording, and usage) of their information and determine when, how, and to what extent their information is processed by others*" (FLORIDI, 2014, p. 151)

necessários para a construção e consolidação de uma esfera privada própria" (DONEDA, 2006, p. 23-24).

Isso é especialmente importante no que diz respeito à construção de uma sociedade democrática, principalmente no que tange à projeção do discurso da privacidade e, consequentemente, do acesso à informação, à coletividade. O direito a ter divulgadas determinadas informações amplia-se rumo a um "direito à democracia", o que identifica o caráter democrático de um sistema com a quota de informações relevantes que circulam em seu interior (RODOTÀ, 2008). A transparência, portanto, é verdadeira premissa para a presença e para a participação efetiva dos cidadãos no interior das organizações sociais e políticas, pois as regras de circulação de informações dentro de uma sociedade impactam diretamente na distribuição de poder nela presente.

2.2 A interpretação ontológica de privacidade informacional

Após a definição de privacidade por Rodotà e de sua evolução dentro dos direitos de personalidade, a partir da proteção de dados, importante se faz discutir como as TIC influenciam na abordagem da privacidade atual, o que será essencial para a discussão da relação entre as redes sociais e a privacidade infantil. Nesse sentido, Floridi (2005, 2006, 2014) realiza uma discussão muito relevante acerca de como a privacidade é construída a partir da arquitetura informacional e de como as TIC podem ser utilizadas para *reontologizar* a infosfera e proteger seus agentes.

Primeiramente, faz-se necessário discutir por que as TIC tornaram o assunto da privacidade um dos mais debatidos dentro da ética da computação. Segundo Floridi (2005), uma das explicações mais aceitas é a de que isso ocorreu devido ao aumento das capacidades de processamento (*processing*), à velocidade com que esses dados podem ser por elas processados (*pace*) e à quantidade e qualidade (*quantity and quality*) de dados que elas podem coletar, armazenar e administrar, teoria esta que pode ser denominada de hipótese 2P2Q.

Segundo o autor, o problema desta hipótese é que ela se concentra apenas nos efeitos óbvios e secundários da evolução digital, a partir de uma perspectiva continuísta, o que será mais bem explicado abaixo. Ela não considera que as TIC também podem ser responsáveis por um aumento da privacidade de seus usuários e, principalmente, por uma mudança radical em sua natureza geral, de modo que elas estariam mais redesenhando do que apagando os limites da privacidade informacional. Os desafios relacionados a essas tecnologias têm suas bases, portanto, em uma transformação radical e sem precedentes na própria natureza

(ontologia) do ambiente informacional, dos agentes informacionais embutidos nele e de suas interações (FLORIDI, 2005).

Para resolver essa problemática, o autor propõe uma interpretação ontológica da privacidade informacional. Para que esse conceito seja bem elucidado, necessário se faz um experimento mental: imagine um modelo de uma região limitada da infosfera[12], representado por pacientes (no caso, os agentes informativos interativos), que se encontram em um mesmo hospital (no caso, o ambiente limitado). Isto posto, dada certa quantidade de informações disponíveis, quanto maior a lacuna informacional entre os pacientes, menos eles se conhecem e mais privadas podem ser suas vidas (FLORIDI, 2006). A lacuna de informação depende, portanto, do grau de acessibilidade dos dados pessoais de cada agente.

A acessibilidade, por seu turno, é um fator epistêmico e dependerá das características ontológicas da infosfera, isto é, da natureza dos agentes específicos (se são surdos, por exemplo), do ambiente em que estão inseridos (se estão no mesmo quarto, se compartilham banheiro etc.) e das interações específicas implementáveis naquele ambiente por esses agentes. Essas características do ambiente fazem parte de um atrito ontológico, que determina o fluxo de informação dentro deste sistema (ex.: paredes de tijolos proporcionam um atrito ontológico muito maior para o fluxo de informações acústicas do que uma partição fina como papel) (FLORIDI, 2006). Sintetizando, a privacidade informacional é uma função da fricção ontológica da infosfera.

Dentro dessa nova interpretação, as TIC são um dos fatores que mais afetam o atrito ontológico da infosfera[13]. As TIC pré-digitais sempre tenderam a reduzir a fricção ontológica e, consequentemente, a privacidade informacional na infosfera, porque "aprimoram" ou "aumentam" os agentes incorporados nela. Um aspirador de pó, um telefone ou um rádio, por exemplo, aprimoram seus usuários assim como um membro artificial. Outros aparelhos, porém, como a máquina de lavar roupa ou a geladeira, assim como as tecnologias capazes de gravar dados (do alfabeto a um gravador de vídeo) são, na verdade, robôs que aumentam seus usuários, na medida em que tarefas bem especificadas podem ser delegadas a eles (FLORIDI, 2005).

---

[12] Segundo Floridi (2008 apud MCBURNEY, 2008), o termo infosfera pode ter dois significados: um deles é estático e significa a totalidade de agentes, objetivos, serviços, relações, processos e espaço informacionais, a partir dos quais se interage no mundo. É um conceito mais amplo que o ciberespaço, mas apenas por incluir domínios analógicos e *offline* como livros, listas de compras etc. (FLORIDI, 2008 apud MCBURNEY, 2008). O segundo significado seria a infosfera como sinônimo de toda a realidade, sendo essa uma forma de se referir ao que existe, ao adotar-se uma perspectiva informacional. Isso significa equacionar a infosfera com o que os filósofos chamam de Ser (FLORIDI, 2008 apud MCBURNEY, 2008).

[13] Outro fator, por exemplo, está ligado ao desenvolvimento social, como a mudança massiva de pessoas da área rural para a urbana e seu correspondente fenômeno do anonimato (FLORIDI, 2006, p. 111).

As TIC digitais, por sua vez, são diferentes porque, sendo interativas, elas também podem aumentar a privacidade informacional ou até mesmo alterar o que se entende como privacidade informacional na medida em que *reontologizam* a própria natureza da infosfera. Isso ocorre porque elas projetam novos ambientes em que os usuários podem habitar. De acordo com uma interpretação "continuísta", as TIC digitais devem ser tratadas como apenas mais uma instância de TIC, que aprimoram ou aumentam seus agentes, causando problemas crescentes de privacidade informacional simplesmente porque são ordens de grandeza mais poderosas do que as tecnologias passadas. Todas as TIC anteriores tendem a reduzir a fricção ontológica na infosfera e as TIC digitais não são exceção, demonstrando a correção da explicação 2P2Q. Todavia, a essência do problema é negligenciada, pois, enquanto as TIC pré-digitais tendem a aprimorar ou aumentar os agentes envolvidos mais e mais, as TIC digitais também pode alterar a própria natureza da infosfera (isto é, do próprio ambiente, dos agentes embutidos nele e de suas interações). A explicação do 2P2Q perde uma diferença fundamental entre as velhas e as novas TIC: as primeiras estão aprimorando ou aumentando os agentes, enquanto as últimas são mais bem compreendidas como tecnologias reontologizadoras (FLORIDI, 2005).

Para deixar mais claro, o autor fornece o seguinte exemplo: imagine que todas as paredes e os móveis da ala do hospital mencionado anteriormente sejam transformados em vidro perfeitamente transparente. Assumindo que nossos pacientes tenham boa visão, isso reduzirá drasticamente o atrito ontológico no sistema. Imagine, depois, que os pacientes são transformados em leitores de mentes proficientes e telepatas. Qualquer privacidade informativa neste tipo se tornará praticamente impossível, pois modificações radicais na própria natureza da infosfera podem mudar drasticamente as condições de possibilidade de privacidade informacional (FLORIDI, 2005, 2006).

A partir dessas considerações, Floridi (2005, 2006) defende que, da mesma maneira em que a revolução digital é mais bem entendida como uma reontologização fundamental da infoesfera, a privacidade informacional requer uma reinterpretação igualmente radical, que leve em conta a natureza essencialmente informacional dos seres humanos e de suas operações como agentes sociais. Essa reinterpretação é obtida considerando cada indivíduo como constituído por suas informações e, portanto, entendendo uma violação da privacidade informacional como uma forma de agressão à sua identidade pessoal. Isso é o que o autor chama de interpretação autoconstituinte de privacidade:

> a interpretação autoconstituinte enfatiza que a privacidade é também uma questão de construção da própria identidade. O direito a ser deixado só também é o direito de ter permissão para experimentar em sua própria vida, para começar de novo, sem ter registros que mumificam sua identidade pessoal para sempre, tirando de você o poder de formar e moldar quem você é e quem você pode ser. Todos os dias, uma pessoa pode querer construir um "eu" diferente, possivelmente melhor. Nós nunca paramos de nos tornarmos nós mesmos, então proteger a privacidade de uma pessoa também significa permitir que essa pessoa tenha liberdade para construir e mudar profundamente. O direito à privacidade é também o direito a uma identidade renovável[14] (FLORIDI, 2014, p. 162, tradução nossa).

Isso vai ao encontro da definição de privacidade e de seus efeitos no Direito discutidas por Rodotà, e reafirma a condição da privacidade como direito fundamental. Deste modo, crianças e adolescentes devem ter sua privacidade e seus dados protegidos de maneira prioritária, pois as TIC são capazes de remodelar o próprio *self* (FLORIDI, 2014).

Essa interpretação é consistente com o fato de que as TIC digitais podem tanto erodir quanto reforçar a privacidade informacional, e, portanto, um esforço positivo precisa ser feito para apoiar não apenas o que o autor chama de *PET* (*Privacy Enhancing Technologies*), mas também as aplicações poiéticas (ou seja, estruturantes), que podem permitir aos usuários projetar, moldar e manter suas identidades como agentes informacionais. Isso não quer dizer que essas tecnologias serão a solução para os problemas de privacidade de nossa época, mas sim que "as TIC digitais já fornecem meios de contrabalancear os riscos e desafios que elas representam para a privacidade" [15] (FLORIDI, 2014, p. 151, tradução nossa).

O fluxo de informações requer algum atrito para manter firme a distinção entre o sistema macro multiagente (a sociedade) e a identidade dos agentes (os indivíduos) que a constituem. Qualquer sociedade, em que nenhuma privacidade informativa é possível, é aquela em que nenhuma identidade pessoal pode ser mantida (FLORIDI, 2005, 2006).

2.3 A proteção de dados de crianças e adolescentes no Brasil

Após uma análise teórica sobre a privacidade e a proteção de dados, vale discutir como é a situação legislativa atual quanto ao tema, ou seja, como o Direito positivo tem

---

[14] No original: "*the self-constituting interpretation stresses that privacy is also a matter of construction of one's own identity. Your right to be left alone is also your right to be allowed to experiment with your own life, to start again, without having records that mummify your personal identity for ever, taking away from you the power to form and mould who you are and can be. Every day, a person may wish to build a different, possibly better, 'I'. We never stop becoming ourselves, so protecting a person's privacy also means allowing that person the freedom to construct and change herself profoundly. The right to privacy is also the right to a renewable identity"* (FLORIDI, 2014, p. 162).

[15] No original: "*digital ICTs are already providing some means to counterbalance the risks and challenges that they represent for privacy*" (FLORIDI, 2014, p. 151).

lidado com esses novos desafios. A primeira regulamentação a ser mencionada é o Marco Civil da Internet. Este foi construído sob três pilares que, além da liberdade de expressão e da neutralidade, inclui a privacidade (SOUZA; LEMOS, 2016), que está inserida como princípio em seu art. 3º, II (BRASIL, 2014). Sendo assim, como à época não existia uma lei geral de proteção de dados vigente, alguns dispositivos inseridos no Marco Civil da Internet inauguraram o tratamento da tutela de dados no Brasil. Ele surge em um contexto em que se contava apenas com dispositivos ora muito genéricos, como o art. 21, do Código Civil – que traz a vida privada como um direito de personalidade (BRASIL, 2002) – e dispositivos ora muito setoriais, como o art. 43, do Código de Defesa do Consumidor (CDC) (BRASIL, 1990b) – que diz respeito ao acesso e retificação de informações em banco de dados de consumidores (SOUZA; LEMOS, 2016). Além desses, os dispositivos constitucionais - como o art. 5º, X, XI, XII e LXXII, que definem os contornos da privacidade como direito fundamental e trazem o *Habeas Data* como remédio constitucional (BRASIL, 1988).

O Marco Civil da Internet trouxe uma abordagem ampla que contempla a privacidade e a proteção de dados como princípios gerais e estes são apresentados de forma separada - art. 3º, II e III (BRASIL, 2014) - o que evidencia a diferença de escopo entre esses dois conceitos (DONEDA, 2014; VIOLA, 2017). Em relação à proteção de dados, a normativa traz no art. 3º, III, a necessidade de seu cumprimento nos termos da lei (BRASIL, 2014), o que deveria ser definido por uma lei geral de proteção de dados.

Embora de grande importância, por ampliar a proteção da privacidade e da proteção de dados no país, o Marco Civil da Internet não é suficiente para a proteção desses direitos de forma integral, de modo que uma lei geral de proteção dados era necessária. Exemplo disso é a falta de uma definição de dados sensíveis[16], a sua aplicação apenas na coleta e no processamento de dados na internet e a falta da definição de uma autoridade autônoma competente para a fiscalização da aplicação das regras sobre privacidade. Ressalta-se, ainda, que o Marco Civil da Internet, assim como o decreto que o regulamenta, não faz especificações acerca da coleta e do processamento de dados de crianças e de adolescentes.

É a partir desta insuficiência que a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), após seis anos de tramitação no Congresso e duas consultas públicas, surge. Ela é extremamente importante dentro da sociedade hiperconectada em que se vive e tem a função de unificar regras no Brasil sobre a proteção de dados, estabelecer regras claras para a coleta e

[16] O Decreto n.º 8.771/2016, que regulamenta o Marco Civil da Internet, traz apenas a definição do que são os dados pessoais: "Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016).

o tratamento destes e promover o desenvolvimento econômico e tecnológico no país. Sua aplicação é feita de maneira transversal e multissetorial, sendo utilizada no âmbito público e no privado, estando os dados presentes de forma *online* ou *offline*. A lei se baseia em 10 princípios a serem levados em consideração na coleta e processamento de dados pessoais, como o princípio da transparência, da necessidade, da finalidade e da não discriminação (BRASIL, 2018).

A lei possui, ainda, uma seção dedicada especificamente à proteção de dados de crianças e adolescentes (seção III). Dessa seção, podem-se tirar três questões principais. Primeiramente, em relação ao uso de dados de crianças[17], é necessário consentimento específico de um dos pais ou do responsável legal e o desenvolvedor deve realizar todos os esforços para que se verifique se esse consentimento foi realmente fornecido - §1º e §5º (BRASIL, 2018). Em segundo lugar, deve-se destacar o principio da minimização[18] da coleta de dados em jogos, aplicações de internet ou outras atividades voltadas a esse público - §4º (BRASIL, 2018). Por fim, a lei obriga a oferta de informações, de maneira acessível e adequada, acerca da coleta e do tratamento de dados de crianças e de adolescentes - §6º (BRASIL, 2018). Sua *vacatio legis* será de 18 meses, a fim de que o setor privado e o governamental se adaptem às novas regras.

Ainda acerca das regulações vigentes, no dia 25 de maio de 2018 o Regulamento Geral sobre a Proteção de Dados (RGPD ou *General Data Protection Regulation – GDPR*, em inglês) da União Europeia entrou em vigor. Este regulamento busca harmonizar as regras de proteção de dados de seus Estados membros e aumentar os níveis de privacidade de seus cidadãos (VOIGT, BUSSCHE, 2017) e é considerado, hoje, um dos padrões mais altos de proteção de dados no mundo, tendo inspirado em muitos âmbitos, inclusive, o projeto da LGPD. Devido a seu escopo transnacional de aplicação[19], esse regulamento afetou, também,

[17] Apesar de o caput do art. 14 da LGPD dizer respeito a crianças e a adolescentes, os parágrafos deste artigo dizem respeito apenas às crianças e o ECA definiu como criança toda pessoa de até 12 anos incompletos (BRASIL, 1990a). Dessa forma, a idade de consentimento no Brasil nestes casos foi definida como 12 anos (BRASIL, 2018).

[18] "O princípio da minimização prevê que os dados pessoais devem ser adequados, pertinentes e limitados em relação aos fins para os quais serão processados. O objetivo é diminuir a quantidade de dados, coletando apenas aqueles que sejam essenciais para o produto ou serviço ofertado" (MANGETH; NUNES; MAGRANI, 2018).

[19] O RGPD é aplicável ao tratamento de informações pessoais "realizado 'no contexto das atividades de um estabelecimento' de responsável pelo tratamento ou por operador situado no território europeu, ainda que o tratamento ocorra fora dos limites territoriais da União Europeia. Para a compreensão do critério eleito pelo legislador europeu, é importante destacar que a noção de estabelecimento foi delineada principalmente a partir da jurisprudência da Corte de Justiça da União Europeia , em sua função de interpretação da Diretiva 95/46/CE, que também se fundava no alargamento do âmbito territorial de aplicação" (POLIDO et al., 2018, p. 14). No caso analisado, a Corte esclareceu que o conceito de estabelecimento se "estende a toda atividade real e efetiva — ainda que mínima — exercida mediante uma instalação estável" (UNIÃO EUROPEIA, 2015 apud POLIDO et al., 2018, p. 14). "Construiu-se aí uma concepção flexível — não formalista — do conceito, válida

diversas sociedades empresárias localizadas fora da União Europeia (VOIGT, BUSSCHE, 2017). Assim, apesar de a LGPD ainda estar em *vacatio legis*, o RGPD se aplica ao *YouTube*, caso analisado neste trabalho, uma vez que este fornece serviços no território europeu[20].

Em relação à proteção de dados de crianças e adolescentes, ao contrário dos Estados Unidos, que possuem uma lei específica para regulamentar seus interesses (o *Children's Online Privacy Protection Act – COPPA*, de 1998), a União Europeia decidiu tratar da questão indicando no RGPD disposições de garantias diferenciadas a este público, dentro de uma regulação geral de proteção de dados.

A partir da leitura da consideração n.º (38) do RGPD, tem-se que "crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais" (UNIÃO EUROPEIA, 2016b). Isso é reforçado nos casos em que os dados de crianças são utilizados para fins de "comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças" (UNIÃO EUROPEIA, 2016b). Assim sendo, a partir do princípio da transparência, consolidado no art. 5º, 1, a, sempre que o tratamento for dirigido às crianças a linguagem deve ser clara e simples, para que seja compreendida facilmente (UNIÃO EUROPEIA, 2016b).

Em relação ao consentimento, o RGPD estabelece a idade mínima de 16 anos[21]. Para os menores de 16 anos, em regra, será necessário o consentimento dos pais ou responsáveis de maneira explícita para a coleta e processamento de seus dados pessoais. Outra questão de destaque, no RGPD, diz respeito à tutela especial quanto ao direito de apagamento de dados, cujo consentimento de coleta foi dado quando o titular ainda era criança. O usuário deve poder exercer este direito mesmo já sendo adulto, o que se encontra presente na consideração n.º (65) e no art. 17, 1, f (UNIÃO EUROPEIA, 2016b).

Diante dessa nova onda legislativa importante em relação à proteção da privacidade e dos dados pessoais, os documentos coletados por este trabalho serão analisados, também, com base em seus princípios e regras, a fim de verificar a aplicação do Direito positivo em seu contexto social.

'especialmente para as empresas que se dedicam a oferecer serviços exclusivamente pela Internet'" (UNIAO EUROPEIA, 2015 apud POLIDO et al., 2018, p. 14).

[20] Nesse sentido, destaca-se que a *Google* atualizou sua política de privacidade no Brasil, no dia 25 de maio de 2018, dia em que o RGPD entrou em vigor.

[21] Destaca-se, porém, que o RGPD autoriza que as legislações específicas de cada Estado membro estabeleçam uma idade menor que 16 anos para o consentimento, mas que não seja abaixo de 13 anos. Assim, as condições para o consentimento de adolescentes entre 13 e 16 anos devem variar nos países da União Europeia (VOIGT, BUSSCHE, 2017).

3 METODOLOGIA

O isolamento do Direito em relação às outras disciplinas das ciências sociais, além da confusão da prática profissional com a pesquisa acadêmica fez com que a pesquisa jurídica no Brasil se desenvolvesse de maneira bastante prejudicada (NOBRE, 2002). Westerman (2011) discute a questão, que parece ter uma escala global no Direito, apontando o problema do terceiro ausente. O terceiro ausente seria uma perspectiva teórica independente, que possibilita a pesquisadora a acessar o escopo e a natureza tanto daquilo que se pretende estudar quanto da ordem normativa existente (WESTERMAN, 2011).

Isso ocorre, pois, nesta área, os pesquisadores tendem a saber exatamente o que pesquisar, mas não como. Assim, busca-se encaixar a novidade a ser estudada (o que pode ser uma nova interpretação da doutrina, uma nova jurisprudência, uma legislação etc.) com o sistema jurídico, de maneira que os conceitos jurídicos passam a desenvolver um papel duplo: fazem parte do sistema legal e do referencial teórico (WESTERMAN, 2011).

Em relação à confusão entre a prática profissional e a pesquisa jurídica, percebe-se, no Direito, uma inclinação em se utilizar técnicas da primeira no desenvolvimento da última, o que torna a pesquisa jurídica parecida com um parecer. Ao realizar-se um parecer, recolhe-se material da doutrina e da jurisprudência, além dos títulos legais, em função da tese a ser defendida, isto é, não se realiza a coleta de todo o material disponível ou de uma amostra confiável deste, mas apenas daquela parte que condiz com tal tese (NOBRE, 2002). Assim, a resposta se desenvolve anteriormente à investigação e não o contrário. Essa forma padrão de argumentação contamina de maneira preocupante a pesquisa jurídica brasileira e é necessário romper com ela a fim de elevar o padrão científico do país (NOBRE, 2002).

Considerando as questões apontadas acima, o desenvolvimento de uma metodologia consistente dentro dos trabalhos acadêmicos brasileiros em Direito se mostra imperativo. Ela é essencial não só para trazer transparência e replicabilidade ao trabalho, mas também para balizar os efeitos da subjetividade que, já se sabe, é inerente a qualquer pesquisa, seja ela quantitativa ou qualitativa, teórica ou empírica. Nesta seção, busca-se, por conseguinte, explanar o caráter empírico do presente trabalho, esmiuçar as técnicas empíricas utilizadas e expor os procedimentos de coleta de dados, assim como o método de análise dos dados.

3.1 A pesquisa empírica em Direito

O Direito como objeto de pesquisa empírica no Brasil é algo recente e pouco consolidado dentro das universidades (IGREJA, 2017). Sua imersão dentro de um contexto social e sua necessidade de aplicação, porém, fazem com que essa prática seja imperiosa, a fim de compreender a relação de forças que o constituem (IGREJA, 2017). Segundo Veronese (2013), o problema estaria ligado, principalmente, aos programas de pós-graduação no Brasil, nos quais a formação tradicional não qualifica o bacharel para que dialogue com outras áreas, sendo este um problema majoritariamente institucional. Essa interdisciplinaridade seria fundamental para integrar a teorização do Direito com as práticas de pesquisa.

A fim de identificar o que é uma pesquisa empírica e seu local de importância dentro da pesquisa em Direito, Veronese (2013) faz uma análise de quatro momentos das relações sociais, aos quais a pesquisa jurídica estaria relacionada. Primeiramente, haveria um debate acerca dos pressupostos da noção de normatividade, em que se busca apreender o "significado intrínseco da validade do direito e seu conceito abstrato em relação à vida social" (VERONESE, 2013, p. 204), ou seja, analisa seus pressupostos epistemológicos.

O segundo momento está ligado à determinação da organização normativa, localmente compreendida e, para isso, é necessário retirar do primeiro momento um pressuposto importante, qual seja, o que é considerado como norma jurídica a fim de se definir "quais são as normas jurídicas vigentes em um espaço e tempo específicos" (VERONESE, 2013, p. 206). A pesquisa empírica é extremamente importante para essa compreensão, pois não é possível entender o sistema jurídico sem considerar como a sociedade o interpreta cotidianamente. Percebe-se, porém, uma baixa utilização da concepção empírica nessa fase (VERONESE, 2013).

Um terceiro momento estaria ligado à interpretação do Direito, ou seja, seria a possibilidade de construção ou análise das teorizações realizadas no primeiro momento, sendo este mais próximo da hermenêutica (VERONESE, 2013). Por fim, o quarto momento está relacionado à análise social e/ou econômica do Direito, isto é, como a normatividade é aplicada socialmente. É neste momento que se encontra grande parte da pesquisa empírica, em que se busca responder como e por que a normatividade é interpretada de certa forma, além das consequências sociais e econômicas dessas interpretações (VERONESE, 2013).

A presente pesquisa está relacionada, portanto, ao quarto momento das relações sociais descritas pelo autor. Nela analisa-se como o *YouTube* tem coletado e processado dados de crianças e adolescentes no Brasil, levando-se em consideração toda a base normativa que diz respeito à proteção de dados no país. Assim, busca-se verificar, empiricamente, como o

Direito tem sido aplicado e interpretado na realidade, assim como as suas consequências sociais e econômicas no que diz respeito a crianças e adolescentes.

Uma vez justificada a necessidade da pesquisa empírica para responder à pergunta de pesquisa e considerando o potencial do estudo jurídico de influenciar políticas públicas (EPSTEIN; KING, 2013), importa destacar que a presente pesquisa seguirá as regras de inferência propostas por Epstein King (2013), com o objetivo de trazer maior confiabilidade e validade às conclusões aqui traçadas.

Segundo os autores, o que torna uma pesquisa empírica é seu embasamento em observações sobre o mundo, que servirão como dados para realizar inferências (EPSTEIN; KING, 2013). Dessa forma, mais do que um resumo dos dados coletados, utilizado para traduzir ou sintetizar informações a fim de que os pesquisares possam dar sentido a elas, as inferências são o "processo de utilizar os fatos que conhecemos para aprender sobre os fatos que desconhecemos" (EPSTEIN; KING, 2013, p. 36). Essas inferências podem ser caracterizadas como descritivas ou causais e, nesta investigação, trabalha-se com a primeira.

Para fundamentar as regras de inferência em uma pesquisa empírica, segundo Epstein e King (2013), três diretrizes gerais devem ser observadas. A primeira delas é que uma pesquisa deve ser replicável, isto é, outra pesquisadora ou pesquisador deve poder entender, avaliar, basear-se em e reproduzir a pesquisa realizada, sem que lhe sejam fornecidas quaisquer outras informações além do que foi exposto metodologicamente (EPSTEIN; KING, 2013). O propósito do padrão de replicação é "garantir que um trabalho publicado seja auto-suficiente" e mantenha "o inquérito empírico acima do nível dos ataques *ad hominem* à aceitação incondicional dos argumentos de autoridade" (EPSTEIN; KING, 2013, p. 53). A transparência sobre os procedimentos realizados na pesquisa é, portanto, fundamental, pois cada escolha realizada pela pesquisadora pode influenciar diretamente os resultados.

A segunda diretriz geral diz respeito ao fato de que a pesquisa é um empreendimento social. A razão por trás do agrupamento de acadêmicos em universidades está totalmente relacionada a esta diretriz, uma vez que o avanço do conhecimento depende da cooperação de uma comunidade de acadêmicos trabalhando juntos para aprender mais sobre o mundo (EPSTEIN; KING, 2013). Ao reconhecer a importância da colaboração e da contribuição à literatura acadêmica para a pesquisa, esforços serão poupados e será possível verdadeiramente solucionar problemas do mundo real.

Por fim, a terceira diretriz está relacionada ao fato de que todo conhecimento e toda inferência na pesquisa são incertos, afinal, "os fatos que conhecemos relacionam-se aos fatos que não conhecemos, mas gostaríamos de conhecer, somente por suposições que jamais

poderemos verificar completamente" (EPSTEIN; KING, 2013, p. 63). Assim, é necessário estimar o grau de incerteza junto a cada conclusão e estimar, dentro do possível, todos os limites inerentes à pesquisa.

Vale ressaltar, ainda, que, além de empírico, este trabalho também é caracterizado como predominantemente qualitativo. As evidências utilizadas como dados conhecidos podem ser numéricas (quantitativas) ou não-numéricas (qualitativas) (EPSTEIN; KING, 2013). Nessa perspectiva, Pires (2008, p. 87) defende que "é falso afirmar que existe uma metodologia qualitativa ou quantitativa: não há senão pesquisas qualitativas ou quantitativas (ou as duas simultaneamente)" e, da mesma forma, não é possível caracterizar a pesquisa qualitativa através do uso de uma técnica particular de coleta de dados. Assim, ambos os tipos de pesquisa seriam intercambiáveis (podendo ser utilizadas dentro de uma metodologia geral das ciências sociais) e a pesquisa qualitativa se caracterizaria apenas pelo fato de "se constituir fundamentalmente a partir de um material empírico qualitativo, isto é, não tratado sob a forma de números [, mas sim sob a forma de letras]; enquanto a pesquisa quantitativa faz o inverso" (PIRES, 2008, p. 90).

Essa afirmação pode ser complementada pela de Igreja (2017, p. 14), segundo a qual a "pesquisa qualitativa se define por uma série de métodos e técnicas que podem ser empregados com o objetivo principal de proporcionar uma análise mais profunda de processos ou relações sociais". Assim, a fim de exercer a função de empreendimento social da pesquisa em Direito, a pesquisa qualitativa tem o condão de analisar em profundidade as ações sociais em seu contexto e todos os significados que delas podem surgir (IGREJA, 2017).

Com base nos dados coletados e em sua análise predominantemente qualitativa, a partir das técnicas de análise documental, proposta por Cellard (2008), e do estudo de caso, a partir de Yin (2005), um processo inferencial descritivo foi realizado para a extração de fatos desconhecidos. Após a realização da inferência, a fim de concluir o processo investigativo e torná-lo mais robusto, foi necessário, ainda, formular implicações observáveis e estabelecer o controle de hipóteses rivais. As implicações observáveis, segundo Epstein e King (2013, p. 79), são fenômenos do mundo real que poderiam ser detectados se a teoria aventada pela pesquisadora estiver correta, o que é de extrema importância para corroborar o processo inferencial realizado. Por outro lado, as hipóteses rivais são teorias ou explicações que não corroboram com a teoria previamente formulada (EPSTEIN; KING, 2013), isto é, são explicações outras para o mesmo fenômeno que devem ser levadas em consideração e enfrentadas, a fim de se evitar uma tendência parecerista na pesquisa.

3.2 O Estudo de caso

Uma das técnicas adotadas pelo presente trabalho, que se utiliza de múltiplas estratégias, é a do estudo de caso. Segundo Machado (2017, p. 357), um caso é "uma construção intelectual que busca oferecer uma representação de um fenômeno jurídico, em um contexto específico, a partir de um leque amplo de dados e informações". O estudo de caso, por sua vez, se constitui em uma estratégia de pesquisa abrangente, não se reduzindo à forma de coleta de dados, permitindo uma investigação mais holística, que preserve as características significativas de acontecimentos da vida real (YIN, 2005). Isto posto, "o estudo de caso nos convoca a mergulhar profundamente em um fenômeno e a observar a partir de variadas fontes e perspectivas" (MACHADO, 2017, p. 361). Em geral, essa técnica deve ser adotada "quando o pesquisador tem pouco controle sobre os acontecimentos e quando o foco se encontra em fenômenos contemporâneos inseridos em algum contexto da vida real" (YIN, 2005, p. 19).

Segundo Yin (2005), uma questão frequente que surge de um estudo de caso, principalmente estudos de caso único, diz respeito à sua capacidade de generalizar teorias. Quanto a isso, o autor explica que os estudos de caso são, na verdade, generalizáveis a proposições teóricas (generalização analítica) e não a populações ou universos (generalização estatística) (YIN, 2005). Isso quer dizer que o *corpus* empírico observado no caso deve ser utilizado para a criação de uma teoria (no caso da presente investigação, em relação às redes sociais) e essa mesma teoria ajudará a identificar outros casos aos quais os resultados são generalizáveis (YIN, 2005). Essa teoria deverá ser, portanto, replicada e confirmada em outros casos, a fim de fortalecê-la e ajustá-la à realidade.

Com o objetivo de compreender como as redes sociais têm coletado dados de crianças e adolescentes no Brasil, decidiu-se por adotar um estudo de caso único explanatório, cuja unidade de análise é a rede social *YouTube*. Essa plataforma foi escolhida, basicamente, por quatro motivos. Primeiramente, segundo a última pesquisa realizada nos Estados Unidos pelo *Pew Research Center* (2018), 85% dos adolescentes utilizam o *YouTube*, que lidera o *ranking* de redes sociais mais utilizadas (seguida do *Instagram* com 72%, do *Snapchat* com 69% e do *Facebook* com 51%)[22]. Em segundo lugar, o *YouTube* é uma plataforma que traz muitas semelhanças com a televisão e, segundo a pesquisa *TIC Kids Online* Brasil de 2017 (NIC.BR,

[22] Infelizmente, não há dados empíricos relacionados ao Brasil quanto ao uso por crianças e adolescentes da plataforma *YouTube*. Na última pesquisa realizada pelo NIC.BR (2017), sabia-se apenas que a rede social mais utilizada pelas crianças e adolescentes brasileiros era o *Facebook*, com 75% dos entrevistados como usuários, mas não foram coletadas informações acerca do *YouTube* para fins de comparação.

2017), a televisão é ainda o meio em que crianças e adolescentes tem mais contato com produtos mercadológicos[23].

Em terceiro lugar, o *YouTube* também tem se revelado uma plataforma bastante utilizada por crianças e adolescentes para ver e expor conteúdo, de modo que *youtubers* mirins acabam tendo um papel fundamental na quantidade de usuários que utilizam a plataforma, que são atraídos por esse conteúdo especializado. Nesse sentido, em mapeamento realizado pelo ESPM *Media Lab*, em 2016, dos 100 canais de maior audiência do *YouTube*, 48 eram direcionados a crianças (CORREA, 2016). Além disso, dos 230 canais analisados pelo mapeamento, os 110 infantis somavam quase 50 bilhões de visualizações, contra pouco mais de 2 bilhões dos 120 canais restantes (CORREA, 2016).

Por fim, outro fato que demonstra a importância do estudo de caso do *YouTube* é a instauração, em julho de 2018, de um inquérito civil pelo Ministério Público do Distrito Federal e Territórios (2018) para apurar a forma como o *YouTube* vem coletando dados de crianças e adolescentes. Apesar de a plataforma exigir o consentimento dos pais ou responsáveis para o uso de menores de 18 anos, aparentemente ela não realiza qualquer esforço para verificar esse consentimento (MPDFT, 2018). Esse inquérito demonstra o interesse público neste caso específico e a presente pesquisa como importante empreendimento social.

No que concerne à validade externa da investigação, apesar de a escolha pela análise da plataforma do *YouTube* ser bastante particular e justificável, vale citar, ainda, que a polêmica por trás da forma com que os dados dos usuários têm sido tratados, atualmente, pelas redes sociais é generalizada. Apenas considerando as plataformas que mais coletam dados no Brasil hoje[24], percebe-se que elas são pertencentes a apenas dois conglomerados: a *Google* e o *Facebook*. Este trabalho se dedicará à análise da *Google* e, com relação ao *Facebook*, a partir dos escândalos descritos na introdução deste trabalho percebe-se que seu comportamento em relação aos dados de crianças e adolescentes também é questionável. Nesse sentido, um documentário investigativo do *Channel 4* demonstrou como o *Facebook* tinha como política ignorar contas de menores de 13 anos, o que mais tarde fez com que a plataforma se comprometesse a agir mais proativamente em relação a estas contas

[23] Isso, porém, tem mudado a cada ano, com a migração das formas de publicidade para a internet. Essa questão é relevante e já foi apresentada por Negri, Fernandes e Rigolon (2018, no prelo), que discutiram a importante relação entre a coleta de dados e a publicidade direcionada ao público infantil, principalmente devido ao modelo de negócios que tem sido adotado na internet, baseado na economia da atenção e na publicidade como financiadora de suas atividades.

[24] Mais de 50% do tráfego de dados de aplicativos no Brasil vêm de 5 plataformas: *Facebook*, *Chrome*, *YouTube*, *WhatsApp* e *Instagram* (CONVERGÊNCIA DIGITAL, 2016).

(CONSTINE, 2018). Se essa plataforma tratava, portanto, as contas de crianças e adolescentes da mesma maneira que as contas de adultos, pode-se inferir que, quando do caso envolvendo a *Cambridge Analytica*, possivelmente contas de crianças e adolescentes também foram utilizadas para a manipulação política. Da mesma maneira, essas contas também seriam alvo da política de anúncios do *Facebook*, modelo de negócios da rede social. Destaca-se que no Brasil, como mencionado anteriormente, 75% das crianças e dos adolescentes usuários da internet no Brasil possuem uma conta na rede social *Facebook*[25]. Levando essas evidencias em consideração, a teoria apresentada nesta investigação para o *YouTube* poderá ser replicada, portanto, em outros casos de coleta e processamento de dados pessoais de crianças e adolescentes em redes sociais, a fim de ser aprimorada e confirmada (YIN, 2005).

Considerando, assim, que os contratos eletrônicos variam pouco entre os diferentes provedores (KESAN; HAYES; BASHIR apud BASHIR et al., 2015) e que há uma falta de alternativa para o uso seguro desses serviços, muitas vezes essenciais aos cidadãos (como, por exemplo, a possibilidade do pagamento pelo serviço ao invés do uso de seus dados pessoais), o uso secundário dos dados é regra e, portanto, o estudo do caso do *YouTube* pode gerar inferências que poderão ser utilizadas em outros casos.

3.3 A análise documental

Tendo em vista a escolha do caso *YouTube*, a fim de compreender como tem sido realizada a coleta e o processamento de dados de crianças e adolescentes, utilizou-se nesta pesquisa a técnica de análise documental dos documentos de consentimento obrigatório para uso do da plataforma (tanto para o sítio eletrônico *YouTube* quanto para o aplicativo *YouTube Kids*). Essa técnica é de extrema importância para que inferências válidas sejam realizadas a partir dos documentos selecionados (CELLARD, 2008). O documento possibilita "acrescentar a dimensão do tempo à compreensão social" e é uma fonte valiosa nas ciências sociais, por possibilitar reconstruções e diminuir a influência da pesquisadora nos dados (CELLARD, 2008, p. 295).

Antes da análise conteudística de um documento, uma análise preliminar deve ser realizada. Essa análise preliminar deve levar em conta alguns elementos, desenvolvidos por Cellard (2008), que ajudarão na interpretação do documento e na realização de inferências a partir dele. Primeiramente, levar em consideração o contexto no qual o documento foi

[25] Ressalta-se, ainda, que, recentemente, outras plataformas, nas quais crianças e adolescentes estão presentes, também tiveram dados vazados, como é o caso do *Twitter* (ROSA, 2018) e do *Snapchat* (ROHR, 2014).

produzido é primordial, como a sua conjuntura política, econômica, social, cultural etc. Também é importante ter em conta os autores do documento, seus interesses e motivos por trás da positivação das ideias nele contidas, o que possibilita "avaliar melhor a credibilidade de um texto, a interpretação que é dada de alguns fatos, a tomada de posição que transparece de uma descrição, as deformações que puderam sobrevir na reconstituição de um acontecimento" (CELLARD, 2008, p. 300).

Em terceiro lugar, é necessário avaliar a autenticidade e a confiabilidade do texto, a fim de se verificar a qualidade da informação transmitida. Em quarto lugar, é preciso avaliar a natureza do texto, uma vez que "a abertura do autor, os subentendidos, a estrutura de um texto podem variar enormemente, conforme o contexto no qual ele é redigido" (CELLARD, 2008, p. 302). Nessa perspectiva, documentos jurídicos, por exemplo, podem só adquirir um sentido para o leitor no contexto particular de sua produção (CELLARD, 2008). Por fim, um quinto elemento de observação necessário seriam os conceitos-chave e a lógica interna do texto, já que delimitar adequadamente o sentido das palavras e dos conceitos é essencial para a construção de seu sentido, ou seja, é necessário analisar a linguagem, na qual o texto foi construído (CELLARD, 2008).

Tendo em vista a técnica de pesquisa acima desenvolvida, dentro do estudo de caso adotado pelo presente trabalho, foram analisados documentos que descrevem os serviços prestados pelo *YouTube* e como os dados pessoais são coletados e processados, isto é, os contratos eletrônicos "assinados" por cada um de seus usuários. Especificamente, foram analisados os "Termos de Serviço", a "Política de Privacidade" e as "Diretrizes da Comunidade". Além disso, tendo em vista o foco deste trabalho, qual seja, a proteção de dados de crianças e adolescentes, escolheu-se, também, analisar o "Aviso de Privacidade do *YouTube Kids*", que é um adendo à Política de Privacidade da *Google*, utilizada pelo *YouTube*, e que só é valido para o uso do aplicativo *YouTube Kids*. Para tal, além da análise preliminar proposta por Cellard (2008), foi desenvolvido um modelo de análise para ajudar na busca por elementos de conteúdo, que ajudasse a responder a pergunta de pesquisa, o que será mais bem detalhado nas próximas seções do trabalho.

3.4 A coleta de dados

A fim de atingir a replicabilidade necessária em uma pesquisa empírica, a partir de Epstein e King (2013) e o critério de confiabilidade da pesquisa, a partir de Yin (2005), é imperioso tornar as etapas do processo de pesquisa transparentes, para que os mesmos

resultados sejam alcançados em uma eventual replicação da pesquisa, assim como para delimitar os efeitos da subjetividade da pesquisadora sobre a ação social. Essa etapa é também importante para que, no caso de pesquisas realizadas em outras plataformas, a partir da mesma metodologia, possa haver a comparação entre os resultados e o fortalecimento da teoria desenvolvida. Assim, a coleta de dados conhecidos deste estudo encontra-se descrita abaixo.

Entre os dias seis de agosto de dois mil e dezoito e dez de agosto do mesmo mês, período em que a coleta dos documentos foi realizada, o sítio eletrônico do *YouTube* (2018) foi acessado a fim de coletar os documentos anteriormente citados. No sítio eletrônico, na caixa cinza à esquerda, ao rolar-se para baixo na barra de rolagem, é possível encontrar os documentos a serem aqui analisados (como demonstra a Figura 1, no Apêndice): a) Os Termos de Serviço do *YouTube* que, na página inicial estão *linkados* apenas com a palavra "Termos" (Figura 2, no Apêndice); b) a Política de Privacidade da *Google* (Figura 3, no Apêndice) que, por ser detentora do *YouTube*, tem suas políticas a ele aplicadas e c) o documento "Políticas e Segurança" (Figura 4, no Apêndice) do *YouTube*[26], que dispõe sobre diretrizes de uso da plataforma para os usuários, o qual é subdividido em sua página principal em "Diretrizes da Comunidade", "Ferramentas e Recursos de Segurança" e "Denúncia e Aplicação da Política". Os três documentos específicos foram coletados, pois são aqueles, com os quais o *YouTube* exige consentimento quando do uso de seu *website*, segundo o disposto em seus Termos de Serviço.

Além do sítio eletrônico oficial do *YouTube* e de seu aplicativo padrão para *tablets* e *smartphones*, desde 2016, no Brasil, é possível acessar o *YouTube Kids*, aplicativo direcionado especificamente ao público infantil. Segundo a *Google*, esse aplicativo foi desenvolvido para filtrar os vídeos impróprios para crianças, possibilitar o controle parental de conteúdo e definir tempo de uso para que crianças e adolescentes utilizem o aplicativo (GOOGLE LLC, 2018). Assim, foi coletado também o "Aviso de Privacidade do *YouTube Kids*" que é um adendo à Política de Privacidade da *Google* e se encontra disponível na página de ajuda da *Google* (GOOGLE INC., 2018a) (Figura 5, no Apêndice).

Os dois primeiros documentos (Termos de Serviço e Políticas de Privacidade) podem ser facilmente visualizados de maneira integral e impressos, caso o usuário deseje. Em relação ao terceiro documento (Políticas e Segurança ou Diretrizes da Comunidade), porém, na página em que se encontra não é disponibilizado todo o seu conteúdo, sendo colocadas apenas

[26] Nos Termos de Serviço do *YouTube*, este documento é denominado "Diretrizes da Comunidade".

chamadas para os seus conteúdos principais, o que dificulta a visualização das diretrizes como um todo (Figura 6, no Apêndice). Não há uma versão para impressão, sendo tudo disposto na forma de perguntas e respostas. Ao se clicar em "saiba mais" em algum dos temas desta página, o usuário é redirecionado à página de "Ajuda do *YouTube*", local em que essa política está disposta na forma de perguntas e respostas.

Nesta página, não se encontra as mesmas subdivisões da página inicial das Diretrizes da Comunidade. Assim, para entender a nova subdivisão feita dentro da página de ajuda, clicou-se no *link* "Ajuda do *Youtube*" na parte superior esquerda da página, o que redireciona o usuário para a página inicial de ajuda. Há várias subdivisões para ajudar o usuário a se guiar dentro da página, mas o *link* que agrupa todas as políticas é chamado agora de "Política, segurança e Direitos autorais" (Figura 7, no Apêndice), que se subdivide em "Políticas, denúncias e aplicação de políticas", "Central de segurança e privacidade" e "Direitos autorais e gerenciamento de direitos". As outras divisões da página de ajuda do *YouTube* estão relacionadas diretamente a dúvidas técnicas quanto ao próprio uso da plataforma (exemplo disso é a aba "assista a vídeos", que traz o passo a passo para que o usuário assista a vídeos no sítio eletrônico)[27] e, portanto, não foram consideradas na presente pesquisa.

Ao clicarmos em uma dessas subdivisões (Figura 8, no Apêndice), percebe-se a existência de diversas entradas que, por sua vez, ao serem selecionadas (Figura 9, no Apêndice), contém explicações sobre o tema em questão. Foram coletadas todas as entradas existentes referentes ao tópico "Política, segurança e direitos autorais", na página de ajuda do *YouTube*. Elas foram, então, dispostas em um documento de texto a parte, utilizado pela pesquisadora para análise posterior junto aos outros documentos. Os quatro documentos coletados foram analisados em conjunto através do modelo de análise que será explicado no próximo tópico.

3.5 O modelo de análise

Com o objetivo de responder à pergunta de pesquisa proposta neste trabalho, é necessário estabelecer variáveis de análise do objeto de estudo e formas de medi-las, ou seja, a comparação deste objeto com algum *standard* (EPSTEIN; KING, 2013). Dessa forma, um cuidado especial deve ser dedicado a essa parte da pesquisa, uma vez que, se as medidas

[27] Como pode ser verificado na Figura 7, no Apêndice, as outras abas que não foram consideradas no presente estudo são denominadas: "Mais assistidos no YouTube"; "Assista a vídeos"; "Crie vídeos e gerencie seus canais"; "Sua Conta no YouTube"; "Assinaturas e compras no YouTube"; "Programas de parceria do YouTube"; "Programa do YouTube para organizações sem fins lucrativos" e "Publicidade no YouTube".

escolhidas pela pesquisadora não traduzem adequadamente os conceitos contidos na teoria, as conclusões extraídas podem ser defeituosas (EPSTEIN; KING, 2013). A adequação das medidas escolhidas para a pesquisa é o que Yin (2005) denomina de validade do constructo[28].

Para o desenvolvimento desses critérios para a análise dos documentos, duas linhas foram observadas: a análise quanto à forma e quanto ao conteúdo dos documentos. Em relação aos critérios relativos ao conteúdo dos documentos, algumas perguntas foram formuladas previamente à leitura destes. Para a formulação dessas perguntas, observou-se aquilo que Rodotà (2008) descreve como princípios básicos de proteção de dados pessoais, observados em diversas legislações atuais, assim como a teoria de Floridi (2005, 2006, 2014) sobre privacidade informacional. Igualmente, foram utilizados alguns critérios já utilizados em estudos passados por outros pesquisadores, como será disposto a seguir.

Os princípios deduzidos como núcleo comum dos padrões atuais de proteção e dados por Rodotà são:

> 1. *princípio da correção* na coleta e no tratamento das informações;
> 2. *princípio da exatidão* dos dados coletados, acompanhado pela obrigação de sua atualização;
> 3. *princípio da finalidade* da coleta dos dados, que deve poder ser conhecida antes que ocorra sua coleta, e que se especifica na relação entre os dados colhidos e a finalidade perseguida (*princípio da pertinência*); na relação entre a finalidade da coleta e a utilização dos dados (*princípio da utilização não-abusiva*); na eliminação, ou na transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*);
> 4. *princípio da publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
> 5. *princípio do acesso individual*, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;
> 6. *princípio da segurança* física e lógica da coletânea dos dados (RODOTÀ, 2008, p. 59, grifos do autor).

Em segundo lugar, a interpretação autoconstituinte e ontológica de privacidade informacional de Luciano Floridi também foi considerada para a realização das questões a serem observadas no documento. Exemplo disso é saber se informações pessoais podem ser vendidas para terceiros. Nessa perspectiva, Floridi (2014) argumenta que se a informação pessoal faz parte da própria identidade das pessoas, então dever-se-ia considerar ilegal o tráfico de informações, assim como é ilegal o tráfico de órgãos e de pessoas. Com base em

[28] Segundo Yin, a fim de testar a validade do constructo, deve-se cumprir duas etapas: "1. selecionar os tipos específicos de mudanças que devem ser estudadas (em relação aos objetivos originais do estudo); 2) demonstrar que as medidas selecionadas dessas mudanças realmente refletem os tipos específicos de mudanças que foram selecionadas." (YIN, 2005, p. 54-55).

sua teoria também foram feitas perguntas acerca da própria arquitetura do *YouTube*, para verificar se as TIC estão sendo utilizadas para aumentar a privacidade de crianças e adolescentes e não apenas para diminui-la.

Em terceiro lugar, também foram levados em conta os critérios elaborados pela pesquisa conduzida pelo Centro de Tecnologia e Sociedade da Faculdade de Direito da Fundação Getúlio Vargas do Rio de Janeiro (CTS/RJ), que analisou Termos de Serviço de mais de 50 plataformas para compreender como lidavam com os direitos humanos à liberdade de expressão, à privacidade e ao devido processo legal (VENTURINI et al., 2016). Todos os critérios se basearam em documentos de direitos humanos e a pesquisa é bastante abrangente em relação ao significado de privacidade e de proteção de dados a partir da ótica do Direito Internacional. Assim, as perguntas realizadas no que concerne ao direito à privacidade foram também levadas em consideração para a formulação dos critérios utilizados por este trabalho.

Destaca-se que, apesar de a maioria dos critérios adotados poderem também ser utilizados para a análise de como os dados de pessoas em geral tem sido coletados e processados pelas redes sociais, o foco aqui adotado diz respeito a crianças e adolescentes. Assim, foi necessário inserir questões específicas relacionadas aos menores, assim como interpretar aquelas que poderiam ser utilizadas para o público em geral com base em suas consequências para crianças e adolescentes.

A partir dos parâmetros elencados acima, as seguintes questões acerca do conteúdo dos documentos foram desenvolvidas:

1. É permitido ao usuário visualizar e copiar todos os seus dados pessoais disponíveis na plataforma?
2. É permitido ao usuário editar e apagar todos os dados pessoais disponíveis na plataforma?
3. A plataforma avisa ao usuário quando há mudanças em seus Termos de Serviço ou em qualquer outro documento de consentimento necessário para seu uso?
4. A plataforma afirma minimizar a coleta de dados?
5. A plataforma especifica quais dados serão coletados?
6. A plataforma especifica a finalidade da coleta dos dados?
7. A plataforma solicita permissão para utilizar as informações do usuário para outros fins, que não aqueles para os quais eles foram originalmente compartilhados?
8. A plataforma permite que o usuário customize suas definições de privacidade e de coleta de dados?

9. A plataforma mantém os dados do usuário por tempo além do necessário para sua operação ou do tempo definido em lei?
10. A plataforma permite o rastreamento e o acesso a dados do usuário por terceiros?
11. A plataforma escaneia conteúdos do usuário que não estão disponíveis publicamente, como *e-mails*, mensagens privadas etc.?
12. A plataforma rastreia os usuários em outros sítios eletrônicos?
13. A plataforma agrega dados de diferentes servidores?
14. A plataforma agrega dados de diferentes dispositivos?
15. A plataforma compartilha dados com terceiros para fins comerciais?
16. A plataforma compartilha dados com terceiros para fins de processamento ou fins técnicos?
17. A plataforma criptografa ou permite a criptografia de informações ou de conteúdo pessoal nela transmitidos?
18. A plataforma criptografa ou permite a criptografia de informações ou conteúdo pessoal armazenado?
19. A plataforma divulga dados para cumprimento da lei ou para fins judiciais?
20. A plataforma permite explicitamente que crianças e adolescentes a utilizem?
21. A plataforma permite a criação de contas específicas para crianças e adolescentes?
22. A plataforma permite que crianças ou adolescentes utilizem as contas de usuário dos pais?
23. A plataforma possui algum tratamento diferenciado no que concerne ao seu uso por crianças e adolescentes?
24. A plataforma utiliza por padrão ou permite a utilização de configurações especiais para uma proteção reforçada dos dados de crianças e adolescentes?
25. A plataforma possui algum mecanismo de checagem acerca do consentimento dado por pais ou responsáveis de crianças ou adolescentes?
26. A plataforma permite que dados fornecidos por menores de idade sejam removidos mesmo quando estes se tornem adultos?

Além do conteúdo dos documentos, foi também necessária uma análise acerca de sua forma. A linguagem, o tamanho da fonte, a acessibilidade dentro do sítio eletrônico, a extensão do documento etc. influenciam diretamente na propensão de leitura e no entendimento do conteúdo por parte do usuário. Dessa maneira, uma vez que algumas desses questões já são propostas na análise preliminar de Cellard (2008), decidiu-se discuti-las em conjunto, na primeira parte do próximo capítulo.

4 A COLETA E O PROCESSAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES PELO *YOUTUBE*

Neste capítulo serão apresentados os dados conhecidos coletados por esta investigação, que servirão como base para a realização de inferências no capítulo 5, no qual serão discutidos os resultados desta pesquisa. Inicialmente será feita a análise preliminar dos documentos, a partir dos passos propostos por Cellard (2008). Neste mesmo item será feita, também, uma verificação de alguns elementos que extrapolam as características formais apontadas por Cellard (2008), que, porém, são importantes, quando se diz respeito à leitura de contratos eletrônicos na internet. Por fim, é apresentada a análise conteudística dos documentos analisados.

4.1 Análise documental preliminar

Como discutido no item 2.3, quando a pesquisa é realizada em documentos, segundo Cellard (2008), uma análise preliminar é necessária, a fim de avaliar elementos extrínsecos ao próprio conteúdo nele presente, que ajudarão na realização de inferências. De maneira geral, é necessário fazer uma análise do contexto em que o documento foi produzido, dos atores que o produziram, da autenticidade e confiabilidade do documento, de sua natureza e, por fim, de seus conceitos-chave e lógica interna.

Primeiramente, em relação ao contexto dos documentos analisados, este já se encontra pormenorizado na introdução deste trabalho. Em síntese, vive-se em uma sociedade hiperconectada, em que os dados são, hoje, considerados mercadoria e possuem valor de troca. A rapidez das mudanças tecnológicas não tem sido acompanhada pelas mudanças no campo jurídico, o que faz com que as categorias nele presentes, do modo como estão formuladas, não deem conta da realidade. No que tange a este trabalho, os contratos eletrônicos - mais especificamente os termos de serviço e as políticas de privacidade - elevaram o nível de complexidade dos contratos de adesão, já existentes em nosso ordenamento antes mesmo dos desafios advindos das novas tecnologias. Assim, o que permite a coleta e o processamento de dados e a formulação do *Big Data* são contratos de serviço que, como já dito anteriormente, raramente são, de fato, lidos.

Em relação a crianças e a adolescentes, 82% deles estão conectados à internet e 91% utilizam a internet no celular, dispositivo mais difícil de controlar que o computador (NIC.BR, 2017). Além disso, nessa mesma pesquisa, 52% dos pais ou responsáveis

responderam que permite que suas filhas ou filhos assistam a vídeos quando estão sozinhos (NIC.BR, 2017). Esses números demonstram que as crianças e os adolescentes incapazes estão acessando a internet e podem estar consentindo sozinhos com esses contratos eletrônicos. Por outro lado, mesmo quando o uso é supervisionado pelos pais, já se sabe que o número de consumidores que realmente lê esses documentos é muito pequeno, algo em torno de 0,5% e 0,22% (BAKOS; MAROTTA-WURGLER; TROSSEN, 2013 apud VENTURINI et al., 2016). A partir desse cenário de desconhecimento dos termos de uso por parte dos usuários, as empresas acabam por consolidar nestes as mais abusivas cláusulas, com o objetivo de transformar os dados de pessoas em mercadorias. No que se refere às crianças e aos adolescentes, isso tem efeitos especialmente nocivos, que serão tratados com mais profundidade nos próximos tópicos.

Em segundo lugar, no que concerne aos autores dos documentos, o *YouTube* é uma plataforma de compartilhamento de vídeo criada por Chad Hurley e Steve Chen, nos Estados Unidos, em 2005. Devido ao seu rápido sucesso, a corporação foi comprada pela *Google* em outubro de 2006, pelo valor de 1,65 bilhões de dólares (FITZPATRICK, 2010) e em março de 2018, foi orçada em 160 bilhões de dólares, caso fosse uma empresa independente (SANDOVAL, 2018), o que demonstra o rápido crescimento de seu valor de mercado. Sendo parte da *Google*, a marca mais valiosa do mundo (SOUSA; MOREIRA, 2018), sua influência na vida em sociedade, hoje, é enorme e perpassa diversas frentes. Exemplos disso são seu poder de influência político, sendo uma das maiores empresas do mundo; seu poder de influência na vida das pessoas, através do financiamento de diversos *youtubers*, atualmente já denominados influenciadores digitais e seu poder de influência através dos dados que possui de cada um de seus usuários[29], que podem ser utilizados para usos secundários.

Quanto às crianças e aos adolescentes, esse poder de influência é cada vez mais debatido, principalmente em relação à publicidade direcionada a este público. Apesar de esse tipo de publicidade ser, hoje, proibida no Brasil[30], 69% das crianças e adolescentes presentes hoje na internet já teve contato com produtos mercadológicos *online* e 33% já pediu para que os pais comprassem um produto, após contato com publicidade na internet (NIC.BR, 2017).

[29] Em maio de 2018, o *YouTube* atingiu a marca de 1,8 bilhão de usuários ativos mensais (WAKKA, 2018).

[30] Crianças e adolescentes são considerados hipervulneráveis nas relações de consumo. A partir da interpretação dos artigos 36, 37 e 39, do CDC (BRASIL, 1990b), e da Resolução 163, do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA, 2014), o direcionamento de privacidade a este público é considerado abusivo, "pois tal prática tira proveito de sua peculiar condição de desenvolvimento para persuadi-la e seduzi-la ao consumo de produtos ou serviços. Tendo em vista as técnicas sofisticadas de micro-direcionamento customizado de publicidade e a aplicação de métodos psicológicos e comportamentais para seduzir internautas, o uso de dados de crianças para fins comerciais tem potencial ainda mais nocivo" (INSTITUTO ALANA, 2018, p. 3).

Aquilo que na década de 90 foi intensamente combatido no âmbito televisivo, retorna de maneira mais profunda, devido à fluidez da internet. Em geral, as empresas enxergam as crianças e os adolescentes como um nicho de mercado importante, já que influenciam decisões de consumo feitas por suas famílias (DONEDA; ROSSINI, 2015), assim, nesses casos, a proteção de dados e a proteção das crianças e adolescentes como consumidores se entrelaçam. Consequentemente, informações sobre seus comportamentos *online* são extremamente atrativas, pois ajudam no desenvolvimento de estratégias comerciais para atingir cada vez mais este público (SHIN; KANG, 2016 apud VIOLA, 2017). Uma dessas estratégias escolhidas pelas empresas é a parceria com *youtubers* mirins, que se tornam verdadeiros promotores de venda.

Assim, pode-se presumir que os interesses do *YouTube* ou da *Google* encontram-se profundamente incrustados nos documentos analisados nesta pesquisa, uma vez que eles regulam sua relação com os usuários da plataforma, o que torna possível tamanho sucesso. Dessa maneira, os documentos devem ser interpretados levando em consideração a sua elaboração a partir do ponto de vista da sociedade empresária, sendo necessário investigar, também, elementos da realidade que a ele possam ser contrapostos, a fim de contrabalancear tal viés.

Em terceiro lugar, importa avaliar a autenticidade e a confiabilidade do texto, para se verificar a qualidade da informação transmitida. Uma vez que os documentos foram retirados diretamente do sítio eletrônico do *YouTube*, sendo estes documentos institucionais, formulados pela própria sociedade empresária e por ela publicizados, pode-se afirmar que sua procedência está verificada.

Em quarto e em quinto lugar estão elementos estruturais do documento, aos quais serão adicionadas algumas questões de análise importantes, como mencionado acima. Essa análise é essencial, pois a forma de um contrato eletrônico ou de uma política de privacidade diz bastante sobre a possibilidade de ele ser lido e entendido. Em um estudo feito por Böhme e Köpsell (2010), com mais de 80.000 usuários da internet, descobriu-se que aqueles participantes que foram apresentados a textos que se parecem com Termos de Uso os aceitavam 26% mais do que requisições educadas ou textos que possibilitavam uma decisão verdadeiramente voluntária na participação da pesquisa. Em outras palavras, os participantes pareciam estar habituados a este tipo de documento coercitivo e quanto mais o texto se parece com Termos de Uso presentes na internet (os chamados *EULA - End User License Agreement*), mais são aceitos sem questionamento pelos usuários. Percebe-se assim, que a

arquitetura na internet é um fator de grande influência de comportamentos e deve ser utilizada a favor dos direitos fundamentais.

Nessa perspectiva, interessa mencionar a "teoria do ponto patético", de Lawrence Lessig. Lessig (2006) discorre sobre 4 formas de regulação social, utilizadas para restringir ou limitar comportamentos: o Direito, as normas sociais, o mercado e a arquitetura. O Direito restringe comportamentos através da ameaça de punição; as normas sociais através do estigma imposto por uma determinada comunidade a um comportamento; os mercados através do preço por ele exigido em relação ao desempenho de alguma conduta e a arquitetura através da carga física por ela imposta (LESSIG, 2006). Dentro do ciberespaço, todas essas formas de regulação de comportamentos podem ser identificadas e a arquitetura, através dos códigos presentes nos *softwares* e *hardwares*, é uma grande influenciadora de comportamentos pelas condições de acesso que impõe ao uso desse espaço.

> O código ou software ou arquitetura ou protocolos definem essas características, que são selecionadas pelos criadores de código. Eles restringem algum comportamento, tornando outro comportamento possível ou impossível. O código incorpora determinados valores ou torna certos valores impossíveis. Nesse sentido, também é regulação, assim como as arquiteturas dos códigos do espaço real são regulação (LESSIG, 2006, p. 125, tradução nossa) [31].

De igual modo, a forma ou a arquitetura em que os termos de serviço ou a política de privacidade é construída atrai ou repele certos comportamentos. Assim, uma análise mais detida acerca de como esses contratos eletrônicos são apresentados aos usuários do serviço é essencial para entender o comportamento destes.

Sendo assim, no que diz respeito à natureza dos documentos, pode-se afirmar que todos tem natureza jurídica, uma vez que são contratos que formalizam o vínculo jurídico entre o usuário e o *YouTube*. Estes documentos podem ser encontrados facilmente, de maneira geral, na página inicial do sítio eletrônico do *YouTube*. Apenas no que se refere ao Aviso de Privacidade do *YouTube Kids*, talvez por ser referente ao aplicativo e não ao sítio eletrônico em si, é necessário entrar na página de ajuda da *Google* para encontrá-lo.

No que se refere aos conceitos-chave e à lógica interna dos documentos, apesar de todos terem natureza jurídica, vinculando os atos de ambas as partes contratantes, a linguagem e a lógica interna de cada um deles é bastante diferente. Por um lado, em relação aos Termos de Serviço, predomina uma linguagem formal, com jargões específicos, o que, juntamente

[31] No original: "*The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation, just as the architectures of real-space codes are regulations*" (LESSIG, 2006, p. 125).

com seu formato, acabaria por desincentivar sua leitura e seu entendimento pela população em geral. Por outro lado, a Política de Privacidade da *Google*, o Aviso de Privacidade do *YouTube Kids* e as Diretrizes da Comunidade são escritas com uma linguagem mais informal e direta, de melhor entendimento para o usuário comum. Destaca-se que os dois primeiros documentos citados contam ainda com um vocabulário técnico, com diversos termos da informática, que podem não ser compreendidos por todos, mas que é amenizado por um glossário integrado.

Destaca-se que na consideração de n.º 58 do RGPD, em que se dispõe o princípio da transparência, exige-se que "qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado" (UNIÃO EUROPEIA, 2016b). A consideração assevera, ainda, que, sempre que o tratamento seja dirigido a crianças, a linguagem utilizada deve ser clara e simples, para que seja por ela bem compreendida (UNIÃO EUROPEIA, 2016b).

A mesma transparência com relação à linguagem e à acessibilidade da informação é exigida pelo art. 6º, VI, da LGPD, assim como por seu art. 9º, caput e §1º (BRASIL, 2018). Especificamente com relação às crianças, a LGPD, em seu art. 14, §6º, estabelece que

> as informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (BRASIL, 2018).

Uma vez que apenas o *YouTube Kids* pode ser verdadeiramente considerado como aplicativo específico para menores de idade, percebe-se que seu Aviso de Privacidade tem linguagem fácil, mas que pode não ser compreendida diretamente por crianças e adolescentes. Apesar de o documento utilizar pronomes de tratamento como "você", não se sabe se o público alvo da leitura são os menores de idade ou os pais. Percebe-se que algumas sentenças são direcionadas a crianças e a adolescentes, como em "Como acessar o *YouTube Kids* com a conta do *Google* **do seu pai/mãe**: Coleta e uso das informações adicionais" (GOOGLE INC., 2018a, grifo nosso). Em outras sentenças, parece que o público alvo são os pais, como em "informações contidas nos perfis limitados que você pode ativar **para que seus filhos** possam editar" (GOOGLE INC., 2018a, grifo nosso). Destaca-se, ainda, que os Termos de Uso do *YouTube*, que também é adotado pelo aplicativo *YouTube Kids*, possui linguagem de difícil acesso, como explicitado acima, o que prejudicaria a leitura deste por crianças e adolescentes.

No que diz respeito ao formato, tanto a Política de Privacidade da *Google* quanto o Aviso de Privacidade do *YouTube Kids* são escritos a partir de tópicos temáticos bem determinados, facilitando a localização de informações específicas e o entendimento do conteúdo. O mesmo ocorre com as Diretrizes da Comunidade que, para atingir o mesmo objetivo, dispõe suas informações em perguntas e respostas, possuindo, ainda, uma ferramenta de busca. No que se refere à extensão da leitura[32] e à fonte utilizada, os documentos variam bastante entre si, indo de 2 a 4 páginas, do Aviso de Privacidade do *YouTube* e dos Termos de Serviço, com fontes pequenas, a 29 e 86 páginas, da a Política de Privacidade e da parte das Diretrizes da Comunidade analisada[33], respectivamente, com fontes que facilitam a leitura. Importa salientar que nem o RGPD nem a LGPD possuem diretrizes específicas sobre a extensão ou a fonte utilizada nesses documentos, apesar de serem claras em relação à necessidade de um texto simples, acessível e transparente, como disposto acima.

4.2 Análise de conteúdo dos documentos

Com o objetivo de responder às perguntas em relação ao conteúdo dos documentos analisados no presente trabalho, mencionadas no capítulo 2, decidiu-se por criar o quadro disposto abaixo. Nesse quadro foram dispostas, à esquerda, todas as questões analisadas no documento e, à direita, as respostas de acordo com o que neles foi observado. Devido à necessidade de replicabilidade da pesquisa, cada informação de resposta inserida no Quadro foi previamente identificada, segundo o documento em que se encontra e sua localização dentro deste.

Nesse sentido, a terminologia **TS** foi utilizada para informações que poderiam ser encontradas nos Termos de Serviço do *YouTube*. Uma vez que este documento possui cláusulas numeradas, essa mesma numeração foi utilizada para identificar o local em que poderia ser encontrada a informação que respondia à questão proposta. A terminologia **PP** foi utilizada para aquelas informações encontradas na Política de Privacidade da *Google*, utilizada pelo *YouTube*. Posto que essa política não possui numeração, para fins de localização, foi utilizado o título sob o qual a informação poderia ser encontrada. Ademais, uma vez que o documento, como um todo, foi coletado através da impressão da página *web*

[32] O tamanho dos documentos em páginas foi definido a partir da versão para impressão de cada documento. Com relação às diretrizes da comunidade, uma vez que não existe versão para impressão deste documento, cada entrada foi copiada para um documento em separado, com fonte *Times New Roman*, 12, espaçamento 1,15 e margens de 2 cm cada.

[33] Destaca-se que a extensão das Diretrizes da Comunidade refere-se apenas à parte analisada pelo trabalho e não a toda a informação disponível nessas diretrizes.

em que se encontrava, também foi inserido o número da página gerado a partir desse comando de impressão - ex.: se a informação estava na página 10 do documento de impressão gerado, sob o título de "Exportar e excluir informações", ela foi inserida na resposta após a designação "Exportar e excluir informações" (p.10). Em relação às Diretrizes da Comunidade, apesar de ser de consentimento obrigatório pelo usuário para o uso do *YouTube*, a elas não foi atribuída uma sigla, vez que não respondia a qualquer das questões propostas. Todavia, seu conteúdo será utilizado no capítulo 5, para a discussão dos resultados. Por fim, a terminologia **APYK** foi utilizada para as informações retiradas do Aviso de Privacidade do *YouTube Kids*.

Quadro – Respostas às questões de conteúdo de acordo com cada documento analisado

	Resposta
1. É permitido ao usuário visualizar e copiar todos os seus dados pessoais disponíveis na plataforma?	**PP** – "Exportar e excluir informações" (p.10); "Você pode exportar uma cópia das suas informações ou excluí-las da sua Conta do *Google* a qualquer momento" (p.14): permite que o usuário visualize e exporte uma cópia do conteúdo da conta da *Google* para fins de *backup* ou para utiliza-la em outros serviços fora da *Google*.
2. É permitido ao usuário editar e apagar todos os dados pessoais disponíveis na plataforma?	**PP** – "Modos de avaliar e atualizar suas informações" (p. 9): permite que o usuário gerencie e edite informações pessoais. - "Exportar e excluir informações" (p.10): permite que o usuário exclua seu conteúdo dos serviços *Google*, em parte ou no todo, segundo a legislação aplicável.
3. A plataforma avisa ao usuário quando há mudanças em seus Termos de Serviço ou em qualquer outro documento de consentimento obrigatório para o seu uso?	**TS** – Item 1B: informa que, apesar de o *YouTube* se esforçar para avisar o usuário de possíveis mudanças, o usuário deve reler os Termos periodicamente, visto que eles podem ser modificados a critério da plataforma, a qualquer tempo. - Item 13: afirma que o *YouTube* poderá modificar os Termos de Serviço a qualquer tempo e sem aviso prévio, sendo responsabilidade do usuário a releitura dos termos periodicamente para verificar qualquer alteração. **PP** – "Alterações nesta política" (p. 16): afirma que, em caso de alterações significativas, avisos com maior destaque serão fornecidos, o que inclui notificação por *e-mail*.

4. A plataforma afirma minimizar a coleta de dados?	Não informa.
5. A plataforma especifica quais dados serão coletados?	**PP** – "Informações que coletamos quando você usa nossos serviços" (p. 2 ss.): traz a relação de dados coletados do usuário quando este utiliza os serviços da *Google*.
6. A plataforma especifica a finalidade da coleta dos dados?	**PP** – "Usamos os dados para criar serviços melhores" (p. 5 ss.): descreve as finalidades da coleta e do processamento de dados.
7. A plataforma solicita permissão para utilizar as informações do usuário para outros fins, que não aqueles para os quais eles foram originalmente compartilhados?	**PP** – "Proteger o Google, nossos usuários e o público" (p. 7): afirma solicitar autorização antes de utilizar informações para fins que não estiverem abordados na Política de Privacidade.
8. A plataforma permite que o usuário customize suas definições de privacidade e de coleta de dados?	**PP** – "Quando você usa nossos serviços, está confiando a nós suas informações (...)" (p.1): afirma ser possível ajustar as configurações de privacidade para controlar o que é coletado do usuário. – "Você tem escolhas em relação às informações que coletamos e como elas são usadas" (p. 7): disponibiliza uma verificação da privacidade para que o usuário customize suas definições de privacidade. – "Exportar, remover e excluir informações" (p. 11): informa a possibilidade de alterar as configurações do navegador para o uso de *cookies* e modificar as configurações de localização do dispositivo.
9. A plataforma mantém os dados do usuário por tempo além do necessário para a sua operação ou do tempo definido em lei?	**PP** – "Você pode exportar uma cópia das suas informações ou excluí-las da sua Conta do Google a qualquer momento" (p.14): afirma armazenar dados por períodos limitados quando precisam ser mantidos para fins comerciais ou legais legítimos. Direciona a um *link* com a descrição das Tecnologias *Google*, que explica a política de manutenção dos dados nos servidores da sociedade empresária. Afirma que, mesmo depois de serem excluídos, alguns dados são mantidos em seus servidores até que a conta seja excluída, como, por exemplo, o histórico de pesquisa. Além disso, mesmo após a exclusão da conta, a *Google* afirma poder manter dados para fins de negócio ou para fins legais, com os seguintes objetivos: segurança e prevenção contra fraude e abuso; manutenção de registros financeiros; cumprimento de requisitos legais ou regulamentares; garantia da continuidade

	dos seus serviços e comunicações diretas com a *Google*.
10. A plataforma permite o rastreamento e o acesso a dados do usuário por terceiros?	**PP** – "Com administradores de domínios" (p. 12): afirma que administradores de domínios que utilizam os serviços da *Google* têm acesso a informações dos membros da organização, como *e-mail* e estatísticas da conta, podem alterar a senha da conta e restringir a capacidade de alteração de configurações de privacidade.
11. A plataforma escaneia conteúdos do usuário que não estão disponíveis publicamente, como *e-mails*, mensagens privadas etc.?	**PP** – "Itens que você cria ou nos fornece" (p.2): afirma coletar o conteúdo que o usuário cria, de que faz *upload* ou que recebe de outras pessoas, ao usar seus serviços, incluindo *e-mails* enviados e recebidos, fotos e vídeos salvos, documentos e planilhas criadas e comentários em vídeos do *YouTube*.
12. A plataforma rastreia os usuários em outros sítios eletrônicos?	**PP** - "Informações que coletamos quando você usa nossos serviços" (p.4): afirma utilizar tecnologias para coletar informações como *cookies*, *tags* de *pixel*, *caches* etc.
13. A plataforma agrega dados de diferentes servidores?	**PP** - "Informações que coletamos quando você usa nossos serviços" (p.4): afirma receber informações de parceiros comerciais. - "Proteger o Google, nossos usuários e o público" (p. 7): afirma poder combinar as informações coletadas em seus diferentes serviços com as informações coletadas por outros sítios eletrônicos e aplicativos.
14. A plataforma agrega dados de diferentes dispositivos?	**PP** – "Proteger o Google, nossos usuários e o público" (p. 7): afirma poder combinar as informações coletadas em diferentes dispositivos para as finalidades de coleta descritas.
15. A plataforma compartilha dados com terceiros para fins comerciais?	**PP** – "Quando o Google compartilha as informações" (p.13): afirma poder compartilhar informações de identificação não pessoal publicamente com parceiros, editores, anunciantes, desenvolvedores ou detentores de direitos.
16. A plataforma compartilha dados com terceiros para fins de processamento ou fins técnicos?	**PP** – "Informações que coletamos quando você usa nossos serviços" (p. 4): afirma receber informações de parceiros de segurança para "proteção contra abuso". – "Para processamento externo" (p. 12):

	afirma fornecer informações às suas afiliadas ou a outras empresas e pessoas confiáveis para processar informações no lugar da *Google*.
17. A plataforma criptografa ou permite a criptografia de informações ou de conteúdo pessoal nela transmitidos?	**PP** – "Incorporamos segurança nos nossos serviços para proteger suas informações" (p. 13): afirma utilizar a criptografia para manter dados privados enquanto estão em trânsito.
18. A plataforma criptografa ou permite a criptografia de informações ou conteúdo pessoal armazenado?	Não informa.
19. A plataforma divulga dados para cumprimento da lei ou para fins judiciais?	**PP** – "Por motivos legais" (p. 12): afirma compartilhar informações caso acreditem ser necessário para cumprir legislação, regulação, processo legal ou solicitação governamental aplicável; para cumprir Termos de Serviços aplicáveis, inclusive para investigação de possíveis violações; para detectar, impedir ou lidar com fraudes, problemas técnicos ou de segurança; para proteger de prejuízos a direitos, à propriedade ou à segurança da *Google*, de seus usuários ou do público, conforme solicitado ou permitido por lei.
20. A plataforma permite explicitamente que crianças e adolescentes a utilizem?	**TS** – Item 1.D: exige que o usuário tenha 18 anos, seja emancipado ou tenha autorização legal dos pais ou de tutores para consentir com os Termos de Serviço; afirma que a plataforma não foi desenvolvida para menores de 18 anos e que estes não devem utilizá-la.
21. A plataforma permite a criação de contas específicas para crianças e adolescentes?	Uma vez que o *YouTube* não permite a utilização, através dos seus Termos de Serviços, da plataforma por menores de idade, não há a possibilidade de criação de contas específicas para crianças e adolescentes. Os menores podem utilizar, todavia, o aplicativo *YouTube Kids* para *tablets* e *smartphones*.
22. A plataforma permite que crianças ou adolescentes utilizem as contas de usuário dos pais?	**TS** – Item 3.A – Impede que usuários utilizem contas de terceiros sem permissão e afirma a necessidade da veracidade dos dados inseridos na conta.
23. A plataforma possui algum tratamento diferenciado no que concerne ao seu uso por crianças e adolescentes?	**APYK** – Apenas o aplicativo *YouTube Kids* possui um Aviso de Privacidade separado, específico para crianças e adolescentes. Seu conteúdo, todavia, em relação à coleta e ao

	processamento de dados, não difere substancialmente do oferecido dentro da plataforma *YouTube*. – "Informações que coletamos" (p. 1): nesse sentido, o aplicativo *YouTube Kids* afirma coletar informações sobre o dispositivo, sobre o acesso, sobre o aplicativo utilizado e sobre identificadores móveis. – "Como utilizamos as informações que coletamos" (p. 1): as informações são utilizadas para fins operacionais, para oferecer conteúdo personalizado e para fornecer publicidade contextual. – "Informações que compartilhamos" (p. 1 ss): afirmam divulgar informações dos usuários com autorização dos pais para empresas, organizações e pessoas físicas fora da *Google*; por razões legais e para processamento externo. – "Interpretação de termos conflitantes" (p. 2): afirma que o Aviso de Privacidade do *YouTube Kids* é, em geral, consistente com a Política de Privacidade da *Google*, mas que, em caso de conflito, o primeiro prevalece.
24. A plataforma utiliza por padrão ou permite a utilização de configurações especiais para uma proteção reforçada dos dados de crianças e adolescentes?	Não informa.
25. A plataforma possui algum mecanismo de checagem acerca do consentimento dado por pais ou responsáveis de crianças ou adolescentes?	Não informa.
26. A plataforma permite que dados fornecidos por menores de idade sejam removidos mesmo quando estes se tornem adultos?	**PP** – "Modos de avaliar e atualizar suas informações" (p. 9): permite que o usuário gerencie e edite informações pessoais. - "Exportar e excluir informações" (p. 10): permite que o usuário exclua seu conteúdo dos serviços *Google*, em parte ou no todo, segundo a legislação aplicável.

Fonte: coleta e sistematização dos dados diretamente realizada pela autora, a partir dos documentos de consentimento obrigatório para o uso da plataforma *YouTube* e para o uso do aplicativo *YouTube Kids*.

A partir deste momento, as informações dispostas no quadro acima serão analisadas com maior profundidade, a fim de serem compreendidas dentro do contexto mais amplo em que se encontram. Sobre a possibilidade de o usuário poder visualizar e copiar todos os seus dados pessoais disponíveis na plataforma, o *YouTube* permite que isso seja realizado (Questão

1[34]). O usuário tem a possibilidade, além de copiar as informações para fins de cópia de segurança (*backup*), de exportar seus dados para outros serviços, funcionando essa cópia como uma forma de portabilidade dos dados para outras plataformas, respeitando o princípio do acesso individual indicado por Rodotà (2008). O princípio do livre acesso aos dados coletados, assim como a portabilidade destes para outros serviços, estão presentes nos artigos 6º, IV, e 18, da LGPD (BRASIL, 2018), bem como no art. 20.º do RGPD (UNIÃO EUROPEIA, 2016b).

Em relação à especificação dos dados coletados, isso é detalhado pela plataforma em sua Política de Privacidade (Q5). O mesmo detalhamento ocorre em relação às finalidades específicas da coleta e do processamento de dados (Q6). Destaca-se que ela afirma solicitar permissão para coletar dados para outros fins além daqueles já especificados em sua política (Q7), algo exigido pela LGPD em seu art. 9º, §2º e 6º, I (BRASIL, 2018). Assim, no que se refere a essas três questões, a *Google* estaria de acordo com o princípio da finalidade e da adequação presentes na LGPD, em seu art. 6º, I e II (BRASIL, 2018), e no RGPD, em seu art. 5.º, 1., b) (UNIÃO EUROPEIA, 2016b). Essa atuação é referida por Rodotà (2008) a partir do princípio da finalidade, que também comporta o princípio da pertinência e o princípio da utilização não abusiva[35].

Também é permitido ao usuário editar e apagar todos os dados pessoais disponíveis na plataforma ou parte deles, o que vai ao encontro dos princípios da correção e da exatidão dos dados (Q2), o que na LGPD é tratado como princípio da qualidade dos dados, em seu art. 6º, V (BRASIL, 2018). Nesse sentido, caso crianças e adolescentes forneçam dados para a plataforma e, mais tarde, quando adultos, decidam apagá-los, isso seria possível (Q26). Essas considerações devem ser mitigadas, todavia, com o fato de a plataforma afirmar armazenar os dados dos usuários, ainda após a requisição do apagamento destes, ou mesmo após a exclusão da conta, para fins legais e comerciais (Q9). Isso pode colocar em risco o direito ao apagamento dos dados, previsto no art. 7º, X, do Marco Civil da Internet (BRASIL, 2014), e no art. 18, V, da LGPD (BRASIL, 2018), bem como o princípio da transparência presente na LGPD, em seu art. 6º, VI (BRASIL, 2018) e o princípio da prevenção, definido pelo art. 6º, VIII da LGPD (BRASIL, 2018). No RGPD, a previsão do apagamento de dados está, dentre outros artigos, presente sem seu art. 17.º (UNIÃO EUROPEIA, 2016b).

[34] A partir deste momento, as referências às questões do quadro serão escritas apenas com a letra Q seguida de seu número respectivo.

[35] Destaca-se que a verificação do cumprimento destes princípios, neste caso, se dá apenas pelo descrito nos documentos analisados, sendo uma limitação deste trabalho a análise de seu cumprimento na prática.

A discussão sobre o apagamento de dados é especialmente importante quando se trata de crianças e adolescentes que, por vezes, podem sofrer consequências, quando adultos, das decisões tomadas enquanto menores de idade. Como já exposto neste trabalho, os problemas causados pela coleta e processamento excessivo de dados pessoais está relacionado à assimetria informacional. Nesse sentido,

> à medida que se acumula um grande volume de informações sobre um indivíduo, torna-se mais provável conhecer aspectos de seu comportamento, permitindo, por exemplo, processos de predição sobre suas futuras condutas ou o seu enquadramento dentro de perfis de comportamento pré-determinados. Tais processos raras vezes são transparentes para o próprio indivíduo, para quem costuma ser mais difícil ainda perceber o efeito concreto que esse tratamento de dados pessoais terá sobre a sua própria vida (DONEDA; ROSSINI, 2015, p. 38).

Quando se trata de pessoas vulneráveis e em desenvolvimento, a impossibilidade de se ter certeza de que aquelas decisões de compartilhamento que fez ainda menor de idade, ou então, que foram realizadas por seus pais ou responsáveis, serão mesmo excluídas gera diversos problemas. Primeiramente, manter informações para fins comerciais, mesmo quando já requisitado seu apagamento pelo indivíduo, pode gerar inúmeras questões relacionadas à manipulação do ambiente social *online* em que a criança ou o adolescente está inserido, através do *marketing*, afetando seu livre arbítrio, sua identidade e sua segurança (UNICEF, 2017). Além disso, pode gerar um engessamento de suas preferências ao longo da vida, sem que se possa delas se desfazer ou mesmo sem que se esteja ciente do uso desses dados para tal fim.

Em segundo lugar, essas informações podem macular a reputação dessas pessoas, fazendo com que tenham problemas no futuro quanto a ser vigiado pelo governo, a se inserir no mercado de trabalho, a conseguir crédito ou mesmo a ter sua dignidade humana respeitada, sem que seu passado as persiga[36]. Destaca-se que, na pesquisa realizada pelo NIC.BR (2017), 22% das crianças e dos adolescentes entrevistados já haviam compartilhado informações na internet, das quais se arrependeram e que, depois, apagaram. Percebe-se, porém, que apagar a informação não é garantia do seu desaparecimento. Egas (2017, p. 34) evidencia o fato de que,

> no caso de cometimento de atos infracionais, por exemplo, o ECA dispõe que o adolescente, ao completar 18 anos, deve ter seu histórico no sistema socioeducativo apagado, justamente porque a passagem dessa fase da vida altera também o seu

[36] Isto está relacionado com a economia da reputação, na qual o histórico *online* vale, hoje, mais do que o histórico de crédito do usuário (NYST, 2017).

> lugar no mundo das relações sociais e jurídicas. No caso das TIC, ainda não existem dados de pesquisas sobre o impacto da exposição indevida na rede para a vida futura desses indivíduos. Considerando, porém, que o desenvolvimento humano é uma constante, a proteção desses indivíduos – ou sua ausência – pode acarretar consequências permanentes, numa fase da vida na qual eles ainda não podem ser responsabilizados por todas as suas escolhas.

Em consonância com o comportamento acima, a plataforma também não se compromete com a minimização da coleta de dados[37], nem nos documentos referentes ao sítio eletrônico *YouTube*, nem em relação ao *YouTube Kids* (Q4; Q23), o que é bastante questionável quando se trata de dados de crianças e adolescentes. O princípio da minimização da coleta de dados, trazido pelo RGPD (UNIÃO EUROPEIA, 2016b), em seu art. 5.º, 1., *c*, também foi adotado também pela LGPD, em relação aos dados de crianças, em seu art. 14, §4º, bem como em seu art. 6º, III (princípio da necessidade) (BRASIL, 2018). Esse princípio busca, justamente, mitigar os problemas expostos no parágrafo anterior. Mesmo considerando apenas o aplicativo *YouTube Kids*, este afirma compartilhar dados com parceiros comerciais e utilizá-los para publicidade contextual (apesar de afirmar não utilizar dados do aplicativo para publicidade baseada em interesses). Ressalta-se que, no Brasil, como discutido acima, qualquer tipo de publicidade direcionada a crianças ou adolescentes é proibida.

Apesar de não afirmar minimizar a coleta de dados, a *Google* destaca, ao longo de sua Política de Privacidade, a possibilidade de o usuário customizar suas definições de privacidade e decidir aquilo que será com ela compartilhado (Q8). Entretanto, as informações fornecidas por este contrato devem ser moderadas com elementos empíricos. Assim, cumpre destacar o estudo realizado pela *Associated Press* (NAKASHIMA, 2018), que verificou que, mesmo requisitando explicitamente nas configurações de privacidade da *Google* que esta pare de rastrear a localização do usuário, esse desejo não é verdadeiramente respeitado. Isso ocorreria, pois alguns aplicativos da *Google* armazenariam automaticamente dados de localização sem requisitar a permissão do usuário (NAKASHIMA, 2018). Nos Estados Unidos, a localização do usuário salva pela *Google* já foi alvo, inclusive, de investigação policial, na qual se requisitou os históricos de localização de uma determinada área para encontrar dispositivos perto de uma cena de assassinato (NAKASHIMA, 2018), o que demonstra a gravidade do armazenamento indevido desse tipo de informação.

[37] Segundo Rodotà (2008), a minimização da coleta de dados diz respeito ao fato de que nenhum dado pessoal deve ser coletado se o propósito específico pode ser alcançado sem o processamento desses dados pessoais. Esse mesmo princípio tem sido denominado, também, como princípio da necessidade, nomenclatura escolhida pela LGPD.

A customização das configurações está também relacionada ao fato de a plataforma não possuir um tratamento diferenciado no que concerne ao seu uso por crianças e adolescentes, mesmo porque seu sítio eletrônico não é adequado para menores, como o próprio *YouTube* afirma. Em relação ao aplicativo *YouTube Kids*, que foi projetado especialmente para crianças e adolescentes, este possui um Aviso de Privacidade separado, com alguns termos especiais (Q23). Não obstante, seu conteúdo em relação à coleta e processamento de dados não difere substancialmente em relação à Política de Privacidade e aos Termos de Serviço do sítio eletrônico tradicional do *YouTube*, no que diz respeito ao tipo de informação que é coletada, à forma de uso dessas informações e às informações que são compartilhadas com terceiros. Isso, como já dito, vai contra o princípio da minimização da coleta de dados deste público, bem como o princípio da prevenção, disposto no art. 6º, VIII, da LGPD (BRASIL, 2018). Também vai contra a necessidade de um tratamento especial dos dados de crianças e adolescentes, presente na consideração n.º 38, do RGPD (UNIÃO EUROPEIA, 2016b), e na consideração n.º 50, da Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho (UNIÃO EUROPEIA, 2016a). A necessidade de um tratamento especial, baseado no melhor interesse da criança e do adolescente também está presente na LGPD, no *caput* de seu art. 14 (BRASIL, 2018). Nessa perspectiva, a plataforma tampouco informa sobre a possibilidade de configurações especiais para uma proteção reforçada de dados de crianças e adolescentes (Q24).

O não uso dessas configurações especiais vai diretamente de encontro àquilo que é trazido pelo RGPD, em seu art. 25.º (UNIÃO EUROPEIA, 2016b), que dispõe sobre a importância da adoção do *Privacy by Design* e do *Privacy by Default*. A LGPD também regula essas questões no art. 46, §2º (BRASIL, 2018). O conceito de *Privacy by Design* determina que qualquer ação de uma empresa ou ente público que envolva coleta e processamento de dados pessoais deve ser feita com a proteção dos dados em mente em cada passo do procedimento, de maneira que a privacidade seja "construída" no próprio sistema durante o processo (IRISH COMPUTER SOCIETY, 2018). Já o conceito de *Privacy by Default* significa que, ao ser lançado ao público, o produto ou serviço deve vir, por padrão, com as configurações mais restritas de privacidade, o que está ligado, diretamente ao princípio da necessidade ou minimização dos dados coletados (ICS, 2018). Esses dois conceitos estão relacionados com a capacidade das TIC digitais de aumentar a privacidade informacional ou, até mesmo, de alterar seu significado, visto que podem reontologizar a própria natureza da infosfera, uma vez que são interativas (FLORIDI, 2005). Também estão

ligados à possibilidade de a arquitetura na internet influenciar comportamentos, como descrito por Lessig (2006).

Por não utilizar configurações especiais mais protetivas por padrão para crianças e adolescentes, esses usuários acabam por fazer cálculos de privacidade diferente daqueles que fariam em uma situação não mediada (BOYD, 2014, p. 62). Desse modo, "ao invés de se perguntar se a informação a ser compartilhada é significante o suficiente para ser publicizada de maneira ampla, eles se perguntam se é íntima o suficiente para requerer proteção especial" [38] (BOYD, 2014, p. 62, tradução nossa). Em outras palavras, quando participam dessas redes, os usuários acabam por adotar o lema "público-por-padrão, privado-por-esforço" [39] (BOYD, 2014, p. 62, tradução nossa), o que gera uma sensação perigosa de que a privacidade é apenas necessária quando se tem algo a esconder (BOYD, 2014).

Quanto às mudanças no conteúdo dos Termos de Serviço ou de outro documento de consentimento obrigatório (Q3), estas são tratadas em diversas cláusulas. Ocorre, porém, que as informações fornecidas pela plataforma quanto a essa questão são bastante conflitantes. Dentro dos Termos de Serviço, o *YouTube* afirma, no item 1.B, que se esforça para avisar o usuário das possíveis mudanças no documento, mas que este deve relê-lo periodicamente. No mesmo documento, no item 13, contudo, a plataforma afirma que a responsabilidade de revisitar os termos é única do usuário e que ela poderá modificá-los sem qualquer aviso prévio e a qualquer tempo. Por outro lado, em relação à sua Política de Privacidade, a *Google* afirma que em caso de alterações significativas, avisos com maior destaque serão fornecidos, como notificação por *e-mail*.

Diante da possibilidade da mudança das políticas de privacidade sem aviso prévio, o usuário, que já não costuma ler estes documentos, acaba por ficar refém da vontade de apenas um dos contratantes, que se autoriza a modificar o contrato unilateralmente. Isso vai de encontro a diversos princípios como o da transparência, positivado no CDC, em seu art. 6º, III (BRASIL, 1990b), e no art. 6º VI, da LGPD (BRASIL, 2018) e o princípio da correção na coleta e processamento de dados (RODOTÀ, 2008). Ressalta-se, também, a falta de transparência e de uma linguagem adequada quando do uso de expressões vagas no contrato, como "se esforça" e "alterações significativas", o que também confunde o consumidor e prejudica a segurança jurídica, principalmente quando se trata de produtos voltados a crianças e adolescentes, que deveriam ser escritos com linguagem simples.

---

[38] No original: "*Rather than asking themselves if the information to be shared is significant enough to be broadly publicized, they question whether it is intimate enough to require special protection*" (BOYD, 2014, p. 62).
[39] No original: *"public-by-default, private-through-effort"* (BOYD, 2014, p. 62).

Em relação às crianças e aos adolescentes, Boyd (2014) assevera que quando os sítios eletrônicos alteram repetidamente as configurações de privacidade, isso acaba por dificultar o desenvolvimento de habilidades por este público para gerenciar como a informação fluirá dentro de uma situação social. Assim, desenvolver as habilidades necessárias para gerenciar o conteúdo visível para outras pessoas torna-se, senão impossível, incrivelmente trabalhoso (BOYD, 2014), o que, na verdade, seria algo essencial no mundo hiperconectado.

No que se refere ao rastreamento e ao acesso a dados dos usuários por terceiros, a *Google* afirma que administradores de domínios que utilizam seus serviços têm acesso a informações dos membros da organização, como *e-mail* e estatísticas da conta, além de poderem alterar a senha da conta e restringir capacidade de alteração de configurações de privacidade (Q10). Nessa perspectiva, a *Google* permite que terceiros restrinjam direitos dos usuários membros da organização da qual fazem parte. Vale citar, ainda, o fato de terceiros terem acesso, assim como a *Google*, a informações de locais não públicos, como *e-mails*, planilhas e fotos (Q11) e, apesar de afirmar que cessaria o escanemaneto de *e-mails* em julho de 2017, isso, até o momento, não foi realizado pela *Google* (POPKEN, 2018).

Em relação ao rastreamento em outros sítios eletrônicos, a *Google* afirma coletar informações do usuário enquanto navega na internet, como através de *cookies*, *caches* etc. (Q12). Os dados coletados nos diferentes sítios eletrônicos são ainda agregados pela *Google* (Q13), assim como os dados de diferentes dispositivos utilizados pelo mesmo usuário (Q14). No que concerne ao compartilhamento com terceiros, a *Google* afirma compartilhar informações de identificação não pessoal publicamente com parceiros, editores, anunciantes, desenvolvedores ou detentores de direitos, para fins comerciais (Q15). Do mesmo modo, afirma compartilhar dados com terceiros para fins de processamento ou fins técnicos (Q16). Todos esses comportamentos acabam por criar um rastro digital, do qual a criança ou o adolescente dificilmente conseguirá se livrar ao longo da vida, o que gera os diversos problemas já expostos acima.

A junção de dados coletados em diversos locais e dispositivos cria, ainda, o problema da bolha dos filtros, algo perverso no crescimento plural de crianças e adolescentes. A partir da análise de tudo o que o usuário costuma fazer na internet, são criados filtros do que chega até ele, para que este fique mais tempo navegando, o que é uma consequência da economia da atenção e da ligação da internet à publicidade, modelo de negócios vigente hoje. Essa edição daquilo que chega até as pessoas mina a capacidade criativa, limita a formação de uma consciência crítica capaz de lidar com a complexidade e pluralidade do mundo e estimula a polarização de ideias. Afinal, “um mundo construído a partir do que é familiar é um mundo

no qual não temos nada a aprender" (PARISER, 2012, p. 16), onde os estereótipos e a discriminações históricas são apenas reforçados. A aldeia global imaginada por McLuhan, que muitos defendiam ser possível através da internet, mostra-se cada vez mais longe da realidade: o que se prevê agora, na verdade, é uma "*web of one*" (PARISER, 2011). Entretanto, crescer em um espaço plural é a "premissa básica para garantir a liberdade de crítica e pensamento, o livre desenvolvimento da personalidade, das representações subjetivas e identitárias e, até mesmo, a igualdade de oportunidades" (HARTUNG; PITA, 2018), algo essencial no desenvolvimento de crianças e adolescentes.

Relativamente à segurança dos dados, a plataforma afirma utilizar a criptografia para dados em trânsito (Q17), mas não informa satisfatoriamente no tocante à criptografia no armazenamento dos dados, declarando apenas a existência de segurança física (Q18), provavelmente devido à necessidade dos dados dos usuários para seu modelo de negócios, como já apontam alguns estudos (SCHULZ; VAN HOBOKEN, 2016). A criptografia e, mais especificamente, a encriptação[40] são elementos importantes para "garantir proteção das informações e da comunicação no âmbito pessoal, comercial e no setor público", bem como "para proteger o anonimato dos agentes de comunicação e, com isso, a privacidade em geral" (SCHULZ; VAN HOBOKEN, 2016, p. 11).

A partir dessa perspectiva, é necessário avaliar a posição da empresa quando ocorrem problemas de segurança de dados por ela mantidos. Em março de 2018, quando o *Facebook* estava sob escrutínio mundial com o escândalo envolvendo a *Cambridge Analytica*, a *Google* identificou um *bug* em seu sistema da rede social *Google+*, que possibilitava que terceiros desenvolvedores de aplicativos tivessem acesso a dados de mais de 500.000 pessoas em sua rede (WONG; SOLON, 2018). Entretanto, a sociedade empresária, diante do que ocorria com o *Facebook*, decidiu por não tornar público tal vazamento, o que foi denunciado pelo *Wall Street Journal*, no mês de outubro do mesmo ano (MACMILLAN; MCMILLAN, 2018). Essas decisões podem dizer bastante sobre o posicionamento adotado pela sociedade empresária, em relação aos dados pessoais de seus usuários e aos problemas que pode ter a partir de vazamentos como este, situações em que deve escolher entre o lucro e a proteção dos dados de milhares de pessoas.

[40] De acordo com as "diretrizes da OCDE, Encriptação e Criptografia são definidas da seguinte forma: 'Encriptação' significa a transformação de dados pelo uso de criptografia para produzir dados ininteligíveis (dados encriptados) para garantir sua confidencialidade. 'Criptografia' significa a disciplina que incorpora princípios, meios e métodos para a transformação de dados a fim de ocultar seu conteúdo informativo, estabelecer sua autenticidade, impedir a sua modificação não detectada, impedir o seu repúdio e/ou impedir o seu uso não autorizado" (SCHULZ; VAN HOBOKEN, 2016, p. 11).

No que diz respeito à vigilância governamental e à divulgação de dados para cumprimento legal ou fins judiciais, a *Google* afirma compartilhar informações, caso acredite ser necessário para cumprir legislação, regulação, processo legal ou solicitação governamental aplicável; para cumprir Termos de Serviços aplicáveis, inclusive para investigação de possíveis violações; para detectar, impedir ou lidar com fraudes, problemas técnicos ou de segurança; para proteger de prejuízos a direitos, à propriedade ou à segurança da *Google*, de seus usuários ou do público, conforme solicitado ou permitido por lei (Q19). Nesse sentido, a *Google* possui um informe chamado *Transparency Report* que traz o número e o tipo de solicitações de compartilhamento de dados que recebe dos governos.

Apesar de disponibilizar esse relatório, a questão da vigilância governamental no que diz respeito a crianças e adolescentes é algo que merece destaque. Isso porque o *YouTube*, como dito anteriormente, faz parte da *Google*, que coleta dados do usuário das mais diversas maneiras, os compartilha com os mais diversos parceiros e deles recebe também dados, que juntos formam o perfil individual de cada usuário. Nesse sentido, essas empresas possuem hoje um verdadeiro dossiê de cada passo dado por qualquer pessoa na internet, contendo todos os termos buscados no *YouTube* e no buscador *Google*, todas as fotos enviadas, todos os locais em que a pessoa já esteve, com data e horário, todos os dados fornecidos a aplicativos, além de terem acesso à *webcam* e ao microfone do usuário[41]. As empresas de tecnologia possuem a capacidade de fazer hoje aquilo que qualquer governo sempre quis: ter acesso a cada ação e pensamento de seus cidadãos. O fato de a *Google* divulgar em um relatório de quais foram as suas contribuições aos governos não autoriza, automaticamente, o ato, principalmente devido ao fato de o Brasil, atualmente, encontrar-se sem uma Autoridade de Proteção de Dados competente e independente para realizar esse tipo de controle.

No caso de crianças e adolescentes atuais, que já nasceram conectados à internet, seus dados têm sido coletados desde o berço e os sensores que os coletam estão cada vez mais comuns em suas casas, presentes desde a assistente virtual utilizada por seus pais até seu urso de pelúcia favorito (caracterizando a *Internet of Things*, especialmente a *Internet of Toys*). Sendo assim, elas são muito mais vulneráveis a este rastro digital e possuirão muito mais dados que os adultos de hoje, quando chegarem à sua idade. Dessa maneira, se não bastasse o acesso a toda a vida da criança e do adolescente para a criação da publicidade direcionada e para outros fins mercadológicos, a mera possibilidade de cooperação da *Google* com

[41] Destaca-se o experimento feito por Curran (2018) que, ao fazer o *download* de todos os dados que a *Google* possuía de sua pessoa, recebeu um verdadeiro diário cronológico de sua vida nos últimos 10 anos, o que correspondia a aproximadamente 400.000 documentos em formato *word* (600MB).

governos, sem um controle mais restrito, coloca em xeque diversos outros direitos e faz com que a vigilância estatal chegue a dimensões nunca antes imaginadas, caracterizando verdadeira distopia de um Estado onipresente e onisciente, que poderá utilizar dados para a manipulação democrática e para violar direitos[42].

Relativamente às questões mais específicas sobre o uso da plataforma por crianças e adolescentes, o *YouTube*, em seus Termos de Serviço, exige que o usuário tenha 18 anos, seja emancipado ou tenha autorização legal dos pais ou dos tutores para consentir com o termos. Afirma, ainda, que a plataforma não foi desenvolvida para menores de 18 anos e que estes não devem utilizá-la (Q20). Tendo em vista que o *YouTube* não permite a utilização, através dos seus Termos de Serviço, da plataforma por menores de idade, não há a possibilidade de criação de contas específicas para crianças. Menores de idade podem utilizar, todavia, o aplicativo *YouTube Kids* para *tablets* e *smartphones* (Q21). Destaca-se, ainda, que a plataforma impede que usuários utilizem contas de terceiros sem permissão e afirma pela necessidade da veracidade dos dados inseridos na conta (Q22), de maneira que crianças e adolescentes não poderiam mentir ao informar a idade, nem utilizar a conta de seus pais ou responsáveis sem a sua permissão.

Nesse segmento, apesar de ser notório o fato de que crianças e adolescentes utilizam o *YouTube* para diversas funções, este se exime de qualquer responsabilidade de seu uso por essas pessoas, terceirizando-a exclusivamente aos pais ou responsáveis. Todavia, como dito no tópico anterior, a quantidade de *youtubers* mirins e de canais voltados para crianças e adolescentes cresce a cada dia, assim como a quantidade de crianças e adolescentes usuários do *YouTube*, o que prova a maciça presença deste público na rede social, apesar das restrições.

Destaca-se ainda que, estando o uso da plataforma por crianças e adolescentes vinculado à autorização legal de seus pais ou responsáveis, ela não menciona qualquer mecanismo de checagem acerca do consentimento ou desta autorização (Q25). Isso acaba por ir contra o art. 14 §1º, da LGPD, que exige um consentimento específico e em destaque dado pelo responsável legal (BRASIL, 2018) e contra o art. 8.º, 2, do RGPD, que exige da plataforma todos os esforços necessários adequados para verificar se o consentimento foi realmente prestado (UNIÃO EUROPEIA, 2016b).

[42] Nessa perspectiva, vale destacar uma experiência recente da China, que tem desenvolvido "um sistema de classificação e hierarquização social a partir dos dados pessoais que os cidadãos entregaram às aplicações móveis. E essa pontuação pode determinar o acesso ao emprego, o lugar num comboio ou até a descoberta de um parceiro sexual" (GUERREIRO, 2018).

Em relação ao documento referente à parte analisada das Diretrizes da Comunidade do *YouTube*, apesar de não responder diretamente às questões propostas neste trabalho, traz algumas reflexões específicas no que diz respeito à relação entre o *YouTube* e os menores de idade. Cabe salientar que o *YouTube* reforça que é uma prioridade sua o bem-estar físico e emocional destes usuários em sua plataforma (GOOGLE INC., 2018d), o que demonstra que a ele está ciente de seu uso cotidiano por crianças e adolescentes. Nesse sentido, reforça a existência da possibilidade de se inserir restrição de idade em vídeos e da necessidade de se respeitar a legislação trabalhista no que se refere ao trabalho infantil (GOOGLE INC., 2018d), discussão advinda, principalmente, do uso profissional da plataforma por *youtubers* mirins. No mesmo tópico, o *YouTube* afirma que, quando há propaganda no vídeo, o usuário que fez seu *upload* deverá avisar que este contém promoção paga, o que confirma que a plataforma também está ciente de seu uso para propaganda direcionada a crianças e adolescentes (GOOGLE INC., 2018d).

Em tópico denominado "Recursos para os pais", o *YouTube* assevera que sua plataforma não deverá ser utilizada por crianças e adolescentes e, ao mesmo tempo, incentiva que pais ou responsáveis assistam a vídeos juntamente com os menores no *YouTube* (GOOGLE INC., 2018c). A plataforma indica, também, que os pais e responsáveis visitem regularmente os canais de seus filhos, para saber sobre o conteúdo postado por eles e que denunciem violações de privacidade, caso as verifiquem (GOOGLE INC., 2018c). Destaca-se, por fim, que, no tópico denominado "Recursos para educadores" (GOOGLE INC., 2018b), o *YouTube* dá dicas para que professores ensinem alunos com mais de 13 anos assuntos como "Como serem membros responsáveis da comunidade do YouTube". Em suma, percebe-se, minimamente, um comportamento conflitante acerca do que a plataforma permite e o que ela incentiva.

A partir da descrição dos documentos de consentimento obrigatório para o uso do sítio eletrônico do *YouTube*, bem como para o uso do aplicativo do *YouTube Kids*, este capítulo pretendeu apresentar os dados conhecidos coletados para a presente investigação. Esses dados conhecidos serão utilizados para a realização de inferências no próximo capítulo, em que serão discutidos os resultados encontrados, serão apresentadas implicações observáveis e será controlada uma hipótese rival.

5 DISCUSSÃO DE RESULTADOS

Como pôde ser observado na descrição dos dados coletados no capítulo 4, a análise de conteúdo e de forma dos contratos eletrônicos não é algo trivial e deve levar em consideração as próprias características extrínsecas do documento, que delimitarão a maneira de interpretá-lo. Assim, propõe-se agora uma síntese dos resultados encontrados, na tentativa de analisar a questão de uma perspectiva mais ampla e responder à pergunta de pesquisa proposta inicialmente.

Com relação à análise preliminar e à forma do documento, após descrever seu contexto e quem são seus atores, percebeu-se que os documentos fazem parte da expressão da própria sociedade empresária e que, por isso, deveriam ser contrapostos a fatos da realidade, com o objetivo de contrabalancear o viés neles embutido. Após ser verificada a autenticidade e confiabilidade dos documentos, iniciou-se uma análise de seus elementos estruturais.

Averiguou-se que todos os documentos possuem natureza jurídica, por formalizarem o vínculo entre o usuário e o *YouTube* e que poderiam ser encontrados na página inicial do sítio eletrônico, exceto o Aviso de Privacidade do *YouTube Kids*, que foi encontrado na página de ajuda da *Google*. Apesar de possuírem a mesma natureza, verificou-se que os documentos variam em relação à linguagem, formato e tamanho. Destaca-se que o uso de linguagem estritamente formal, com jargões que podem não ser de conhecimento de todos e com expressões vagas em alguns dos documentos podem comprometer o seu entendimento e a pré-disposição de leitura por parte dos usuários, principalmente quando se trata de crianças e adolescentes.

No que diz respeito ao conteúdo, de maneira geral, nos documentos de consentimento obrigatório, nota-se que a *Google* e, mais especificamente, o *YouTube*, são transparentes no que concerne à relação de dados que coletam e à finalidade para a qual são utilizados. Da mesma forma, o usuário tem seu direito de acesso a seus dados satisfeito, assim como seu direito à portabilidade. A plataforma também permite a exclusão total ou parcial dos dados dos usuários, algo essencial para contemplar o direito ao apagamento, todavia os reveses em relação ao comportamento da sociedade empresária começam a aparecer neste ponto. Como foi verificado, mesmo após o pedido de exclusão de dados, ela afirma manter dados para fins legais ou econômicos, sendo este último não permitido pela legislação brasileira, nem pelo RGPD, e capaz de trazer diversos problemas para a vida adulta de crianças e adolescentes, como foi anteriormente discutido.

A rede social também não afirma minimizar a coleta de dados de crianças e adolescentes, nem no sítio eletrônico comum do *YouTube*, nem mesmo no aplicativo *YouTube Kids*, esse último voltado especificamente para este público e, por isso, estando em desacordo com o art. 14 da LGPD (BRASIL, 2018). Mesmo permitindo "customizar" as preferências de privacidade, verificou-se que isso, por vezes pode ser enganoso e trabalhoso para o usuário. De igual modo, a plataforma não tem um tratamento diferenciado dos dados de crianças e adolescentes, sendo estes tratados e coletados da mesma forma que dados de adultos, tanto no *YouTube*, quanto no *YouTube Kids*. Os dados são utilizados, inclusive, para a propaganda direcionada a este público, algo proibido no Brasil. Similarmente, a rede social não possui mecanismos de checagem do consentimento sobre o compartilhamento de dados de crianças e adolescentes por seus pais.

Destaca-se também a contradição existente entre diversos termos no documento que dizem respeito a mudanças futuras no contrato. Mesmo durante o período de *vacatio legis* da LGPD, a transparência, a necessidade de segurança jurídica e a boa fé contratual dentro da relação consumerista já seriam suficientes para rechaçar comportamentos como o observado. Controversa também é a abrangência de coleta e compartilhamento de dados do usuário por parte da plataforma. Os dados são coletados das mais diversas fontes e dispositivos e também são compartilhados com diversos parceiros, criando o rastro digital individual, algo bastante perverso na vida de crianças e adolescentes. Isso se torna ainda mais perigoso quando se trata de compartilhamento de dados com governos. Evidencia-se, ainda, a segurança dos dados dos usuários nos servidores da *Google*, algo que foi contestado com notícias de vazamento que não foram notificadas aos usuários em tempo razoável.

Por fim, no que diz respeito às Diretrizes da Comunidade, depreende-se do documento que o *YouTube* tem consciência do uso de sua plataforma por crianças e adolescentes – tanto como *youtubers* quanto como espectadores - através das medidas de segurança por ele indicadas, da necessidade de se colocar restrição de idade nos vídeos e de se respeitar a legislação trabalhista quando o *YouTube* se torna meio de trabalho de crianças e adolescentes. Nesse mesmo documento, a plataforma relembra a necessidade de aviso de promoção paga, mesmo quando são vídeos voltados a menores de idade. Percebe-se, também, no comportamento da sociedade empresária, uma conduta incoerente, ao se afirmar em diversos momentos que a plataforma não é adequada a crianças e adolescentes e, ao mesmo tempo, incentivar que pais e responsáveis a utilizem junto com eles e que educadores ensinem maiores de 13 anos como utilizá-la.

Diante do tratamento dos dados de crianças e adolescentes por parte do *YouTube*, verifica-se que a privacidade como "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (RODOTÀ, 2008, p. 15) não está sendo plenamente observada. De fato, crianças e adolescentes estão tendo seus dados coletados como se fossem adultos e sua vulnerabilidade mobilizada para interesses financeiros, não respeitando diversos dos princípios acima discutidos. Nesse sentido, nem a criança ou o adolescente, nem seus pais possuem o verdadeiro controle de seus dados pessoais, que fazem parte do que Rodotà (2004) chama de "corpo eletrônico".

Segundo Rodotà (2004), é imperativo pensar a integridade não mais somente em seu aspecto físico, vez que o corpo eletrônico – "decomponível, passível de ser disseminado multiplicável, manipulável, falsificável" (RODOTÀ, 2004, p. 106) – torna possíveis novas formas de controle, o que exige garantias mais eficazes. Essa necessidade de reinterpretação do que é a integridade e de como isso está ligado à dignidade humana é reforçada por Floridi (2014), que considera cada indivíduo como constituído por suas informações e, portanto, entende uma violação de sua privacidade informacional como uma forma de agressão à sua identidade pessoal.

Essa interpretação autoconstituinte acentua a relação entre a construção da identidade e a privacidade, que dá ao indivíduo a possibilidade de formar e moldar quem ele quer ser, todos os dias. Nesse sentido, ao se considerar crianças e adolescentes como pessoas em formação, a privacidade e a proteção de dados é fundamental para que elas se enxerguem no mundo e entendam quem elas são de verdade: não um corpo-mercadoria, mas sim pessoas únicas em construção. Tendo essa visão de privacidade e proteção de dados como base, bem como o princípio da proteção integral da criança e do adolescente no ordenamento brasileiro, é imprescindível que as TIC digitais passem a ser utilizadas não para reduzir o atrito ontológico da infosfera, mas para aumentar a privacidade informacional, ao reontologizarem a própria natureza da infosfera.

A privacidade e a proteção de dados pessoais são direitos fundamentais autônomos e são ferramentas essenciais para o livre desenvolvimento da personalidade (RODOTÀ, 2008). Assim sendo, o direito à proteção de dados deve ser tratado como direito de personalidade e não como um direito de propriedade, de modo que as salvaguardas devem ser pensadas a partir dessa característica, principalmente no que diz respeito aos dados sensíveis (RODOTÀ, 2008). O controle dos próprios dados pessoais serve, portanto, não apenas como instrumento para garantir a exatidão e o uso correto das informações da cada um, mas também para equilibrar a nova distribuição de poder que se delineia na sociedade atual (RODOTÀ, 2008).

É justamente por ter esse papel de equilibrar poderes dentro de uma sociedade que esse controle deve ser dilatado à dimensão coletiva, na qual não se leva em conta somente a proteção do indivíduo como tal, mas como pertencente a um grupo (RODOTÀ, 2008). Assim, fazendo parte de uma comunidade e assumindo a necessidade da alteridade para o desenvolvimento humano, o indivíduo, como tal, não existe, mas sim coexiste, juntamente com outros indivíduos (BODIN DE MORAES, 2008).

Diante do exposto, infere-se, a partir dos dados coletados nesta pesquisa, que a *Google*, a partir da rede social *YouTube*, não tem adotado medidas protetivas à privacidade e à proteção de dados de crianças e adolescentes e vários indícios levam a crer que este é um comportamento comum entre as redes sociais que mais coletam e processam dados deste público. Ao contrário, esses dados têm sido tratados de maneira proprietária, assumindo-se as partes do corpo eletrônico como objetos de troca e utilizando-se de contratos repletos de irregularidades para autorizar tal atitude. Desconsidera-se a necessidade de um controle efetivo e democrático por parte do usuário, algo essencial para que este molde sua identidade. Nesse sentido, verifica-se que a hipótese inicial deste trabalho foi corroborada. Os efeitos do tratamento dos dados de crianças e adolescentes como propriedade foram delineados ao longo do trabalho e, caso não sejam discutidos pela sociedade como um todo, podem se agravar cada vez mais.

É diante de situações como esta que Rodotà (2008, p. 21) relembra a importância de não deixar que o direito à proteção de dados seja salvaguardado por entes privados, uma vez que estes "tenderão a oferecer garantias que convenham a seus interesses". Mesmo que o sítio eletrônico *YouTube* não seja adequado para menores de idade, como o *YouTube* dispõe em seus Termos de Uso, o fato é que ele aufere lucro com todos esses acessos e, portanto, não tem interesse em uma abordagem preventiva e protetiva dos direitos das crianças e adolescentes.

Como disposto anteriormente, 48 dos 100 canais de maior audiência da plataforma são voltados para crianças e, dos 230 canais analisados em sua investigação, Correa (2016) verificou que os 110 canais infantis tinham quase 50 bilhões de visualizações, contra pouco mais de 2 bilhões dos 120 canais restantes. Sendo assim, eximir-se de sua responsabilidade com termos abusivos e continuar a coletar e processar dados de crianças e adolescentes como se fossem adultos pode ser um forte indício de que a exploração dos dados dessas pessoas e sua abordagem privatistica é lucrativa para a sociedade empresária[43]. Isso é ainda mais grave

[43] Outro indicativo do lucro da sociedade empresária com crianças e adolescentes é o fato de o *youtuber* mais bem pago do mundo em 2018 ter sido Ryan, de 7 anos, do canal Ryan *ToysReview* (JOHNSTON, 2018). Ryan,

no que diz respeito ao *YouTube Kids* que, sendo um aplicativo específico para menores de idade, não difere o tratamento de dados substancialmente daquele feito a partir do sítio eletrônico *YouTube*. Ao que parece, portanto, o aplicativo é apenas mais uma forma de aliciar este público desde cedo.

Essa inferência pode ser comprovada também por contraste, ao se verificar que o *YouTube* não permite alguns vídeos que tenham em seu conteúdo armas de fogo, conteúdo sexual explícito, spam etc., o que está descrito em suas Diretrizes da Comunidade, no tópico "Políticas, denúncias e aplicação de políticas". Todavia, apesar de não ser permitido pela legislação brasileira, a sociedade empresária deixa, por exemplo, que conteúdos publicitários direcionados a crianças e adolescentes circulem livremente na plataforma, isto é, ela acaba por selecionar o que é permitido ou não segundo seus próprios interesses.

Nesse sentido, diante da necessidade inexorável do uso da internet e das redes sociais por crianças e adolescentes para poderem concretizar os mais diferentes direitos no séc. XXI, é imperativo discutir esse uso em sociedade, considerando a atuação de todos os atores interessados. Não é mais possível ignorar o uso dessas ferramentas por essas pessoas e proibi-las de utilizá-las a partir de um contrato eletrônico que não tem seus efeitos verificados na realidade. O Direito, principalmente aquele criado unilateralmente por uma das partes, não pode se afastar das condutas sociais daqueles que mais precisam de tutela e ignorar que o direito ao acesso à internet é, hoje, um direito fundamental, cuja concretização deve ter como pressuposto a necessidade de privacidade e de proteção de dados.

É neste cenário que a dignidade humana deve ser utilizada sempre como pressuposto axiológico, na tentativa de assegurar à pessoa "seu tratamento como um fim em si mesmo, e não como um meio a ser usado de forma arbitrária pela vontade dos outros" (BAIÃO, GONÇALVES, 2014, p. 5). A dignidade da pessoa humana, assim, não existe sem autonomia, sendo necessário assegurar ao indivíduo a possibilidade de autodeterminação, ou seja, "o direito de decidir os rumos da própria vida e de desenvolver livremente sua personalidade" (BAIÃO, GONÇALVES, 2014, p. 6). Todavia,

> a proteção da dignidade da pessoa humana não é sinônimo de retirada das instituições do espaço no qual o indivíduo se autodetermina; ao contrário, implica sua presença a fim de proporcionar aos indivíduos não apenas a liberdade de realizar escolhas existenciais fundamentais para o desenvolvimento da sua personalidade, mas também assegurar-lhes a maior autonomia possível, resguardando a liberdade de poder considerar e rever criticamente as razões dessas escolhas entre diferentes formas possíveis de desenvolvimento da pessoa, sem ter necessariamente de

---

que faz vídeos de críticas de brinquedos e possui 17 milhões de seguidores na plataforma, ganhou 22 milhões de dólares neste ano (JOHNSTON, 2018).

> permanecer dentro uma identidade particular cristalizada. (GIOVANNI, 2005, p. 405 apud BAIÃO; GONÇALVES, 2014, p. 8).

Desse modo, a dignidade precisa ser, além de reconhecida, tutelada, a fim de que existam possibilidades reais de que cada um viva em condições de dignidade plena, com possibilidades objetivas de decisão e escolha (BAIÃO, GONÇALVES, 2014). Não tutelar não significa, portanto, proporcionar mais liberdade ao indivíduo, já que a relação deste com as grandes coletoras e processadoras de dados é desigual. Em relação a crianças e adolescentes, essa situação é ainda de maior vulnerabilidade.

Diante dessas considerações, portanto, tratar dados como se fossem mercadorias, assumindo que estes fazem parte da própria personalidade humana, é tratar as próprias pessoas em uma lógica mercantil, isto é, como um meio e não como um fim em si mesmo. Através da análise da forma com que os dados de crianças e adolescentes têm sido tratos pelo *YouTube*, percebe-se que é justamente essa a abordagem a escolhida pela plataforma.

5.1 Hipótese rival: privacidade como propriedade

A partir da corroboração da hipótese inicial dessa investigação no tópico anterior, busca-se, neste item, controlar uma hipótese rival importante, qual seja, a da abordagem patrimonialista do direito de privacidade como necessária para protegê-lo. Aqui se focará nos argumentos aventados por Lessig (2002), porém argumentação análoga também pode ser encontrada em Schwartz (2004), Rees (2013) e Cloud (2017).

Lessig (2002) defende que a abordagem no âmbito da propriedade, em relação ao direito de privacidade (e, neste sentido, poder-se-ia estender, também, à proteção de dados), poderia ampliar a força retórica por trás desse direito. O autor argumenta que, assim como os detentores de direitos de *copyright* querem controlar quem acessa as informações protegidas, os indivíduos também querem controlar quem e quando se acessa suas informações (LESSIG, 2002). Nesse sentido, qualquer um com senso histórico acharia também estranho falar de patentes como propriedade, visto que estas, anteriormente, eram vistas como direitos de exclusividade garantidos pelo governo a partir de um propósito público (LESSIG, 2002). Essa, porém, não é a forma como as patentes são vistas hoje e são, por isso, bem protegidas a partir de diversos recursos sociais que poderiam ser utilizadas para a proteção da privacidade (LESSIG, 2002).

O autor segue com outro exemplo para ilustrar seu ponto, a partir da mudança dos Termos de Uso pela *Amazon*, no ano 2000, que definiu a possibilidade de alienação dos dados de seus clientes a outros parceiros. Ele cita a possibilidade de, em um contrato de depósito em um estacionamento, estar prevista uma cláusula de que este contrato poderá ser modificado a qualquer tempo pelo gerente. Ao chegar para buscar seu carro, o cliente se depara com a argumentação do gerente de que os termos mudaram enquanto ele estava fora e que, agora, os carros do estacionamento passariam a ser vendidos. Em uma lógica proprietária, essa seria uma ideia absurda e, portanto, uma vez que não se pensa em privacidade e proteção de dados nesta lógica, a mudança de termos de uso pela *Amazon* não é vista com tanto choque por seus clientes. Assim, falar de propriedade seria um recurso retórico robusto, principalmente no que concerne à cultura americana (LESSIG, 2002).

Com base nessa argumentação, pode-se depreender alguns pressupostos a serem refutados. Primeiramente, o autor assume a privacidade como uma questão individual. Isso é evidenciado quando o autor, ao dizer que seu argumento é regularmente refutado por ser um fator de isolamento de indivíduos, afirma que, no contexto da privacidade, esse é o objetivo: empoderar indivíduos para que estes escolham estar isolados (LESSIG, 2002). Isso tem relação com a própria definição de privacidade que, atualmente, é vista por Rodotà (2008) e Floridi (2004, 2005, 2014) como direito autodeterminativo e não mais como o direito a estar só. Como discutido anteriormente, o indivíduo não vive de maneira isolada e os dados hoje só tem a força econômica que têm, pois são utilizados em massa. Nesse sentido, é inegável a necessidade de um tratamento coletivo da privacidade, que enxergue o indivíduo e suas informações como pertencente a um grupo. A partir desse entendimento, a dignidade da pessoa de cada indivíduo, a partir da tutela de sua privacidade, só pode ser protegida se os dados de seus pares também o forem. Isso é especialmente verdade em relação a crianças e a adolescentes que necessitam de proteção especial como uma parte vulnerável da comunidade.

Em segundo lugar, ter a propriedade de informações poderia gerar diversos problemas em relação à necessidade da circulação de informações dentro de uma sociedade democrática. O acesso a dados está diretamente ligado ao direito à informação, de maneira que a distinção entre as disciplinas da proteção de dados e do acesso à informação é meramente formal: onde houver maior circulação de informações é onde deve haver maior possibilidade de controle (RODOTÀ, 2008). Dentro de uma sociedade democrática, o direito à informação é um instrumento importante, que tem a capacidade de determinar formas de redistribuição de poder (RODOTÀ, 2008), principalmente quando se trata de informações necessárias à tomada de decisões, estando elas em mãos públicas ou privadas. Nesse cenário, o sigilo decorrente da

propriedade acaba por ser contrário à publicidade, algo que não ocorre com o controle de informações (RODOTÀ, 2008). Destaca-se, porém, que Lessig (2002) propõe a necessidade de o direito à privacidade como propriedade ser regulado, o que poderia mitigar o problema narrado neste parágrafo.

Em terceiro lugar, essa interpretação ainda corresponde à visão da privacidade como direito burguês, isto é, como um privilégio de uma minoria. Isso, porque se se permite a definição de dados como propriedade, poderia haver uma alienação em massa da privacidade, o que geraria cada vez mais desigualdades e problemas de classe. A partir dessa perspectiva, só teriam seus direitos concretizados aqueles que pudessem pagar por eles, sem que seus dados fossem utilizados para outras finalidades o que, ao se assumir a necessidade de igualdade social, não teria assento em um Estado Democrático de Direito. Ao ser confrontado com esse aumento de alienação do direito de privacidade, Lessig (2002) contesta que a essência do direito de propriedade é a de que a pessoa que o deseja deve negociar com seu detentor antes de o possuir, de maneira que tornar a privacidade um direito de propriedade faria com que se reforçasse o direito individual de recusar a alienação de sua privacidade e de escolher o quanto gostaria de alienar. O mesmo é defendido por Schwartz (2004), que tenta mostrar como o fato de tornar informações pessoais uma propriedade pode responder à falha do mercado de privacidade atual.

Diante dessas respostas, percebe-se que os autores acreditam na igualdade entre as partes na negociação contratual o que, como discutido anteriormente, não é necessariamente verdadeiro. “O usuário de serviços informáticos e telemáticos se encontra em tal situação de disparidade de poder em relação aos fornecedores de serviços que, a rigor, não se pode falar em consentimento livremente manifestado para transações referentes à privacidade” (RODOTÀ, 2008, p. 52-53). Dentro de um cenário de oligopólio de sociedades empresárias na internet, não é razoável exigir que o usuário simplesmente não utilize as redes sociais, o *YouTube* ou o buscador da *Google*. Igualmente, tendo em vista o fator adesão do contrato, também não é permitido ao usuário negociar seus termos. Assim, não há igualdade entre as maiores empresas de tecnologia e o usuário e, por esse motivo, há a necessidade de tratar o tema em comunidade. O problema, portanto, não é somente como o mercado lida com essas informações, mas a própria negociação de informações pessoais dentro do mercado, que transforma o corpo eletrônico em mercadoria.

O autor também questiona o que ele chama de paternalismo em relação à proteção dos usuários, que seriam protegidos de compartilhar mais do que eles “deveriam” (LESSIG, 2002). Lessig (2002) afirma que não era possível saber, à época do desenvolvimento desta

teoria, se a quantidade de dados a ser alienada seria maior do que se "deveria", posto que os perigos que a internet poderia criar em relação aos dados pessoais ainda eram incertos. De fato, no estágio em que a internet se encontrava em 2002, não se vislumbrava, ainda, o *Big Data* e todos os perigos que isso poderia gerar nas vidas das pessoas. Atualmente, porém, esse já é um fato notório e o que ocorre, na realidade, não é um somente um chamado *oversharing*, isto é, um compartilhamento maior do que o necessário pelo usuário, mas também o uso desses dados em massa para fins secundários pelas empresas de tecnologia. Como dito anteriormente, a regulação como direito de personalidade é necessária a fim de que a dignidade de todos os usuários seja respeitada, garantindo a possibilidade de uma escolha livre, principalmente no que diz respeito àqueles mais vulneráveis.

Diante dessa discussão, não é necessário que a privacidade seja tratada como propriedade para que seja mais bem tutelada ou que tenha uma força retórica mais robusta. Principalmente no Brasil, em que a educação digital anda a passos lentos, a falta de um conhecimento mínimo sobre como os dados são utilizados pelas empresas e sobre as consequências desse uso é um fator extremamente importante em relação ao valor dado às próprias informações por essas pessoas.

De igual modo, considerar a privacidade e a proteção de dados como direitos de personalidade não implica na falta de possibilidades de cobrar pela violação desses direitos. No momento em que se verifica lesões a esses direitos, a repercussão no conteúdo patrimonial do lesado pode ser mobilizada, gerando indenização ou reparação (BAIÃO, GONÇALVES, 2014). "Nesse viés, portanto, o patrimônio é composto não apenas por relações jurídicas economicamente apreciáveis, mas também por relações de caráter extrapatrimonial, que ao serem violados podem tomar parte no patrimônio do indivíduo" (BAIÃO, GONÇALVES, 2014, p. 11).

Por fim, ressalta-se, ainda, o custo de se manter a proteção dos dados pessoais e da privacidade no campo individual e da propriedade. Isso foi aventado, inclusive, por Lessig (2002), que mitiga seus argumentos a partir da assunção de que um tal sistema de proteção poderia ter seus custos excedendo seus benefícios. Isso é especialmente válido quando se trata de obras ou, no caso, de dados, que circulam na internet. O controle de obras com copyright na internet tem se mostrado desafiador, em razão de sua imaterialidade, de modo que "os mecanismos de criação artificial de escassez desenvolvidos pela indústria (como a inclusão de travas anticópia) se provaram tão caros quanto ineficientes" (BRANCO, BRITTO, 2013).

5.2 Desdobramentos de governança para uma rede segura para crianças e adolescentes

O objetivo deste trabalho foi investigar como os dados de crianças e adolescentes têm sido tratados (coletados e processados) pelo *YouTube*, ou seja, traçar um diagnóstico da situação brasileira, no que tange à forma de tratamento dos dados e de seus efeitos, o que foi endereçado nas seções anteriores. Nesta seção, tratar-se-á tanto de desdobramentos da teoria aventada na seção anterior (implicações observáveis) tanto de alternativas ao modelo proprietário que têm sido discutidas atualmente.

Nesse sentido, sendo as crianças e os adolescentes considerados pessoas em desenvolvimento, o ordenamento jurídico concede a eles uma tutela especial. A tutela integral da criança e do adolescente é o princípio pelo qual "a invisibilidade social do menor cedeu lugar ao princípio do melhor interesse da criança, elemento norteador das decisões que lhes dizem respeito" (MENEZES; BODIN DE MORAES, p. 527). Ela representa, portanto, um princípio hermenêutico necessário devido a um "conjunto de pressupostos de entendimentos que são sintetizados pelas noções de vulnerabilidade e desenvolvimento como caracterizadores da peculiaridade do estado infantil" (SÊCO, 2014, p. 11). Nesse sentido, Sêco (2014) propõe que o princípio do melhor interesse da criança, abarcado por essa tutela especial, seja entendido a partir do modelo de triangulação de perspectivas. Nessa visão de proteção à criança e ao adolescente, utiliza-se uma metáfora geométrica, em que em um dos vértices encontra-se a sociedade, por intermédio do Estado, no segundo a família e, no terceiro, a própria criança ou adolescente.

Evidencia-se a importância individual de cada parte nessa formação geométrica, assim como a necessidade de todos atuarem em conjunto, conforme determinou a CRFB, em seu art. 227, que estabelece como obrigação da família, do Estado e da sociedade, bem como do setor empresarial, assegurar a prioridade absoluta dos direitos de crianças e de adolescentes (BRASIL, 1988; HARTUNG; PITA, 2018). Isso faz com que as consequências da atuação dos três entes estejam sempre ligadas ao pressuposto da dignidade da pessoa humana e que as intervenções por parte do Estado, no que diz respeito à criança e ao adolescente, estejam sempre em função dos interesses destes (SÊCO, 2014), sem desconsiderar suas potencialidades e necessidades.

Em um cenário de mudanças tecnológicas e de instabilidade em relação ao direito de privacidade e de proteção de dados, essa atribuição de responsabilidades horizontal é ainda mais importante. Assim, deixar a proteção de crianças e adolescentes apenas na capacidade de "monitoramento" e de educação dos pais ou responsáveis, que tampouco tiveram uma

educação digital capaz de mitigar os efeitos adversos das novas tecnologias, não parece ser a melhor solução. Exemplo disso é a própria prática do *sharenting*, que consiste no hábito de os pais ou responsáveis postarem informações na internet sobre os menores que estão sob sua tutela (EBERLIN, 2017). Mesmo que a intenção não seja a de expor os menores, esses pais ou responsáveis postam informações e dados pessoais sobre eles, o que vai sendo utilizado para a criação de rastros digitais (EBERLIN, 2017). O *sharenting* também abarca situações em que os próprios pais ou responsáveis "fazem a gestão da vida digital de seus filhos na internet, criando perfis em nome das crianças [e dos adolescentes] em redes sociais e postando, constantemente, informações sobre sua rotina" [44] (EBERLIN, 2017, p. 258).

Além das práticas de *sharenting*, deve-se destacar que os pais também não têm pleno controle sobre as informações coletadas de seus filhos. Exemplo disso é a Internet das Coisas aplicada aos brinquedos (*Internet of Toys*), que promete uma experiência única no brincar, em que o brinquedo interage com a criança a partir de respostas individualizadas (LEAL, 2017). A despeito de a ideia parecer interessante de início, estes produtos têm sido questionados devido à fragilidade da privacidade e da segurança dos usuários. Essa fragilidade pode advir da invasão da rede a que o brinquedo se encontra conectado, do monitoramento constante da criança ou do adolescente, além da falta de transparência quanto ao uso dos dados coletados por estes brinquedos (LEAL, 2017). Mesmo que apenas o consentimento dos pais fosse eficiente na proteção dos filhos quando do uso desses brinquedos, diversas situações nebulosas podem ocorrer, como a utilização do brinquedo por outra criança, cujos pais não consentiram em seu uso (SOUZA, 2018).

Assim, exigir que os pais sejam unicamente responsáveis pelo que ocorre com os dados de seus filhos na internet é bastante controverso, vez que eles também não tiveram uma educação digital adequada para consentir livre e esclarecidamente com essas práticas e são os filhos, inclusive, que costumam ajudar os pais na manipulação das novas tecnologias[45]. Além disso, como exposto anteriormente, a arquitetura da internet e a forma com que esses contratos eletrônicos são apresentados aos usuários influenciam seu comportamento e, de maneira geral, fazem com que não sejam lidos.

Mesmo que os usuários lessem os documentos, isso tomaria grande parte de seu tempo: 76 dias por ano, em média (MADRIGAL, 2012) e a leitura não é uma garantia de que os usuários entenderiam estes termos. Em um estudo feito por Bashir et al. (2015)

[44] Ressalta-se que, entre as crianças e adolescentes que possuem um perfil em redes sociais, 27% criou junto com outra pessoa e 21% afirma que foi outra pessoa quem criou o perfil para eles (NIC.BR, 2015).
[45] Na pesquisa realizada pelo NIC.BR(2017), 76% dos adolescentes entrevistados concordou com a afirmação de que sabiam mais sobre a internet do que seus pais.

demonstrou-se que as pessoas em geral não possuem uma compreensão básica sobre o uso de nuvens de dados na internet, o que seria necessário para interpretar o significado desses termos. “Por exemplo, em uma das duas perguntas que questionavam sobre como os *sites* gratuitos ganham dinheiro, 44% dos entrevistados não sabia que os *sites* gratuitos poderiam lucrar com a venda de informações do usuário diretamente para as empresas de *marketing*” [46] (BASHIR et al., 2015, p. 5, tradução nossa, grifo nosso). Todavia, “66% dos entrevistados respondeu corretamente que as empresas de publicidade poderiam usar *e-mails* enviados e recebidos em contas de *webmail* gratuitas para personalizar anúncios” [47] (BASHIR et al., 2015, p. 5, tradução nossa, grifo nosso). Além disso,

> 68% (...) respondeu corretamente às perguntas sobre o que as empresas de publicidade on-line podem fazer para coletar informações pessoais sobre os usuários Esses padrões de resposta destacam uma deficiência de compreensão em relação ao comércio de dados para informações pessoais na Internet[48] (BASHIR et al., 2015, p. 5, tradução nossa).

Assim, “se os usuários não entendem o básico do *design* da tecnologia, como esperar deles um consentimento livre e esclarecido?” [49] (BASHIR et al., 2015, p. 5, tradução nossa). Ao mesmo tempo, 74% dos usuários entrevistados disseram se preocupar com a privacidade *online* e 77% com a segurança *online*, sendo estes influenciadores de seu comportamento (BASHIR et al., 2015). Essas respostas vão de encontro, porém, ao fato de que apenas 43% dos entrevistados indicaram que desistiram de utilizar um sítio eletrônico devido aos Termos de Uso ou à sua Política de Privacidade (BASHIR et al., 2015). “Essa discrepância é um indicativo do paradoxo da privacidade, que se refere a uma desconexão entre as preferências de privacidade do usuário e seu comportamento em relação à privacidade” [50] (NISSENBAUM, 2009 apud BASHIR et al., 2015, p. 7).

Deve-se questionar, também, se o trabalho de leitura destes contratos faz sentido no mundo atual. Aqueles que dependem, por diversos motivos, de serviços de empresas como a

---

[46] No original: “*For example, in one of the two questions that asked about how free websites make money, 44% of respondents did not know that free websites could profit by selling user information directly to marketing companies*” (BASHIR et al., 2015, p. 5).
[47] No original: “*66% of respondents correctly answered that advertising companies could use emails sent and received on free webmail accounts to personalize advertisements*” (BASHIR et al., 2015, p. 5).
[48] No original: “*68% of respondents correctly answered questions about what online advertising companies can do to collect personal information about users. These response patterns highlight a deficiency of comprehension in regard to the data trade for personal information on the Internet*” (BASHIR et al., 2015, p. 5).
[49] No original: “*This is problematic because if users do not understand the basics of the technology's design, how can they be expected to give informed consent?*” (BASHIR et al., 2015, p. 5)
[50] No original: “*This discrepancy is indicative of the ‘privacy paradox’, which refers to a disconnect between user preferences for privacy and user behavior in relation to privacy*” (NISSENBAUM, 2009 apud BASHIR et al., 2015, p. 7).

Google, *Facebook* e *Twitter* estariam mesmo em uma posição individual de negociar seu próprio contrato? Teriam eles real escolha entre aceitar ou não compartilhar seus dados? Dentro de um cenário de impossibilidade de mudança dos termos, qual o sentido de ler esses documentos?

Questiona-se, ainda, como essa abordagem deve ocorrer em relação a crianças e adolescentes. No Brasil, como já exposto, a idade de consentimento *online* foi definida como 12 anos. Assim, além da discussão sobre se o consentimento dos pais em relação aos menores de 12 anos é suficiente para a sua proteção, é essencial discutir se o consentimento dos adolescentes entre 12 e 17 anos pode ser considerado válido e protetivo.

Nesse sentido, Teixeira (2017, p. 3) dispõe que "o diálogo entre o regime das incapacidades e o exercício da autoridade parental deve ser no sentido de proteção e promoção do livre desenvolvimento da personalidade dos filhos". Isso ocorre, pois os pais seriam titulares de um "poder jurídico" sobre os filhos, revelado através de um conjunto de deveres, com um "fim exclusivo de permitir ou facilitar o cumprimento desses deveres. Assim, os pais devem exercer o poder familiar exclusivamente no interesse do filho" (BARBOZA, 2005, p. 131).

Quando o equilíbrio no espaço familiar é quebrado, excepcionalmente, este deverá sofrer ingerências estatais para proteger sujeitos familiares vulneráveis, "denotando como marca do Estado Democrático de Direito a busca por igualdade material, obtida pela conformação da autonomia privada por preceitos de solidariedade" (TEIXEIRA, 2017, p. 2). Neste caso específico, o equilíbrio é afetado pelas novas tecnologias, que desafiam a capacidade de proteção e decisão dos pais ou responsáveis pelas crianças, como já discutido anteriormente. Apesar de a heterodeterminação do Estado, em relação ao melhor interesse do menor, somente se justificar em casos excepcionais (MENEZES; MULTEDO, 2016), essa situação específica parece representar um perigo particular à proteção de dados das crianças e dos adolescentes e, portanto, deve ser tratada como tal.

A discussão deve ser ainda mais intensa no que tange aos interesses dos adolescentes, entre 12 e 17 anos, que poderão não ter a assistência parental para o consentimento na internet. Nesse sentido,

> é louvável a atribuição de validade à vontade da criança e do adolescente para a prática de atos existenciais, principalmente em razão da dificuldade funcional de se separar titularidade de exercício de direitos da personalidade. Todavia, deve-se levar em consideração o estágio de desenvolvimento e maturidade em que o menor se encontra, a fim de se verificar qualitativamente os tipos de atos que ele pode expressar, de forma a implementar o seu melhor interesse. A autonomia a ser protegida, portanto, é a autonomia responsável, que mede e suporta as

> consequências dos seus atos. Por isso, a tutela da criança e do adolescente que protege e promove seus melhores interesses existenciais deve ser balizada pela investigação do seu discernimento, do estágio de completude do seu desenvolvimento cognitivo (KONDER; TEIXEIRA, 2016).

No caso dessas pessoas, apesar de a discussão da flexibilização dos efeitos da incapacidade ser fundamental, assim como a necessidade de se levar em conta o discernimento, ou seja, "a capacidade para compreender o ato praticado e suas consequências" (NEVARES; SCHREIBER, 2016), o consumo em massa de produtos e serviços que demandam o consentimento em contratos eletrônicos fazem com que essa análise particular seja dificultada, mesmo porque se trata de contratos de adesão. Não há neste caso, portanto, a atribuição de uma autonomia responsável e de acordo com o melhor interesse deste adolescente.

Dessa forma, discutir a questão de maneira descontextualizada, sem a participação do menor e sem analisar a responsabilidade das empresas privadas e do próprio Estado, deixando toda a responsabilidade para os pais ou responsáveis é bastante problemático em um mundo fluido, em que as tecnologias de captação de dados podem ser encontradas em todo lugar. A criança ou o adolescente deve ser visto como um sujeito ativo "titular do direito de manifestar suas razões, crenças e pensamentos" (MENEZES; BODIN DE MORAES, p. 527) e o Estado deve ser colocado em sua função regulatória e sancionatória. O direito fundamental à proteção de dados deve ser interpretado, portanto, segundo essa condição especial da criança e do adolescente e, consequentemente, a educação digital, tanto em relação aos pais e aos responsáveis quanto em relação aos menores, deve ser uma política pública de prioridade.

Dentro dessa discussão, apesar de o consentimento ser um bom caminho entre a *regulation* e a *deregulation*, utilizá-lo como pilar de uma política de proteção de dados é bastante perigoso (RODOTÀ, 2008). Isso ocorre, pois o consentimento faz parte de uma perspectiva unidimensional, ligada à visão proprietária dos dados, que ignora a dimensão relacionada às consequências sociais e às consequências para o próprio interessado (RODOTÀ, 2008). A possibilidade de usufruir de certos serviços, importantes, inclusive, para concretizar direitos fundamentais como o direito à informação, ao lazer e à cultura tem dependido não somente do fornecimento de dados por parte do usuário, mas também do consentimento para a utilização secundária dessas informações (RODOTÀ, 2008). Assim, utilizar o consentimento em todos os casos não é a solução, principalmente no que concerne às relações de Direito Civil com partes vulneráveis, a fim de se limitar a possibilidade de se recorrer à lógica do mercado e negociar livremente dados pessoais (RODOTÀ, 2008). A partir

de uma análise do Direito como prática social, portanto, já não é mais possível culpar os usuários por aquilo que lhes torna vítimas de um sistema injusto.

Isto posto, a fim de suprir o *gap* de poder entre os "senhores" da informação e os indivíduos, Rodotà (2008) reforça o tratamento coletivo do problema.

> Para realizar esse objetivo, parece indispensável permitir um acesso "assistido" por especialistas, de forma a viabilizar não somente o conhecimento das informações pessoais referentes ao interessado, mas também os "critérios utilizados para os tratamentos automáticos" (como prevê o art. 3º da lei francesa de 1978). Ainda mais importante revela-se o reconhecimento de um direito de acesso individual "integrado" pela presença de um sujeito coletivo (sindicato, associação de direitos civis, associação de tutela dos consumidores, e assim por diante) (...) realizando assim um efetivo controle sobre os coletores das informações (RODOTÀ, 2008, p. 68).

Diante do exposto, um ambiente seguro na internet depende das ações de diversos atores políticos que, em conjunto, devem tomar medidas para incentivar a confiança da rede. Depende, também, de uma Autoridade de Proteção de dados independente, que possa fazer esse controle sem qualquer influência de governos ou de empresas. Soluções simplistas, baseadas apenas no consentimento do usuário, podem não ser suficientes e a governança na internet é essencial para promover uma rede de confiança, que seja uma alavanca e não um entrave para o desenvolvimento. Em um ambiente seguro, crianças e adolescentes se sentem livres para serem cidadãos do mundo virtual, hoje tão ou mais relevante que o mundo físico. Assim, a democracia é concretizada na sua mais abrangente forma e os direitos humanos podem se materializar também no mundo virtual.

Por fim, o papel das sociedades empresárias na prevenção também deve ser discutido. Como discutido anteriormente, o art. 227 da CRFB dispõe que é dever de toda a sociedade a consolidação dos direitos das crianças e dos adolescentes, o que inclui o setor privado (BRASIL, 1988). Isso deve ser enfatizado nos casos em que as próprias sociedades empresárias criam normas através da arquitetura virtual, o que afeta diretamente o comportamento dos usuários e que assim como é capaz de proteger direitos, é também capaz de violá-los, como argumentado por Floridi (2005, 2006, 2014). No caso de crianças e adolescentes esse papel está ligado diretamente ao princípio da prevenção, disposto na LGPD, em seu art. 6º, VIII. Nesse cenário, necessário se faz discutir o papel do sistema jurídico na regulação da atuação dessas sociedades empresárias, vez que ao se "compreender a capacidade e a complexidade envolvida nos códigos tecnológicos, as medidas regulatórias podem trazer novas perspectivas para que as legislações se atualizem aos novos tempos" (FERES, OLIVEIRA, 2017).

Diante desse cenário, é ilusório considerar que é possível uma intervenção única do Direito, sendo necessária uma gama articulada de medidas, que correspondem aos diversos níveis em que a tecnologia da informação já produz seus efeitos (RODOTÀ, 2008). É necessário individualizar princípios e associá-los a tendências de longo prazo, a fim de diminuir a sensação de distância entre "o velocíssimo mundo da inovação tecnológica e aquele lentíssimo do planejamento sócio-institucional" (RODOTÀ, 2008, p. 42). Isso tem sido endereçado, em certa medida, pelo Marco Civil da Internet e pela LGPD, no Brasil. Todavia, essa tendência terá de ser confirmada pela aplicação e pela jurisprudência decorrente da nova lei, a partir de fevereiro de 2020, bem como pela atuação da Autoridade de Proteção de Dados no Brasil, ainda a ser criada.

Mais uma vez, a perspectiva de fortalecimento apenas de uma defesa individual, como pode ser considerada a aposta em contratos eletrônicos mais acessíveis de maneira geral à população, continua sendo fundamental, mas é apenas um ponto de partida (RODOTÀ, 2008). Indivíduos e grupos precisam ser dotados de ferramentas que os possibilitem fazer valer essas garantias dinamicamente, para permitir "a transparência dos processos de decisão, [a] capacidade de controle difuso dos detentores do poder, [e a] possibilidade de fazer novas identidades coletivas", de maneira a exaltar as razões individuais e não invisibilizá-las (RODOTÀ, 2008, p. 58).

6 CONCLUSÃO

As TIC digitais, apesar de terem mudado a vida em sociedade, proporcionado diversos avanços sociais e possibilitado a concretização de diversos direitos, representam, hoje, um desafio à seara jurídica. Os serviços ofertados através da *Web 3.0*, que tem como principal característica a personalização do conteúdo para cada usuário, não são gratuitos: paga-se por eles através de dados, de pedaços do corpo eletrônico. O uso secundário dos dados permite a utilização de técnicas de *targeting* e *profiling*, que ajudarão na formação do perfil individual e social de cada usuário, e ao se saber tudo sobre o indivíduo é possível manipulá-lo, seja para fins comerciais, seja para fins políticos. Os dados são o novo petróleo e saber utilizá-los é saber ascender na escala de poder.

Nesse sentido, quanto mais dados se coleta de uma pessoa, mais fácil será o controle sobre sua vida. Assim, um alvo fácil dessa conduta são crianças e adolescentes que, desde a infância têm seus dados coletados e processados, a fim de serem influenciados todos os dias com informações que podem ser de "seu interesse". Essas pessoas da geração Z, ao mesmo tempo em que têm mais facilidade com as tecnologias, posto que já nasceram em um mundo hiperconectado, são também as mais afetadas, por estarem desde sempre nele inseridas.

Crianças e adolescentes aprendem através de estímulos e, considerando que a tecnologia não é neutra, uma vez que ela absorve todos os valores daqueles que a criaram, pode-se vislumbrar problemas, já que os estímulos tecnológicos contribuirão para a pessoa que eles irão se tornar. Assim, a forma com que os menores de idade estão aprendendo sobre o mundo, atualmente, os torna pessoas melhores e cidadãos para o mundo ou apenas os torna consumidores e partes de uma geração que teve sua subjetividade uniformizada pelo conteúdo advindo da internet?

Diante dessa inquietude, a presente investigação buscou compreender como os dados de crianças e adolescentes têm sido coletados e tratados pelo *YouTube*. Para conduzir este estudo e responder a este questionamento, escolheu-se analisar os contratos eletrônicos que mediam essa relação jurídica e permitem esse tipo de uso do corpo eletrônico para fins particulares e voltados ao lucro. Foi utilizada a pesquisa empírica, a partir das regras de inferência de Lee Epstein e Gary King, a fim de trazer replicabilidade, confiabilidade e validade para a pesquisa. Como técnicas de pesquisa, utilizou-se o estudo de caso, a partir de Robert Yin, estratégia abrangente e que permite a análise em profundidade de um caso, a fim de se elaborar teorias que poderão ser replicadas em outros casos. Também foi utilizada a técnica de análise documental, baseada em André Cellard, que pretende trazer maior

complexidade ao conteúdo do documento em questão ao se analisar elementos extrínsecos a este, como contexto, atores, linguagem etc., o que permite balizar a interpretação de seu conteúdo.

Enquanto referencial teórico utilizou-se a teoria desenvolvida por Stefano Rodotà, entendendo-se a privacidade como o direito de manter o controle sobre suas próprias informações e de se determinar a maneira de construir sua própria esfera particular. Essa concepção é harmônica à interpretação ontológica e autoconstituinte de privacidade informacional de Luciano Floridi, também adotada por este trabalho, que entende a privacidade como construção da própria identidade e defende a necessidade de que um esforço deve ser feito para que as TIC digitais não apenas violem, mas reforcem a privacidade informacional, a partir de uma reontologização da própria infosfera.

A partir das técnicas e referenciais teóricos apontados acima, foram analisados quatro documentos: os Termos de Uso, a Política de Privacidade, as Diretrizes da Comunidade e o Aviso de Privacidade do *YouTube Kids*. Estes documentos foram escolhidos por serem de consentimento obrigatório quando do uso do sítio eletrônico do *YouTube* (os três primeiros) e do aplicativo *YouTube Kids* (todos eles). Inicialmente, foi realizada uma análise preliminar, a partir dos passos desenvolvidos por Cellard (2008) e de perguntas acerca da forma dos documentos. Em um segundo momento, foi realizada uma análise conteudística desses documentos, a partir de questões desenvolvidas em um modelo de análise. O capítulo 4 foi utilizado para trazer as respostas dessa análise, isto é, os dados conhecidos da pesquisa.

No capítulo 5, discutiu-se os resultados dessa investigação e a hipótese inicial foi corroborada, qual seja, a de que o *YouTube* tem tratado os dados de crianças e adolescentes de maneira proprietária e desconsiderado a necessidade de se reforçar estruturas que permitam aos usuários moldarem suas identidades como agentes informacionais. Percebe-se que a plataforma vem desrespeitando a necessidade de um tratamento especial para crianças e adolescentes, presente em nosso ordenamento a partir do princípio do melhor interesse da criança e do adolescente, por serem pessoas vulneráveis e em desenvolvimento.

Mais uma vez destaca-se a necessidade de a dignidade humana ser utilizada como pressuposto axiológico, a fim de que esse público seja tratado como um fim em si mesmo e não como meio para a aferição de lucro a partir do uso secundário de seus dados. Os dados pessoais, como argumentado durante o trabalho, fazem parte da construção da própria identidade das crianças e dos adolescentes e a mercantilização do corpo eletrônico desde tenra idade pode trazer efeitos geracionais nunca antes experimentados.

Nesse mesmo capítulo, controlou-se e refutou-se uma hipótese rival, qual seja, a de que o tratamento privatistico da privacidade e da proteção de dados é uma boa forma de proteger esses direitos. Verificou-se que essa visão poderia ir contra a necessidade de um tratamento coletivo desses direitos, a circulação de informações dentro da sociedade, a necessidade de um tratamento igualitário entre os cidadãos e, finalmente demandaria um aparato custoso de proteção.

Por fim, após o diagnóstico proposto pela pergunta de pesquisa, no que se refere ao comportamento do *YouTube* e aos efeitos deste nas crianças e nos adolescentes brasileiros, discutiu-se, brevemente, desdobramentos de governança para uma rede segura para essas pessoas. Foi debatida a forma com que os contratos eletrônicos são apresentados aos usuários, atualmente, e o fato de que a proteção integral de crianças e adolescentes, nesse sentido, é deixada apenas aos pais e responsáveis, em uma política baseada no consentimento. Em um ordenamento que preza pelo princípio do melhor interesse da criança e do adolescente, que se consagra no art. 227 da CRFB, a participação de todos os atores da sociedade nessa proteção é fundamental, de maneira que uma discussão mais aprofundada acerca da responsabilidade das empresas de tecnologia, bem como da ingerência estatal nesses casos é imperativa. Isso poderia ser realizado, principalmente, através de uma política de educação digital, bem como da atuação ativa e independente de uma autoridade de proteção de dados na concretização das normas presentes no ordenamento brasileiro.

A privacidade e a proteção de dados são direitos fundamentais das crianças e dos adolescentes, que devem ser garantidos desde o seu nascimento, não devendo ser enxergados como um vir a ser, isto é, como algo a ser endereçado apenas quando estes se tornam adultos. Violar esses direitos é violar sua segurança, comprometer sua reputação, favorecer a discriminação e a datatificação da infância, bem como prejudicar seu livre desenvolvimento. Percebe-se, portanto, que o Brasil terá um grande desafio pela frente na aplicação e interpretação da LGPD, a fim de que esses direitos sejam, finalmente, concretizados.

REFERÊNCIAS

BAIÃO, Kelly C. Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**, [S.l.], v. 3, n. 2, p.1-24, 2014. Disponível em: <http://civilistica.com/wp-content/uploads/2015/02/Bai%C3%A3o-e-Gon%C3%A7alves-civilistica.com-a.3.n.2.2014.pdf>. Acesso em: 23 out. 2018.

BAGOST, Ian. My Cow Game Extracted Your Facebook Data. **The Atlantic.** [S.l.]. 22 mar. 2018. Disponível em: <https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/>. Acesso em: 06 jul. 2018.

BARBOZA, Heloiza Helena. Bioética e biodireito: quem defende os interesses da criança? In: BRAZ, Marlene; SCHRAMM, Fermin Roland. **Bioética e saúde:** novos rumos para mulheres e crianças? Rio de Janeiro: Fiocruz, 2005. p. 125-138.

BASHIR, Masooda et al. Online privacy and informed consent: The dilemma of information asymmetry. **Proceedings Of The Association For Information Science And Technology**, [s.l.], v. 52, n. 1, p.1-10, 2015.

BODIN DE MORAES, Maria Celina. Ampliando os direitos de personalidade. In: VIEIRA, José Ribas. **20 anos da constituição cidadã de 1988:** efetivação de impasse constitucional. Rio de Janeiro: Forense, 2008. p. 369-388.

BÖHME, Rainer; KÖPSELL, Stefan. Trained to Accept? A Field Experiment on Consent Dialogs. In: ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI), 2010, Atlanta. **Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.** Atlanta: Chi, 2010. p. 2403 - 2406.

BOYD, Danah. **It's complicated:** the social lives of networked teens. New Haven: Yale University Press, 2014.

BRANCO, Sergio; BRITTO, Walter. **O que é Creative Commons?** novos modelos de direito autoral em um mundo mais criativo. Rio de Janeiro: FGV, 2013. 176 p.

BRASIL. **Constituição** (1988). Constituição da República Federativa do Brasil. Brasília 1988.

BRASIL. Decreto n.º 8.771, de 11 de maio de 2016. Brasília, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm>. Acesso em: 07 jul. 2018.

BRASIL. Lei n.º 8.069, de 13 de julho de 1990. **Estatuto da Criança e do Adolescente**. Brasília, 1990a. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 03 jul. 2018.

BRASIL. Lei n.º 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor**. Brasília, 1990b. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/l8078.htm>. Acesso em: 10 jul. 2018.

BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. **Código Civil**. Brasília, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 10 jul. 2018.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Brasília, 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 07 jul. 2018.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Lei Geral de Proteção de Dados**. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 05 out. 2018.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian.** [S.l.]. 17 mar. 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 06 jul. 2018.

CELLARD, André. A análise documental. In: POUPART, Jean et. al. (Org). **A pesquisa qualitativa:** enfoques epistemológicos e metodológicos. Petrópolis: Vozes.

CLOUD, Morgan. Property is privacy: Locke and Brandeis in the twenty-first century. **American Criminal Law Review**, [S. L.], v. 55, p.37-75, 31 jul. 2017.

CONSELHO NACIONAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE (CONANDA). Resolução n.º 163, de 13 de março de 2014. . Brasília, Disponível em: <http://www.crianca.mppr.mp.br/pagina-1635.html#resolucao_163>. Acesso em: 10 ago. 2018.

CONSTINE, Josh. Facebook and Instagram change to crack down on underage children. **Techcrunch.** [S.l.]. jul. 2018. Disponível em: <https://techcrunch.com/2018/07/19/facebok-under-13/>. Acesso em: 20 out. 2018.

CONVERGÊNCIA DIGITAL. **Brasileiros são campeões mundiais no uso das redes de mensagens instantâneas.** 2016. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=42318&sid=17#.W7tgBs5KjIV>. Acesso em: 20 jul. 2018.

CORREA, Luciana. **Geração YouTube:** Um mapeamento sobre o consumo e a produção de vídeos por crianças. São Paulo: ESPM Media Lab, 2016. Disponível em: <http://www2.espm.br/sites/default/files/pagina/media-lab_luciana_correa_2016.pdf>. Acesso em: 07 set. 2018.

CURRAN, Dylan. Are you ready?: Here is all the data Facebook and Google have on you. **The Guardian.** [S.l.]. 30 mar. 2018. Disponível em: <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>. Acesso em: 09 out. 2018.

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

DONEDA, Danilo. **Privacy and Data Protection in the Marco Civil da Internet (Brazilian Civil Rights Framework for the Internet Bill of Rights)**. [S.l.]. 2014.

DONEDA, Danilo; ROSSINI, Caroline Almeida A.. Proteção de dados de crianças e adolescentes na Internet. In: Barbosa, A. F. (Coord). **TIC Kids Online Brasil 2014:** pesquisa sobre o uso da internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2015, p. 37-46. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_Kids_2014_livro_eletronico.pdf>. Acesso em: 05 abr. 2018.

EBERLIN, Fernando Büscher von Teschenhausen. Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: O papel dos provedores de aplicação no cenário jurídico brasileiro. **Revista Brasileira de Políticas Públicas**, [S.l.], v. 7, n. 3, p.256-273, 2017. Centro de Ensino Unificado de Brasília.

EGAS, Heloiza. Estratégias para a proteção integral de crianças e adolescentes no mundo digital. In: (NIC.BR), Núcleo de Informação e Coordenação do Ponto Br. **TIC Kids Online Brasil:** pesquisa sobre o uso da internet por crianças e adolescentes no Brasil 2016. São Paulo: Comitê Gestor da Internet no Brasil (CGI.BR), 2017. p. 29-37. Disponível em: < https://www.cetic.br/media/docs/publicacoes/2/TIC_KIDS_ONLINE_2016_LivroEletronico.pdf>. Acesso em: 08 out. 2018.

EPSTEIN, Lee; KING, Gary. **Pesquisa Empírica em Direito:** as regras de inferência. São Paulo: Direito GV, 2013. 253 p. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/11444>. Acesso em: 21 out. 2016.

FERES, Marcos Vinício Chein; OLIVEIRA, Jordan Vinicius de. Dos Códigos Legais aos Códigos do Ciberespaço: reflexões sobre Direito e Deep Web. **Revista de Propriedade Intelectual, Direito Contemporâneo e Constituição**, Aracaju, v. 11, n. 2, p.234-253, jun. 2017. Disponível em: <http://www.pidcc.com.br/artigos/11022017/09.pdf>. Acesso em: 20 out. 2018.

FITZPATRICK, Laura. Brief History YouTube. **Time Magazine.** [S.l.]. 31 maio 2010. Disponível em: <http://content.time.com/time/magazine/article/0,9171,1990787,00.html>. Acesso em: 29 ago. 2018.

FLORIDI, Luciano. Four challenges for a theory of informational privacy. **Ethics and Information Technology**, [S.l.], v. 8, n. 3, p.109-119, 25 out. 2006. Springer Nature.

FLORIDI, Luciano. On Human Dignity as a Foundation for the Right to Privacy. **Philosophy & Technology**, [S.l.], v. 29, n. 4, p.307-312, 26 abr. 2016. Springer Nature.

FLORIDI, Luciano. **The 4th revolution:** How the infosphere is reshaping human reality. Nova York: Oxford University Press, 2014. 334 p. Ebook.

FLORIDI, Luciano. The Ontological Interpretation of Informational Privacy. **Ethics and Information Technology**, [S.l.], v. 7, n. 4, p.185-200, dez. 2005. Springer Nature.

GOOGLE INC. **Aviso de privacidade do YouTube Kids.** 2018a. Disponível em: <https://kids.youtube.com/t/privacynotice>. Acesso em: 20 set. 2018.

GOOGLE INC.. **Recursos para educadores.** 2018b. Entrada da página de ajuda do YouTube. Disponível em: <https://support.google.com/youtube/answer/2802327?hl=pt>. Acesso em: 22 out. 2018.

GOOGLE INC. **Recursos para os pais.** 2018c. Entrada da página de ajuda do YouTube. Disponível em: <https://support.google.com/youtube/answer/2802272?hl=pt-BR>. Acesso em: 22 out. 2018.

GOOGLE INC. **Segurança infantil no YouTube.** 2018d. Entrada da página de ajuda do YouTube. Disponível em: <https://support.google.com/youtube/answer/2801999?hl=pt-BR>. Acesso em: 22 out. 2018.

GOOGLE LLC. **YouTube Kids.** 2018. Disponível em: <https://play.google.com/store/apps/details?id=com.google.android.apps.youtube.kids&referrer=utm_source%3Dwebsite%26utm_medium%3Dytk%26utm_campaign%3Dlp>. Acesso em: 07 set. 2018.

GUERREIRO, Pedro. Na China, um ranking social vai listar os bons e os maus cidadãos. **Público.** [S.l.]. 15 jan. 2018. Disponível em: <https://www.publico.pt/2018/01/15/tecnologia/noticia/quantos-pontos-vale-a-sua-vida-1798308>. Acesso em: 09 out. 2018.

HARTUNG, Pedro; PITA, Marina. Proteger dados de crianças e adolescentes é garantir a liberdade. **Estadão.** São Paulo. 30 jun. 2018. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/proteger-dados-de-criancas-e-adolescentes-e-garantir-a-liberdade/>. Acesso em: 06 jul. 2018.

IGREJA, Rebecca Lemos. O Direito como objeto de estudo empírico: o uso de métodos qualitativos no âmbito da pesquisa empírica em Direito. In: MACHADO, Maíra Rocha (Org.). **Pesquisar empiricamente o direito.** São Paulo: Rede de Estudos Empíricos em Direito, 2017. p. 11-37.

INSTITUTO ALANA. **Manifesto pela proteção de dados com prioridade absoluta de crianças e adolescentes.** São Paulo, 2018. Disponível em: <http://prioridadeabsoluta.org.br/wp-content/uploads/2018/06/manifesto-pl-protecao-de-dados.pdf>. Acesso em: 07 jul. 2018.

INTERNATIONAL BUSINESS MACHINES (IBM). **Extracting business value from the 4 V's of big data.** 2018a. Disponível em: < https://ibm.co/1S02bPm>. Acesso em: 08 jul. 2018.

INTERNATIONAL BUSINESS MACHINES (IBM). **The Four V's of Big Data.** 2018b. Disponível em: < https://ibm.co/18nYiuo>. Acesso em: 08 jul. 2018.

IRISH COMPUTER SOCIETY. **What is Privacy by Design & Default?** 2018. Disponível em: < https://www.ics.ie/news/what-is-privacy-by-design-a-default>. Acesso em: 14 jul. 2018.

JOHNSTON, Chris. Youtuber Ryan, de 7 anos, ganha US$ 22 milhões e é o mais bem pago do mundo em 2018. **BBC News.** [S.l.]. 4 dez. 2018. Disponível em: <https://www.bbc.com/portuguese/salasocial-46435004>. Acesso em: 15 jan. 2019.

KONDER, Carlos Nelson; TEIXEIRA, Ana Carolina Brochado. Crianças e adolescentes na condição de pacientes médicos: desafios da ponderação entre autonomia e vulnerabilidade. **Pensar**, Fortaleza, v. 21, n. 1, p.70-93, 2016.

LAPERRIÈRE, Anne. Os critérios de cientificidade dos métodos qualitativos. In: POUPART, Jean et al. **A pesquisa qualitativa:** enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2008. p. 410-435.

LEAL, Livia Teixeira. Internet of Toys: os brinquedos conectados à internet e o direito da criança e do adolescente. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, n. 12, p.175-187, 2017.

LESSIG, Lawrence. **Code:** version 2.0. Nova York: Basic Books, 2006.

LESSIG, Lawrence. Privacy as Property. **Social Research**, [S.l.], v. 69, n. 1, p.247-269, 2002. Privacy in Post-Communist Europe.

MACHADO, Maira Rocha. O estudo de caso na pesquisa em direito. In: MACHADO, Maira Rocha (Org.). **Pesquisar empiricamente o direito.** São Paulo: Rede de Estudos Empíricos em Direito, 2017. p. 357-389.

MACMILLAN, Douglas; MCMILLAN, Robert. Google Exposed User Data, Feared Repercussions of Disclosing to Public. **The Wall Street Jornal.** [S.l.]. 08 out. 2018. Disponível em: <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194?mod=hp_lead_pos1>. Acesso em: 09 out. 2018.

MADRIGAL, Alexis C. Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days. **The Atlantic.** [s. l.]. 01 mar. 2012. Disponível em: <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>. Acesso em: 07 jul. 2018.

MANGETH, Ana Lara; NUNES, Beatriz; MAGRANI, Eduardo. **Seis pontos para entender o Regulamento Geral de Proteção de Dados da UE.** 2018. ITS Rio. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-prote%C3%A7%C3%A3o-de-dados-pessoais-gdpr-d377f6b691dc>. Acesso em: 22 out. 2018.

MARX, Gary; STEEVES, Valerie. From the Beginning: Children as Subjects and Agents of Surveillance. **Surveillance & Society**, [S.l.], v. 7, n. 3/4, p.192-230, 17 jun. 2010.

MCBURNEY, Vincent. Professor Luciano Floridi on the Philosophy of the Infosphere. **Toolbox.** [S.l.]. 08 abr. 2008. Disponível em: <https://it.toolbox.com/blogs/vincentmcburney/professor-luciano-floridi-on-the-philosophy-of-the-infosphere-040808>. Acesso em: 28 out. 2018.

MENEZES, Joyceane Bezerra de; BODIN DE MORAES, Maria Celina. Autoridade parental e privacidade do filho menor: o desafio de cuidar para emancipar. **Novos Estudos Jurídicos**, [S.l.], v. 20, n. 2, p.501-532, 31 jul. 2015. Editora UNIVALI.

MENEZES, Joyceane Bezerra de; MULTEDO, Renata Vilela. A autonomia ético-existencial do adolescente nas decisões sobre o próprio corpo e a heteronomia dos pais e do Estado no Brasil. **A&C**, Belo Horizonte, v. 63, n. 16, p.187-210, 2016.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. **MPDFT investiga como YouTube trata os dados pessoais de crianças brasileiras.** 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10186-mpdft-investiga-como-youtube-trata-os-dados-pessoais-de-criancas-brasileiras>. Acesso em: 09 out. 2018.

NAKASHIMA, Ryan. Google tracks your movements, like it or not. **Associated Press.** São Francisco. 13 ago. 2018. Disponível em: <https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not>. Acesso em: 06 out. 2018.

NEGRI, Sergio Marcos Carvalho de Ávila. As razões da pessoa jurídica e a expropriação da subjetividade. **Civilistica.com**, Rio de Janeiro, v. 2, n. 5, p.1-18, 2016. Disponível em: < http://civilistica.com/wp-content/uploads/2016/12/Negri-civilistica.com-a.5.n.2.2016.pdf>. Acesso em 09 ago. 2018.

NEGRI, Sergio Marcos Carvalho de Ávila; FERNANDES, Elora Raad; RIGOLON, Maria Regina Detoni Cavalcanti. A proteção integral de crianças e adolescentes: desafios jurídicos de uma sociedade hipercontectada. In: CONGRESSO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO: POLÍTICA & LEIS, 1., 2018, Belo Horizonte. **Anais do I Congresso de ciência, tecnologia e inovação: Política & Leis.** Belo Horizonte. No prelo.

NEVARES, Ana Luiza Maia; SCHREIBER, Anderson. Do sujeito à pessoa: uma análise da incapacidade civil. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (Org.). **O direito civil entre o sujeito e a pessoa:** estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. p. 39-56.

NYST, Carly; GEARY, Patrick; GOROSTIAGA, Amaya. **DISCUSSION PAPER SERIES: Children's Rights and Business in a Digital World:** Privacy, protection of personal information and reputation rights. [S.l.]: UNICEF, 2017. UNICEF Child Rights & Business Unit. Disponível em: <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf>. Acesso em: 5 out. 2018.

NOBRE, Marcos. Apontamentos sobre a pesquisa em direito no Brasil. In: Simpósio "O que é pesquisa em direito", 2002, São Paulo. Cadernos Direito GV. São Paulo: FGV Direito SP, 2009. p. 1 - 19. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/2779>. Acesso em: 29 out. 2018.PARISER, Eli. **Beware online "filter bubbles"**. In: TED2011, 2011. Long Beach. Disponível em: <https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles>. Acesso em: 06 jul. 2018.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). **TIC Kids Online Brasil 2014:** pesquisa sobre o uso da internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil (CGI.BR), 2015. 392 p. Disponível em: <https://cetic.br/media/docs/publicacoes/2/TIC_Kids_2014_livro_eletronico.pdf>. Acesso em: 06 jul. 2018.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). **TIC Kids Online Brasil 2016:** pesquisa sobre o uso da internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil (CGI.BR), 2017. 332 p. Disponível em: <

https://cetic.br/media/docs/publicacoes/2/TIC_KIDS_ONLINE_2016_LivroEletronico.pdf>. Acesso em: 06 jul. 2018.

PARISER, Eli. **O filtro invisível:** o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012. 287 p.

PEW RESEARCH CENTER. **Teens, social media & Technology 2018. [**S.l.]: Pew Research Center, 2018. Disponível em: <http://assets.pewresearch.org/wp-content/uploads/sites/14/2018/05/31102617/PI_2018.05.31_TeensTech_FINAL.pdf>. Acesso em: 12 ago. 2018.

PIRES, Álvaro P.. Sobre algumas questões epistemológicas de uma metodologia geral para as ciências sociais. In: POUPART, Jean et al. **A pesquisa qualitativa:** enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2008. p. 43-94.

POLIDO, Fabrício B. Pasquot et al. **GDPR e suas repercussões no direito brasileiro:** primeiras impressões de análise comparativa. Belo Horizonte: Iris, 2018, 39p. Elaborado pelo Instituto de Referência em Internet e Sociedade (IRIS). Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-Primeiras-impress%C3%B5es-de-an%C3%A1lise-comparativa-PT.pdf>. Acesso em: 22 out. 2018.

POPKEN, Ben. Google sells the future, powered by your personal data. **NBC News.** [S.l.]. 10 maio 2018. Disponível em: <https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501>. Acesso em: 09 out. 2018.

PRENSKY, Marc. Digital Natives, Digital Immigrants. **On The Horizon**, [S.l.], v. 9, n. 5, p. 1-6, set. 2001.

REES, Christopher. Tomorrow's privacy: personal information as property. **International Data Privacy Law**, [S.l.], v. 3, n. 4, p. 220-221, 9 out. 2013. Oxford University Press (OUP).

RIBEIRO, Susana Almeida. O que é a Web 3.0? **Público.** [s. l.]. 29 jun. 2009. Disponível em: <https://www.publico.pt/2009/06/29/tecnologia/noticia/o-que-e-a-web-30-1389325>. Acesso em: 08 jul. 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** A privacidade hoje. Rio de Janeiro: Renovar, 2008. 382 p.

RODOTÀ, Stefano. Entrevista à RTDC. **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 3, n. 11, jul.-set. 2002, p. 225–308. Entrevista concedida a Danilo Doneda.

RODOTÀ, Stefano. Transformações no corpo. **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 19, p. 65-107, 2004.

ROHR, Altieres. Vazamento de dados do Snapchat expõe milhares de fotos na web. **G1.** [S.l.]. 10 out. 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/10/vazamento-de-dados-do-snapchat-expoe-milhares-de-fotos-na-web.html>. Acesso em: 14 nov. 2018.

ROSA, Bruno. Falha no Twitter pode ter gerado vazamento de dados de clientes. **O Globo.** [S.l.]. 21 set. 2018. Disponível em: <https://oglobo.globo.com/economia/falha-no-

twitter-pode-ter-gerado-vazamento-de-dados-de-clientes-23090778>. Acesso em: 14 nov. 2018.

SANDOVAL, Greg. Morgan Stanley figured out how much YouTube would be worth if it were a separate company, and it's more valuable than Disney. **Business Insider.** [S.l.]. 18 mar. 2018. Disponível em: <https://www.businessinsider.com/morgan-stanley-values-youtube-160-billion-dollars-2018-5>. Acesso em: 29 ago. 2018.

SÊCO, Thaís Fernanda Tenório. Por uma nova hermenêutica do direito da criança e do adolescente. **Civilistica.com**: Revista Eletrônica de Direito Civil, [S.l.], v. 2, n. 3, p.1-26, 2014.

SCHULMAN, Gabriel. www.privacidade-em-tempos-de-internet.com: o espaço virtual e os impactos reais à privacidade das pessoas. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (coord.). **O direito civil entre o sujeito e a pessoa:** estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. p. 17-35.

SCHULZ, Wolfgang; VAN HOBOKEN, Joris. **Direitos humanos e criptografia.** Paris: Organização das Nações Unidas Para A Educação, A Ciência e A Cultura (UNESCO), 2016. 104 p. Tradução brasileira por Instituto de Tecnologia e Sociedade do Rio (ITS Rio).

SCHWARTZ, Paul M.. Property, Privacy, and Personal Data. **Harvard Law Review**, [S.l.], v. 117, n. 7, p.2055-2128, maio 2004.

SOUSA, Dayanne; MOREIRA, Beth. Google mantêm liderança em ranking das marcas mais valiosas. **Exame.** [S.l.]. 30 maio 2018. Disponível em: <https://exame.abril.com.br/negocios/google-mantem-lideranca-em-ranking-das-marcas-mais-valiosas/>. Acesso em: 29 ago. 2018.

SOUZA, Carlos Affonso Pereira de. Os 5 hábitos dos brinquedos altamente conectados. **Uol Notícias.** [S. l.]. 13 mar. 2018. Disponível em: <https://tecfront.blogosfera.uol.com.br/2018/03/13/os-5-habitos-dos-brinquedos-altamente-conectados/>. Acesso em: 07 jul. 2018.

SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. **Marco Civil da Internet:** construção e aplicação. Juiz de Fora: Editar, 2016.

TEIXEIRA, Ana Carolina Brochado. Resenha à obra "Liberdade e Família: Limites para a intervenção do Estado nas relações conjugais e parentais", de Renata Vilela Multedo. **Civilistica.com**: Revista Eletrônica de Direito Civil, [S. l.], v. 2, n. 6, p.1-6, 2017.

TENE, Omer; POLONETSKY, Jules. Privacy in the age of Big Data: a time for big decisions. **Stanford Law Review**, Stanford, v. 64, p.63-69, fev. 2012.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento Civil-constitucional brasileiro. In: TEPEDINO, Gustavo. **Temas de Direito Civil.** 3. ed. Rio de Janeiro: Renovar, 2004. p. 23-58.

TEPEDINO, Gustavo. O papel atual da doutrina do direito civil entre o sujeito e a pessoa. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (coord.). **O**

direito civil entre o sujeito e a pessoa: estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. p. 17-35.

THE ECONOMIST (Ed.). The world's most valuable resource is no longer oil, but data. **The Economist.** [S.l.]. 6 maio 2017. Disponível em: < https://econ.st/2Gtfztg>. Acesso em: 08 jul. 2018.

UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do parlamento europeu e do conselho de 27 de abril de 2016. 2016a. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=EN>. Acesso em: 09 out. 2018.

UNIÃO EUROPEIA. Regulamento n.º 2016/679, de 27 de abril de 2016. **Regulamento Geral Sobre A Proteção de Dados**. 2016b. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#ntc7-L_2016119PT.01000101-E0007>. Acesso em: 09 jul. 2018.

UNITED NATIONS CHILDREN'S FUND (UNICEF). **The state of the world's children 2017:** Children in a Digital World. Nova York, 2017. 215 p.

VENTURINI, Jamila et al. **Terms of Service and Human Rights:** an Analysis of Online Platform Contracts. Rio de Janeiro: Editora Revan, 2016. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/18231>. Acesso em: 08 set. 2018.

VERONESE, Alexandre. Considerações sobre o Problema da Pesquisa Empírica e sua Baixa Integração na Área de Direito: a Tentativa de uma Perspectiva Brasileira a partir da Avaliação dos Cursos de Pós-Graduação do Rio de Janeiro. **Revista da Procuradoria Geral do Estado de Mato Grosso do Sul**, Campo Grande, v. 14, n. 1, p.197-237, dez. 2013. Disponível em: <http://www.pge.ms.gov.br/wp-content/uploads/sites/48/2015/03/Considerações_sobre_o.pdf>. Acesso em: 22 maio 2018.

VIOLA, Mario. **Child Privacy in the Age of Web 2.0 and 3.0:** challenges and opportunities for policy. Florence: UNICEF Office Of Research - Innocenti, 2017.

VIOLA, Mario. Data Protection & Privacy in the Internet Era: the Internet Bill of Rights. In: SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; LEMOS, Ronaldo. **Brazil's Internet Bill of Rights:** a closer look. 2. ed. Rio de Janeiro: Institute For Technology And Society Of Rio de Janeiro (its Rio), 2017. Cap. 4. p. 81-87.

VOIGT, Paul; BUSSCHE, Axel von Dem. **The EU General Regulation Data Protection (GDPR):** a pratical guide. Cham: Springer, 2017. 385 p. Ebook.

WAKKA, Wagner. YouTube já tem mais de 1,8 bilhão de usuários ativos por mês. **Canal Tech.** [S.l.]. 04 maio 2018. Disponível em: <https://canaltech.com.br/redes-sociais/youtube-ja-tem-mais-de-18-bilhao-de-usuarios-ativos-por-mes-113174/>. Acesso em: 29 ago. 2018.

WARREN, Samuel D.; BRANDEIS, Louis D.. The Right to Privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p.193-220, 14 dez. 1890.

WESTERMAN, Pauline C.. Open or autonomous?: the debate on legal methodology as a reflection of the debate on law. In: VAN HOUECKE, Mark. **Methodologies of Legal Research:** Which kind of method for what kind of discipline?. Portland: Hart Publishing, 2011. p. 87-110.

WONG, Julia Carrie; SOLON, Olivia. Google to shut down Google+ after failing to disclose user data breach. **The Guardian.** São Francisco. 09 out. 2018. Disponível em: <https://www.theguardian.com/technology/2018/oct/08/google-plus-security-breach-wall-street-journal>. Acesso em: 09 out. 2018.

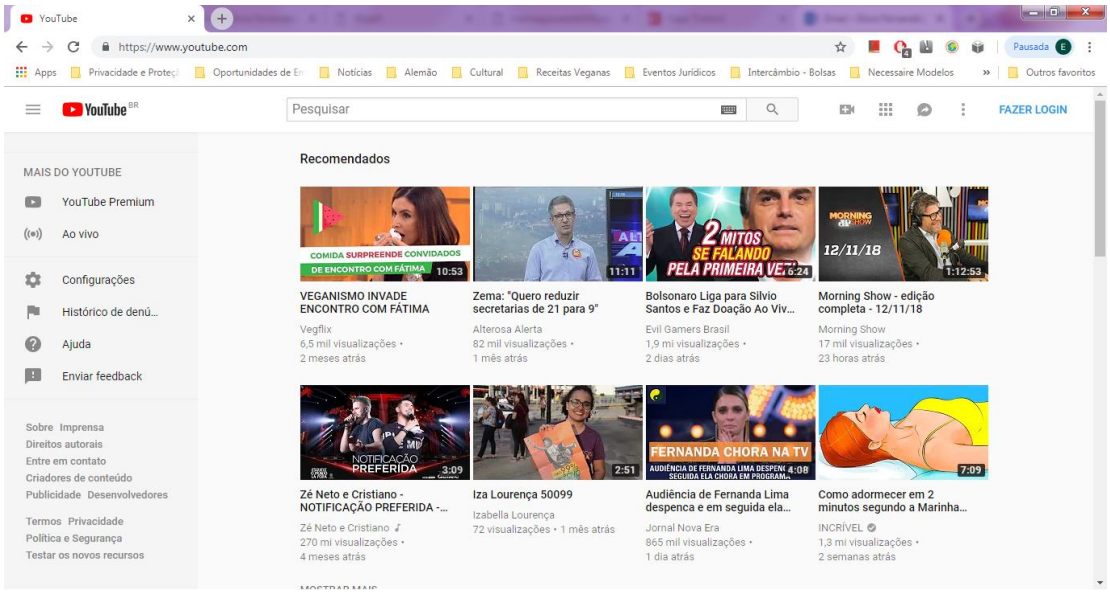
YIN, Robert. **Estudo de caso:** planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.

YOUTUBE. **Início.** 2018. Disponível em: <https://www.youtube.com/>. Acesso em: 10 ago. 2018.

YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. Computer-based personality judgments are more accurate than those made by humans. **Proceedings Of The National Academy Of Sciences**, [s.l.], v. 112, n. 4, p.1036-1040, 12 jan. 2015. Proceedings of the National Academy of Sciences.

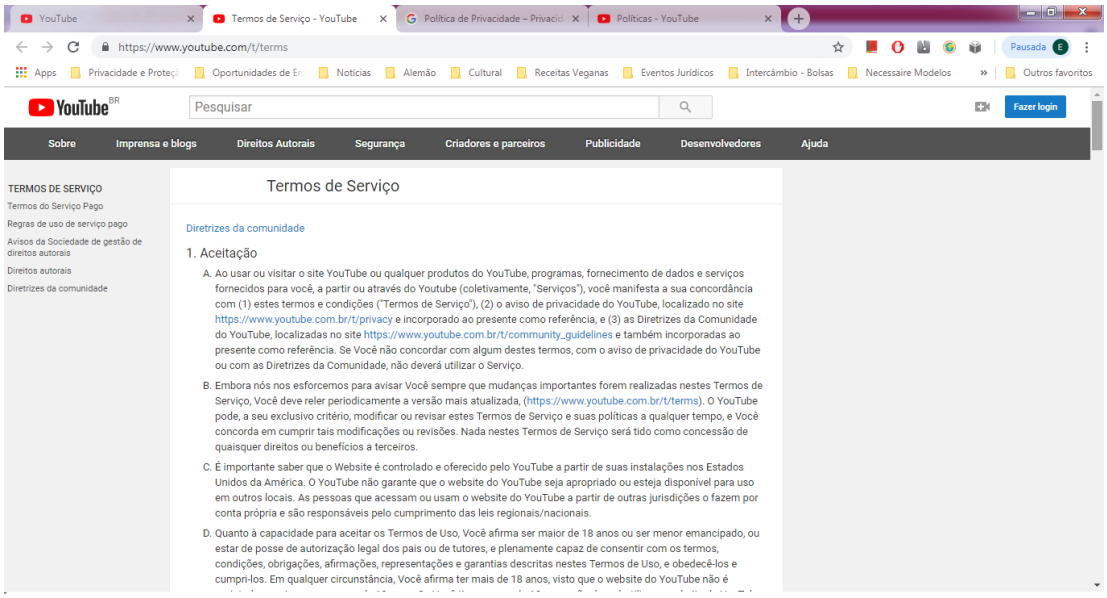
APÊNDICE – ILUSTRAÇÕES DA COLETA DE DADOS

Figura 1



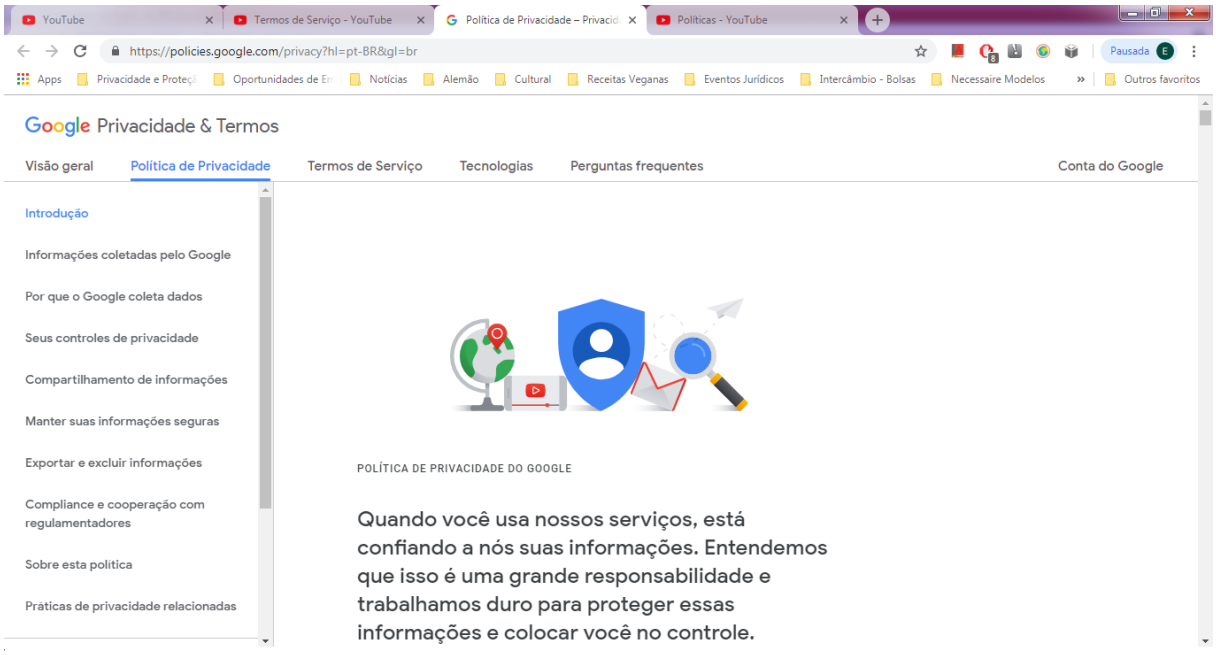
Fonte: Captura de tela realizada pela autora.

Figura 2



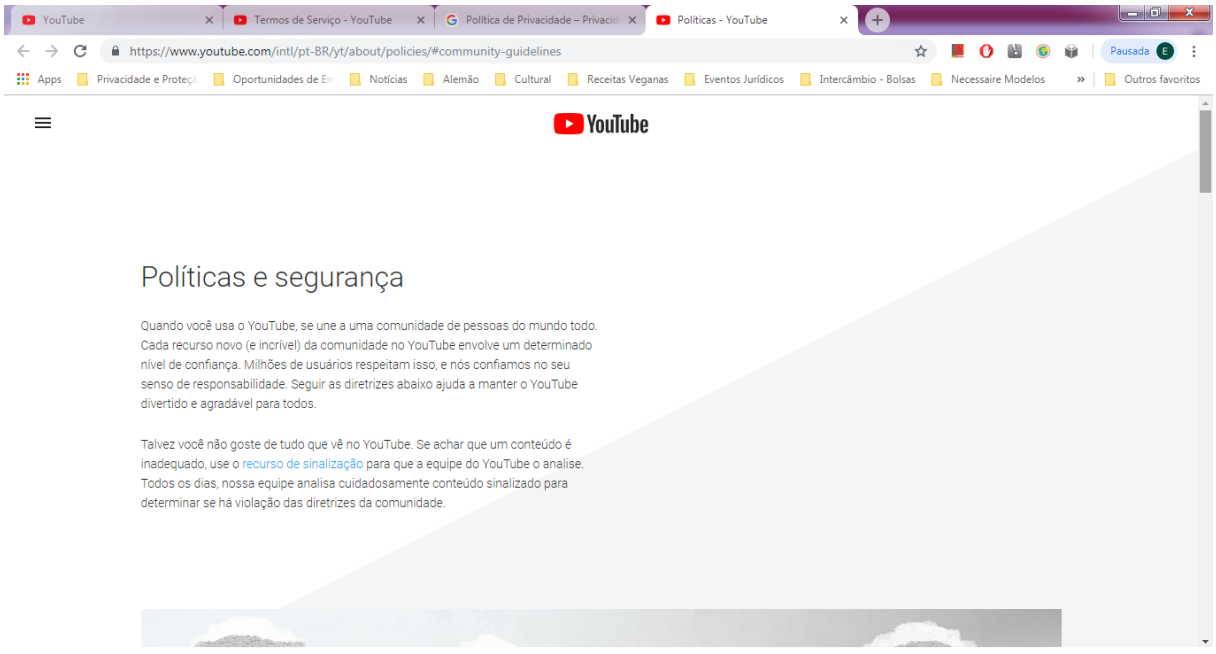
Fonte: Captura de tela realizada pela autora.

Figura 3



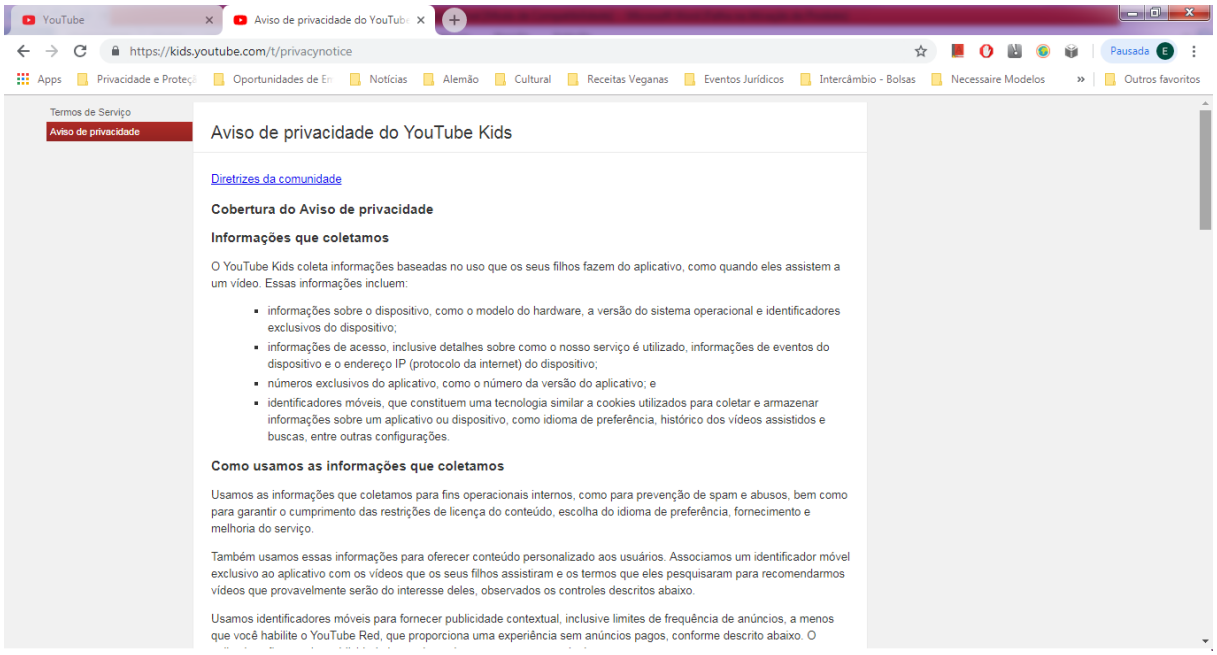
Fonte: Captura de tela realizada pela autora.

Figura 4



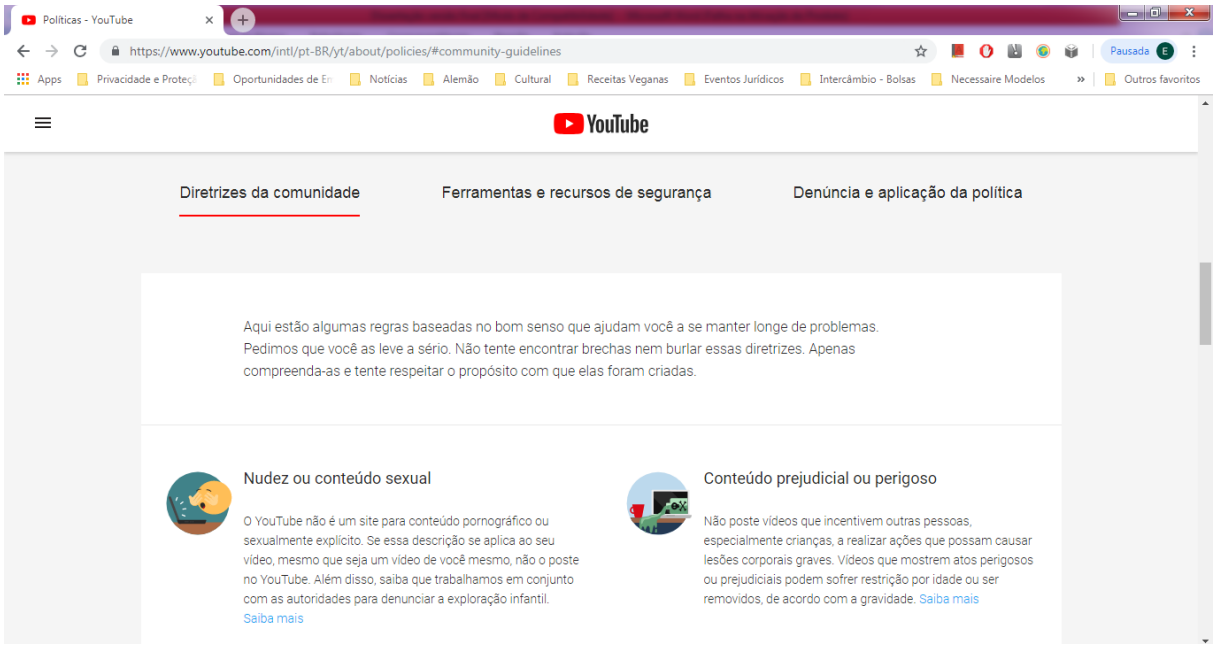
Fonte: Captura de tela realizada pela autora.

Figura 5



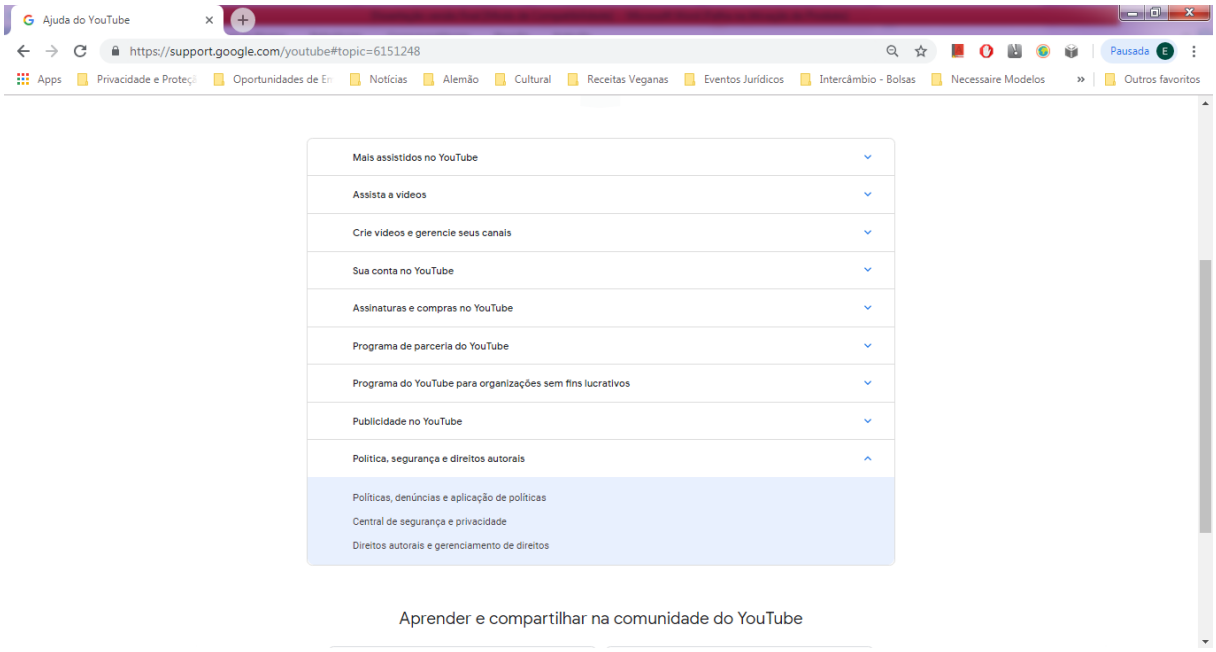
Fonte: Captura de tela realizada pela autora.

Figura 6



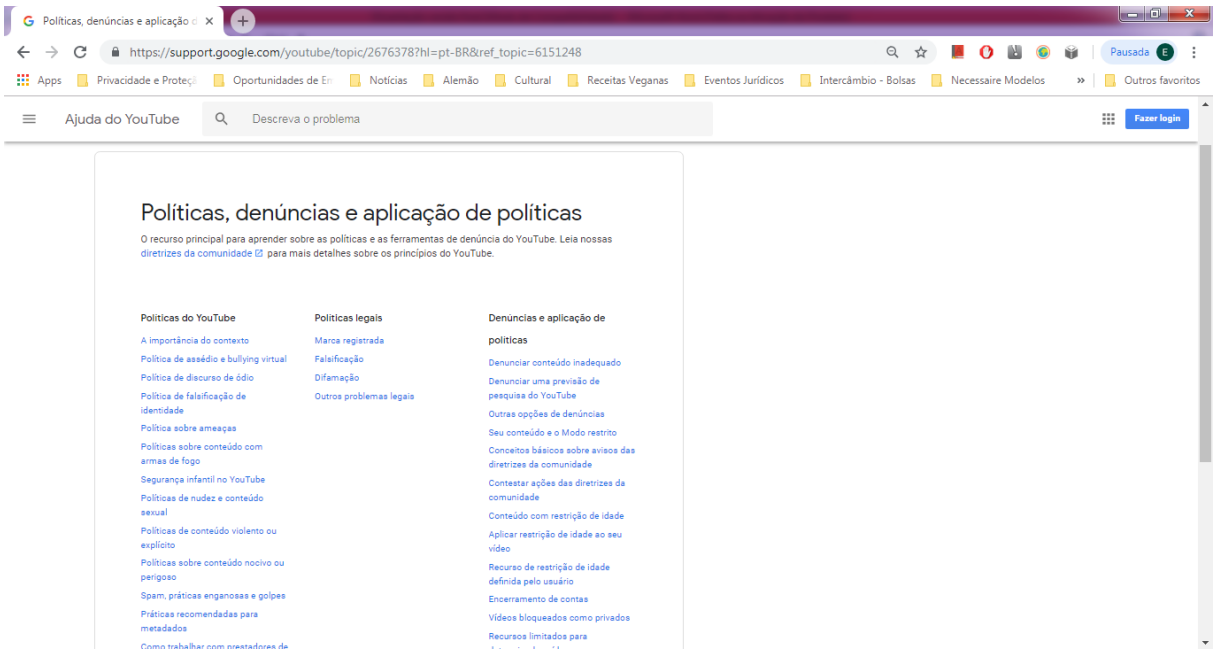
Fonte: Captura de tela realizada pela autora.

Figura 7



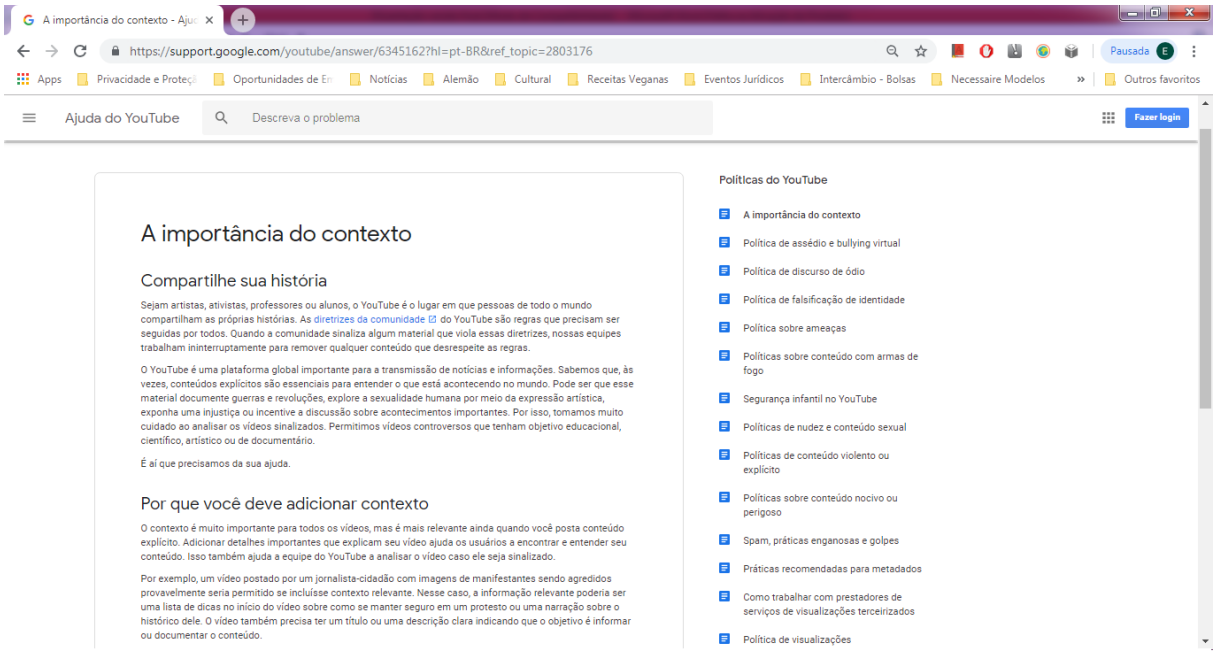
Fonte: Captura de tela realizada pela autora.

Figura 8



Fonte: Captura de tela realizada pela autora.

Figura 9



Fonte: Captura de tela realizada pela autora.