Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 15.12.2020
Aprovado em: 26.12.2020

Revista de Direito, Governança e Novas Tecnologias

TOYS THAT LISTEN E A PROTEÇÃO DA PRIVACIDADE E DE DADOS PESSOAIS DE CRIANÇAS A PARTIR DA VIGILÂNCIA POR BRINQUEDOS *ONLINE*: OS CASOS *HELLO BARBIE* E *MY FRIEND CAYLA*

Diogo Dal Magro[1]
Vinícius Borges Fortes[**]

Resumo: O objetivo geral do estudo é analisar como os "brinquedos que ouvem" podem operar em potenciais violadores de privacidade e de dados pessoais de crianças, buscando possibilidades para assegurar os direitos de privacidade da internet. No Brasil, a Lei Geral de Proteção de Dados Pessoais constitui-se em significativo avanço na temática de proteção de dados pessoais e, consequentemente, na proteção da privacidade. Entretanto, os riscos da *Internet of Toys* ainda não são suficientemente precisos.

[1] Mestrando em Direito pela Faculdade Meridional - IMED. Graduado em Direito pela Faculdade Meridional - IMED (2016-2020). Membro dos Grupos de Pesquisa "Latin America Privacy Hub", "Direito, Novas Tecnologias e Desenvolvimento" e "Ética, Cidadania e Sustentabilidade", vinculados ao Programa de Pós-Graduação Stricto Sensu - Mestrado em Direito - da Faculdade Meridional - IMED. Bolsista MITACS (2019), tendo desenvolvido pesquisas no projeto "Démocratie digitale (digital democracy) en contexte de rapports linguistiques complexes", na Universitè de Moncton (Canadá). Membro Fundador do Capítulo Legal Hackers de Passo Fundo-RS. Bolsista PROBIC - FAPERGS/IMED (2018/2019). Bolsista PIBIC - CNPq/IMED (2017/2018). Co-fundador da Lawtech Hi ORDER Regulação e Tecnologia. Advogado. E-mail: diogodalmagro@gmail.com.

[**] Possui Estágio de Pós-Doutorado em Direito pela Vrije Universiteit Brussel, Bélgica (2016), com pesquisa voltada aos Direitos de privacidade na internet e o sistema de proteção de dados. Doutorado em Direito pela Universidade Estácio de Sá - UNESA (2015), com período sanduíche na Universidad de Zaragoza (2014-2015), com financiamento do PDSE/CAPES. Mestrado em Direito pela Universidade de Caxias do Sul (2011). Graduação em Direito pela FAPLAN - Faculdades Planalto (2008). Atualmente, é pesquisador e Bolsista de Produtividade em Pesquisa com dedicação exclusiva ao CETID - Centro de Pesquisa, Tecnologia e Inovação Digital da Fundação Meridional, no Projeto de Pesquisa "Tecnologia, Inovação e Sustentabilidade". Além disso, atua como pesquisador-membro do Projeto de pesquisa "O Distrito Federal e a Governança da Internet: tecnologias e informação", financiado pela Fundação de Amparo à Pesquisa do Distrito Federal. Ainda, é líder do Projeto de Pesquisa Latin America Privacy Hub (LAPH), certificado pela IMED no Diretório de Grupos de Pesquisa do CNPq, financiado pelo CETID/Fundação Meridional. Sua pesquisa está focada nas áreas de Tecnologia, Inovação e Sustentabilidade, com ênfase em Direitos de Privacidade na Internet; Proteção de Dados Pessoais; Regulação e Tecnologia para a Democracia e para a Sustentabilidade. É professor visitante no Law, Science, Technology and Society Research Group (LSTS) da Vrije Universiteit Brussel (VUB), Bélgica, bem como do Brussels Privacy Hub, desde o ano 2016. Mantém parcerias de pesquisa com instituições e pesquisadores brasileiros (UnB, PUCPR, UFSM, Uniritter, UFRGS), e estrangeiros (VUB/Bélgica, Brussels Privacy Hub/Bélgica, LSTS/Bélgica, Universidad de Zaragoza/Espanha). Professor permanente do Programa de Pós-Graduação Stricto Sensu em Direito da IMED - Faculdade Meridional, onde foi coordenador no período 2017-2019. Professor dos cursos de Graduação em Direito e Ciência da Computação da IMED - Faculdade Meridional. Tem experiência profissional como advogado e empreendedor no segmento Lawtech, tendo fundado a Hi ORDER Regulação e Tecnologia, startup focada na oferta de soluções jurídicas e tecnológicas voltadas à elaboração e automação de contratos de tecnologia; blindagem contratual e tecnológica em operações empresariais que envolvam tecnologia; suporte regulatório e tecnológico a provedores de aplicação e conexão à internet; gestão de propriedade intelectual e bancos de dados; aplicação de soluções jurídicas inteligentes na produção de prova processual por blockchain e outras tecnologias. Líder do capítulo Legal Hackers Passo Fundo, atuando como articulador do tema Direito e Tecnologia entre profissionais da área jurídica, TI e mídias digitais. E-mail: vinicius.fortes@imed.edu.br Instagram: @vbfortes Facebook: @vborgesfortes.

Palavras-chave: Brinquedos que ouvem. Crianças. Dados Pessoais. Privacidade. Paul Bernal.

TOYS THAT LISTEN AND THE PROTECTION OF CHILDREN'S PRIVACY AND PERSONAL DATA FROM ONLINE TOOL SURVEILLANCE: THE HELLO BARBIE AND MY FRIEND CAYLA CASES

Abstract: The general objective of the study is to analyze how the "toys that listen" can operate in potential violators of privacy and personal data of children, looking for possibilities to ensure the privacy rights of the internet. In Brazil, the General Law of Protection of Personal Data constitutes a significant advance in the area of protection of personal data and, consequently, in the protection of privacy. However, the risks of Internet of Toys are not yet precise enough.

Keywords: Toys that listen. Children. Personal Data. Privacy. Paul Bernal.

INTRODUÇÃO

A indissociável presença da internet no cotidiano da grande parcela da população mundial tem trazido consequências e desafios para diferentes campos científicos. Ao direito, cabe o dever de garantir que a utilização da internet ocorra de modo seguro e que não venha a causar prejuízos e danos ao usuários, compreendendo-se, nesse sentido, os danos materiais, morais, psíquicos, entre possíveis outros.

Evidente que a internet, atualmente, não constitui-se em um ambiente totalmente inseguro e desprovida de qualquer regulamentação – como pretendido, por determinados grupos, no passado. Além de computadores e celulares, a internet passou a conectar-se com, televisões, carros, relógios, lâmpadas, geladeiras e o número e a diversidade desses objetos só aumentam. A essa "nova internet", que a tudo vem se conectando, denominou-se Internet da Coisas.

E se aos adultos a internet trouxe facilidades, às crianças a Internet das Coisas possibilitou novas experiências, não apenas com celulares e *tablets*, mas também com as tradicionais bonecas, que agora podem facilmente comunicar-se com a criança, desenvolvendo eficientes diálogos com perguntas e respostas. Essa interação opera por meio da captação da fala da criança com o consequente processamento e a devolução de respostas, mantendo-se, assim, um diálogo – H2M2H *(human-to-machine-to-human).* Brinquedos desse

gênero são usualmente denominados de "brinquedos que ouvem", uma tradução literal de *toys that listen*.

Acompanhando o promissor mercado desses brinquedos, há desafios que devem ser enfrentados envolvendo fatores de proteção dos direitos da criança, uma vez que esses brinquedos operam por meio de uma coleta de dados pessoais, de modo que pode-se verificar potenciais violações da privacidade e dos dados pessoais da criança.

Diante dessa realidade, propõe-se a seguinte pergunta, com o intuito de expressar o problema de pesquisa deste trabalho: como o ordenamento jurídico brasileiro protege a privacidade e a proteção de dados pessoais da criança em face dos "brinquedos que ouvem", visto que esses constituem-se em potenciais violações aos quatro direitos base (teoria de Bernal), que compõem os direitos de privacidade da internet?

Como hipótese de pesquisa que visa responder, provisoriamente ao problema, tem-se que o Marco Civil da Internet reconhece como terminal qualquer dispositivo que se conecte à internet. Assim, os "brinquedos que ouvem", por serem enquadrados como terminais, operam com as mesmas potencialidades de violação de privacidade e de dados pessoais que quaisquer outros, sendo que a situação agrava-se ao considerar-se que as vítimas são crianças, sendo elas tuteladas sob estatuto próprio e, portanto, objeto de proteção específica. A teoria da proteção integral, que rege o Estatuto da Criança e do Adolescente, considera a peculiar condição das crianças, sendo motivo pelo qual a proteção deve ser incisiva. No entanto, somente com o advento da Lei Geral de Proteção de Dados Pessoais, promulgada em 2018 e com vigência a partir de 2020, é que o tema da proteção de dados pessoais passou a contar com legislação de proteção específica.

O Objetivo Geral que visa reger o presente estudo é analisar como os "brinquedos que ouvem" podem operar em potenciais violadores de privacidade e de dados pessoais de crianças, buscando possibilidades para assegurar os direitos de privacidade da internet. Como Objetivos Específicos, elege-se: *a)* apresentar casos de "brinquedos que ouvem", abordando seu funcionamento e suas complicações para a privacidade e proteção de dados; *b)* verificar se as previsões legais, nacionais e estrangeiras, são suficientes para salvaguardar os direitos de privacidade e de proteção de dados pessoais de crianças; *c)* examinar disposições legislativas sobre os "brinquedos que ouvem", buscando, consequentemente, apontar sugestões para possíveis resoluções sobre o caso; e *d)* identificar, a partir da teoria de Paul Bernal, complementos à legislação pátria sobre a matéria.

O Método utilizado para a realização do trabalho é o Hipotético-Dedutivo. As Técnicas de Pesquisa que viabilizaram o Método são: Pesquisa Bibliográfica e Documental[2], a Categoria[3] e o Conceito Operacional[4].

1 ASPECTOS JURÍDICOS DA INTERNET DAS COISAS: OS CASOS *HELLO BARBIE* E *MY FRIEND CAYLA*

Tornou-se cada vez mais comum encontrar objetos do dia a dia conectados à Internet. Carros, relógios, aparelhos de televisão, geladeiras, lâmpadas são apenas alguns dos exemplos de objetos (coisas/bens) com que naturalmente convivemos e utilizamos diariamente, e que podem – e gradualmente vem sendo – conectados à Internet.

O termo Internet das Coisas (*Internet of Things*, ou simplesmente IoT) foi cunhado pelo britânico Kevin Ashton, em 1999 (GUBBI et al., 2013, p. 1646). De lá para cá, o conceito de IoT evoluiu acompanhando a própria expansão da utilização da Internet. "O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade." (MAGRANI, 2018, p. 20).

Sob o ponto de vista conceitual, a Internet das Coisas pode ser analisada sob três diferentes aspectos, relacionados com a capacidade dos *smart objects* ("objetos inteligente", sendo aqueles que estão conectados à Internet) em: (i) serem identificáveis (*anything identifies itself*); (ii) comunicarem (*anything communicates*); e (iii) interagirem (*anything interacts*) (MIORANDI et al., 2012, p. 1498). Essas três dimensões possibilitam a compreensão de que a grande malha da Internet das Coisas encontra-se interligada entre objetos (coisas), usuários e Internet.

A interação entre objetos e usuários adquire cada vez mais experiências, sofisticando-se. Essa interação é realizada através da coleta (captação) de dados[5] dos usuários,

[2] "[...] Técnica de investigação em livros, repertórios jurisprudenciais e coletâneas legais." (PASOLD; 2001, p. 207).

[3] "[...] **palavra ou expressão estratégica à elaboração e/ou expressão de uma ideia**". (PASOLD; 2011, p. 25). Grifos originais da obra em estudo.

[4] "[...] **uma definição para uma palavra ou expressão, com o desejo de que tal definição seja aceita para os efeitos das ideia que expomos** [...]". (PASOLD; 2011, p. 25). Grifos originais da obra em estudo. As categorias utilizadas neste estudo serão destacadas com inicial maiúscula.

como, por exemplo, referente à temperatura, localização, condições de acessibilidade, deslocamento, as quais são utilizadas com o escopo de proporcionar os usuários uma melhor experiência, intensificando e aprimorando a interação entre humano e máquina (H2M, *human-to-machine*).[6]

A coleta de dados pessoais por esses objetos implica em um complexo sistema de monitoramento, que torna-se mais ou menos imbrincado, de acordo com o objeto, sua finalidade e a experiência desejada. Para exemplificar, um aparelho celular tende a coletar um número maior de dados – que se destinam a oferecer informações – do que uma lâmpada inteligente.

Entre os objetos que compõem o mundo da Internet das Coisas estão alguns brinquedos, compondo a *Internet of Toys* (internet dos brinquedos). Conhecidos como *toys that listen*, esses brinquedos surgiram com o intuito de aumentar a interação entre crianças e brinquedos, de modo com que esses indivíduos tenham experiências de diálogo, e não apenas uma conversa monóloga. A criança fala com o brinquedo, sendo que o mesmo retribui uma conversação à criança, de modo com que haja uma interação semelhante a interação entre dois humanos.

Em 2015 a Mattel realizou o lançamento de seu primeiro *toy that listen*, com o intuito de reanimar as vendas em brinquedos, que estavam em queda por conta do aumento de opções interativas digitais. Com o nome de Hello Barbie, a boneca possui um sistema de conexão wi-fi, por meio do qual a boneca capta a fala da criança, envia os dados para a empresa Toy Talk, que as processa os dados, coletando as informações e as armazena. A

[5] A fim de esclarecimento conceitual, nesse trabalho, define-se dados como sendo o conjunto total de variáveis coletadas pelo objeto, no caso dos *toys that listen*, por meio da fala da criança, e que são encaminhadas para tratamento. A partir do tratamento/processamento realizado sobre esses dados, obtém-se as informações que são necessárias para que o brinquedo interaja com a criança.

[6] Registre-se, por importante: "Em relação à segurança dos dados, ainda não há um consenso entre os fabricantes de produtos de IoT. Os próprios desenvolvedores ainda não têm uma noção completa do que é realmente necessário em termos de segurança. A fórmula indicada é continuar com a prática de testes de vulnerabilidade em softwares e sistemas, além de conscientizar os usuários da importância de sempre manter seus dispositivo atualizados com as ferramentas de segurança acessíveis.

O desafio da segurança de dados no cenário de IoT também envolve dar enfoque a questões como gestão de armazenamento, servidores e redes de *data center*, bem como à responsabilidade de cada empresa que opere nessa cadeia de produtos e serviços. Isso decorre do crescimento da quantidade dos dispositivos conectados, o que aumenta o volume de dados capturados e de operadores que atuam nessa cadeia econômica.

Tendo em vista que a lot abrange diversos setores, alguns delica dos, como saúde e meio ambiente, isso nos faz crer que deverão surge novos desafios de segurança envolvendo o grande fluxo de dados, sendo necessário acompanhar a complexidade da segurança no tratamento de *big data*." (MAGRANI, 2018, p. 92).

partir do processamento desses dados pessoais, novas informações são enviadas à boneca, para que ela possa responder à criança, por meio de um alto falante (LINN, 2015).

A boneca não apenas mantém o diálogo com a criança, mas também é capaz de gravar gostos, nomes e informações relacionadas à personalidade da criança. Isso ocorre pelo processo de armazenamento das informações coletadas a partir da fala da criança. Essas informações passam a formar um banco de dados pessoais, armazenados pela Toy Talk, parceira da Mattel. Assim, toda vez que a criança referir-se a uma informação "importante" já dita (coletada), ao acessar o bando de dados, o brinquedo saberá qual é essa informação – gostos pessoais e preferências – e irá fornecê-la à criança (LINN, 2015).

Linn – que é professora de psiquiatria de Harvard – ressalta que "quando crianças falam com brinquedos, elas podem revelar segredos, trabalhar experiências perturbadoras e explorar seus sonhos e esperanças. Conversas com brinquedos são janelas para seus corações e mentes." (LINN, 2015). São nessas situações que informações íntimas e privadas da criança, e até de pessoas próximas a ela, são coletadas e armazenadas, sem nenhuma garantia de como serão processadas e como (ou, ainda, se) serão protegidas e, ao final, eliminadas.[7]

Em novembro de 2015, o jornal britânico The Guardian publicou matéria relatando os problemas de segurança do brinquedo, contendo comentários do pesquisador em segurança norte americano Matt Jakubowski à NBC (*National Broadcasting Company*). Para Jakubowski, quando conectada à Internet, a boneca apresenta um alto grau de vulnerabilidade, permitindo um fácil acesso ao sistema, informações da conta e os arquivos de áudio armazenados. "Você pode tirar essa informação e descobrir a casa ou empresa de uma pessoa. É apenas uma questão de tempo até que possamos substituir os seus servidores pelos nossos e mandá-la dizer o que quisermos"[8] (GIBBS, 2015).

[7] "Em última instância, a diversão se transformou em um processo de criação de bases de dados. Quantas vezes a criança acessou o brinquedo? Quais informações ela trocou com ele? Quem tem acesso a essa comunicação e onde os dados são armazenados? O que pode ser feito com eles, além de melhorar a performance do brinquedo e do jogo? Existe um debate complexo sobre o consentimento dos pais e responsáveis para o tratamento de dados pessoais de seus filhos. Ainda que os pais tenham consentido com o uso do brinquedo e instalado um aplicativo que permite que eles controlem a brincadeira, há aspectos nebulosos nessa relação que precisam ser melhor debatidos. O que acontece se uma outra criança brincar junto e se comunicar com a boneca ou jogo? Enquanto cada vez mais brinquedos e jogos se conectam à rede, mais cedo as crianças também passam a utilizar a Internet. Duas certezas provenientes desse cenário são a transformação das práticas de diversão e os desafios constantes para a proteção da privacidade e dos dados pessoais." (TEFFÉ; SOUZA, 2018, p. 33).

[8] Tradução livre de: *"You can take that information and find out a person's house or business. It's just a matter of time until we are able to replace their servers with ours and have her say anything we want."*

A transferência dos dados a partir da boneca até o seu processamento, embora possua um sistema de segurança, é frágil e vulnerável, o que permite, por exemplo, a substituição dos servidores por outro, podendo tomar o controle da boneca, possibilitando a condução da conversa com a criança. Isso porque, o sistema adotado é o SSL (*Secure Socket Layer*), um protocolo adicionado sobre o sistema HTTP (*Hyper Text Transfer Protocol*), o qual resulta no HTTPS (*Hyper Text Transfer Protocol Secure*) (SMITH, 2017, p. 125). Tal protocolo permite uma criptografia dos dados enviados, bem como uma confirmação de autenticidade do servidor, por meio de um sistema de certificação digital.

A Hello Barbie não é o único brinquedo com essas configurações e características. Distribuída pela *Genesis* nos EUA e pela *Vivid* no Reino Unido, outra boneca chamada My Friend Cayla repercutiu, especialmente, na Alemanha. Com um sistema praticamente igual ao da Hello Barbie, o brinquedo foi "banido" pela *Bundesnetzagentur* (uma espécie de "Agência Federal de Intercomunicações") (BBC, 2017). A justificativa da Agência é de que o microfone e a conexão – que nesse caso é realizada via bluetooth – fazem do brinquedo "[...] em um possível instrumento de espionagem não permitido por lei. 'Objetos que ocultam câmeras ou microfones e que podem transmitir dados de forma despercebida ameaçam a esfera privada das pessoas', manifestou em comunicado o presidente da Agência, Jochen Homann." (O DIA, 2017).[9]

No caso alemão, há uma violação da Telekommunikationsgesetz (Lei de Telecomunicações), visto que essa prevê a proibição de vender ou possuir qualquer equipamento que esteja disfarçado de um outro qualquer, inclusive de uso diário, sendo que tal objeto opere por meio da captura da fala, por exemplo (ALEMANHA, 2004).

[9] *"The range of sophisticated sensors embedded in Internet-connected toys, such as microphones, location and movement detectors, touch sensors and cameras magnify the security and privacy risks of hacking and hijacking. Together with voice recognition software, and a capacity for facial recognition processing, these new dataveillance (Clarke, 1988) capabilities generate huge quantities of information about a child and their social context which can be collected and distributed without the family knowing or understanding the implications. In this sense, therefore, there will be a variety of new (as well as those already known) potential risks as the market develops 'concerning information security and both privacy and data protection, which must be considered' (European Commission, 2103, p.1)."* (HOLLOWAY; GREEN, 2016, p. 516). Tradução livre: A gama de sensores sofisticados embutidos em brinquedos conectados à Internet, como microfones, detectores de localização e movimento, sensores de toque e câmeras aumentam os riscos de segurança e privacidade de hackers e sequestros. Juntamente com um software de reconhecimento de voz e uma capacidade de processamento de reconhecimento facial, esses novos recursos de vigilância de dados (Clarke, 1988) geram grandes quantidades de informações sobre uma criança e seu contexto social que podem ser coletadas e distribuídas sem que a família saiba ou compreenda as implicações. Neste sentido, portanto, haverá uma variedade de novos (bem como aqueles já conhecidos) riscos potenciais à medida que o mercado se desenvolve "no que diz respeito à segurança da informação e à privacidade e proteção de dados, que devem ser considerados" (Comissão Europeia, 2103, p .1).

Embora a Hello Barbie não esteja disponível para compra diretamente no Brasil, esta pode ser facilmente adquirida em sites de compras, por meio de importação. Diante dessa realidade, enquanto países como, a título exemplificativo, Alemanha e Estados Unidos da América possuem legislações rígidas e específicas sobre telecomunicações (Telekommunikationsgesetz) e proteção da privacidade online (COPPA – Children's Online Privacy Protection Act of 1998), no Brasil, apenas em 18 de setembro de 2020 é que começou a vigorar a Lei Geral de Proteção de Dados Pessoais, dispondo sobre questões envolvendo coleta de dados e proteção da privacidade online.

2 INTERNET DAS COISAS E A LEGISLAÇÃO BRASILEIRA

A Constituição Federal, conforme notoriedade, garante (artigo 5º, X) que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação." (BRASIL, 1988). De modo mais específico, o Marco Civil da Internet, em seu artigo 3º, acentua entre os princípios do uso da Internet no Brasil a proteção da privacidade e a proteção dos dados pessoais (BRASIL, 2014).

Entre outras garantias e direitos dos usuários da Internet, o Marco Civil da Internet também prevê (artigo 7º, VIII) que o usuário deverá ter "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais [...]". Garante, ainda, que os dados "somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet." (BRASIL, 2014).

A Lei nº 12.965, de 23 de abril de 2014, que instituiu o Marco Civil da Internet, também é inovadora no ponto que apresenta um rol de categorias que auxiliam na definição técnica a fim de facilitar a interpretação da norma (FORTES, 2016, p. 126). O ponto a ser observado, portanto, consiste no que diz respeito à classificação dos *smart objects* com o ordenamento jurídico pátrio.

No que concerne à definição técnica, o Marco Civil da Internet, em seu artigo 5º, II, estabelece que, para os efeitos legais, reconhece-se como "terminal: o computador ou qualquer dispositivo que se conecte à internet;" (BRASIL, 2014). Essa disposição, mais do

que trazer diretrizes de conceituação, traz ao caso dos *smart objects* a consequência de que venha-se a reconhecê-los como terminais e, portanto, sujeitos à legislação referente aos direitos e deveres para o uso da Internet no Brasil.

Uma vez reconhecidos como terminais, os *smart objects* – e entre eles, ressalta-se, os *toys that listen* – são a porta de entrada para um conjunto de funcionalidades que são acessadas pelo objeto, o qual passa a coletar os dados, enviando-os para uma central de tratamento, onde o usuário pode não saber, pelo menos com precisão, qual tratamento seus dados receberão. Ainda, registre-se a dificuldade em realizar uma coleta restrita de dados, na qual somente serão coletados e utilizados os dados estritamente necessários ao funcionamento do *smart object* e/ou, também, somente os dados pelos quais o usuário concedeu permissão para coleta. A Hello Barbie, por exemplo, demonstra a impossibilidade de limitar a coleta somente aos dados necessários para o funcionamento. Uma vez em funcionamento, o brinquedo coleta todos os dados, úteis e não úteis para seu desempenho.

Oportuno destacar que, referente aos *toys that listen*, figuram como usuários as crianças, de modo que, consoante disposição do Estatuto da Criança e do Adolescente, tratam-se de indivíduos que apresentam-se em condição peculiar de desenvolvimento (DIAS, 2016, p. 48). Essa condição faz com que seja observado, entre outras questões, a prioridade no tratamento de problemas, bem como, uma segurança jurídica reforçada aos direitos e garantias fundamentais, em face da teoria da proteção integral. Além de positivar e declarar direitos, a teoria da proteção integral preceitua limitações à atividade intervencionista que ameace ou viole os direitos da criança e do adolescente. Observa-se, ainda, que tal teoria apresenta-se de forma aberta e receptiva de novas bases que contribuam com a promoção de novos direitos e garantias (DIAS, 2016, p. 36), nesse caso, referentes à privacidade e à proteção de seus dados pessoais.

Em que pese a proteção da privacidade e dos dados pessoais já fosse mencionada pelo Marco Civil da Internet e por outros dispositivos legais, nenhuma legislação o fazia de maneira satisfatória e específica, até a promulgação, em 2018, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), que somente passou a vigorar em setembro de 2020. O Brasil carecia de uma legislação específica para proteção da privacidade e dos dados pessoais: "A grande questão é que, ao tempo que a Europa se dedica diretamente ao tema há mais de cinco décadas; os Estados Unidos, ao seu modo, há quase duas décadas; alguns países sul-americanos [...] a cerca de uma década; o Brasil conta com tímidos avanços

indiretos." (BOLESINA, 2017, p. 168-169). Desse modo, somente agora é que o tema da proteção de dados pessoais passou a inserir-se na agenda política brasileira.

Veja-se que, os Estados Unidos contam, desde 1998, com o COPPA (*Children's Online Privacy Protection Act* – Lei de Proteção da Privacidade *Online* da Criança), o qual estabelece diretrizes para coleta de dados de crianças. De acordo com a lei, toda informação que for coletada de indivíduos com menos de 13 anos deve possuir expressa autorização dos pais. Estabelece, ainda, as responsabilidades que um operador de site mantém com a privacidade e com a segurança *online* das crianças, incluindo, ainda, a restrição de utilização de determinados métodos de *marketing* destinados às crianças (COPPA, 1998).

O COPPA determina como "informações pessoais" as informações coletadas *online* que permitem a identificação de um indivíduo, incluindo: a) nome e sobrenome; b) casa ou qualquer outro endereço físico, incluindo nomes de ruas e cidades; c) endereço de e-mail; d) número de telefone; e) "Social Security Number" (semelhante ao Cadastro de Pessoas Físicas no Brasil); f) qualquer outro dado que identifique e que, com isso, permita o contato, físico ou *online* com o indivíduo; ou g) qualquer outra informação que esteja relacionada à criança ou seus pais, coletada online, que possa permitir a identificação com qualquer um dos outros identificadores acima referidos (COPPA, 1998).

Ao observar-se as disposições do COPPA e, verificando o modo de operação dos *toys that listen*, pode-se enquadrá-los sob a égide das normas de proteção da privacidade *online*, uma vez que as crianças, ao falarem com o brinquedo, tem sua fala captada e armazenada em um "banco de dados pessoais". Esse conjunto de dados, por evidente, armazena dados que podem facilmente identificar a criança, como nome, endereço, informações da criança e de todo o ambiente em que convive, incluindo-se pais, familiares, amigos, entre outros. Destaca-se que, o fato de os pais permitirem com que a criança brinque com esses artigos não dá a autorização para que os dados sejam coletados, uma vez que, por exemplo, por condições de hipossuficiência, seja ela técnica ou econômica, pode haver um desconhecimento do modo de operação do brinquedo.

A questão envolvendo a proteção dos dados pessoais de crianças não resume-se apenas aos atos de coleta e tratamento dos dados. O armazenamento dos dados coletados é um fator de risco, por inúmeros motivos. O primeiro envolve a possibilidade de exposição dos dados, visto a fragilidade e vulnerabilidade da proteção. O segundo, envolve a dificuldade na eliminação dos dados pelo usuário, de modo que também a simples destruição do brinquedo

ou a exclusão de um possível cadastro (conta) não gera, necessariamente, a exclusão dos dados já coletados, podendo permanecerem, portanto, armazenados. Diante dessas questões, as empresas que armazenam os dados possuem uma responsabilidade de garantir o seguro armazenamento desses.

Uma outra perspectiva sobre o armazenamento de dados advém do fator de desenvolvimento da criança. Uma vez que a criança se torna adolescente ou adulta, a mesma pode ficar ciente da enorme quantidade de informações que o brinquedo coletou enquanto criança, e pode ter o desejo de deletar tais dados. Contudo, nem a empresa que armazena, nem a legislação, concedem tal prerrogativa a criança (futuro adulto), a qual passa a ficar desamparada.

Ainda nessa seara, suponha-se que a criança, que encontra-se agora na adolescência ou na fase adulta, tem suas informações vazadas. A partir desse vazamento, encontram-se informações privadas desse usuário que, enquanto criança, eram banais e insignificantes, mas agora, passada essa fase, podem ser encaradas de forma a gerar consequências para a profissão ou para a vida pública desse usuário. Ainda que fosse possível a responsabilização da empresa pelo vazamento, as consequência para a vida pessoal podem ser inevitáveis.

No que diz respeito às normas de venda e consumo, ao importar uma boneca Hello Barbie, por exemplo, possíveis problemas envolvendo a segurança do consumidor são tutelados pelo Código de Proteção e Defesa do Consumidor, eis que este impõe a responsabilização ao fornecedor[10] do produto (BRASIL, 1990). Salienta-se que, entre os direitos básicos do consumidor (artigo 6º), estão "a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos", bem como "a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos" (BRASIL, 1990).

A Lei Geral de Proteção de Dados Pessoais[11] trouxe avanços importantíssimos na regulamentação da matéria, concedendo direitos e impondo responsabilidades, aos usuários e

[10] De acordo com o Código de Proteção e Defesa do Consumidor (artigo 3º), "fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, **importação**, exportação, distribuição ou comercialização de produtos ou prestação de serviços." (BRASIL, 1990). (Grifos dos autores).

[11] "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; [...] XII - consentimento: manifestação livre, informada e

empresas, respectivamente. Para fins da análise aqui realizada, é importante destacar que a referida lei estabelece que (artigo 7º, I) o tratamento de dados pessoais poderá ser realizado mediante o fornecimento de consentimento pelo titular (BRASIL, 2018), sendo que, no caso dos brinquedos que ouve, tal consentimento deve ser dado pelos pais/responsáveis.

Note-se que, toda coleta de dados pessoais que ocorrer em território brasileiro está sujeita à legislação. Aqui, um impasse: a Hello Barbie, por exemplo, embora não esteja à disposição, diretamente para compra em lojas nacionais, sua importação é facilmente acessível por meio de companhias como a Amazon, por um custo também acessível (ao acessar o endereço da Amazon, verifica-se a possibilidade de importá-la com facilidade, pelo valor aproximado de $ 75,00[12]). Nesse sentido, o imbróglio consiste em como garantir que empresas estrangeiras, que eventualmente possam ter brinquedos importados ao Brasil, sejam compelidas a observar a legislação pátria. Ainda, considerando-se a situação de transferência internacional de dados pessoais, o problema agrava-se.

Embora a proteção do consumidor e dos dados pessoais seja formalmente prevista em lei, a possibilidade de defasagem na aplicação prática de tais disposições é latente. Evidentemente que a Autoridade Nacional de Proteção de Dados Pessoais, órgão ligado à Presidência da República e criada pela Lei nº 13.853, de 8 julho de 2019, tem competência para fiscalizar o cumprimento da legislação. No entanto, a transnacionalidade das empresas podem ser um fator de empecilho à execução de medidas de coibição de violações aos dados pessoais.

3 POR UMA GARANTIA DOS DIREITOS DE PRIVACIDADE NA INTERNET EM RELAÇÃO AOS DISPOSITIVOS QUE CONSTITUEM A INTERNET DAS COISAS

A Constituição de 1988 é inovadora na ordem constitucional brasileira, no que concerne ao proteção das privacidade. É a primeira Constituição brasileira a assegurar,

inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; [...] XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. (BRASIL, 2018).

[12] As informações podem ser conferidas em: https://www.amazon.com/Barbie-DKF74-Hello-Doll/dp/B012BIBAA2. Acesso em: 26 set. 2020.

expressamente, a inviolabilidade quanto à "intimidade, a vida privada, a honra e a imagem das pessoas", reproduzindo também, de modo aperfeiçoado, a inviolabilidade da casa, bem como, assegurando o "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas", nos termos do artigo 5º, respectivamente, X, XI e XII (BRASIL, 1988).[13]

Além da Constituição Federal, alguns outros dispositivos de legislações, como o Marco Civil da Internet, determinam a proteção da privacidade e dos dados pessoais. No entanto, apenas recentemente é que a matéria passou a ganhar proteção legal específica, com o fim da *vacatio legis* da Lei Geral de Proteção de Dados Pessoais. Com a disseminação da Internet das Coisas, a coleta e o tratamento de dados cresceram exponencialmente, o que corrobora a incorporação, quase tardia, dessa proteção específica.

A Lei Geral de Proteção de Dados Pessoais, embora importante avanço para a regulamentação da matéria no Brasil, pode apresentar certa incompletude. Nesse sentido, propõe-se, como possibilidade para efetivar uma proteção de dados pessoais, com maior relevância no que tange à proteção de dados pessoais *online*, a teoria de Paul Bernal (BERNAL, 2014). Essa base teórica consiste em, além de reconhecer o direito à privacidade na internet, subdividi-lo, abrangendo a proteção de quatro "direitos base", originalmente denominados pelo autor de "*Internet Privacy Rights:* o direito de navegar pela internet com privacidade; o direito de monitorar quem monitora, o direito de deletar os dados pessoais; o direito a uma identidade online." (FORTES, 2016, p. 183).

O primeiro direito base consiste na possibilidade de navegar pelas páginas da internet com privacidade, não absoluta, mas com uma razoável garantia da privacidade durante a navegação (BERNAL, 2014, p. 117-139). Trata-se de possuir a garantia de que, ao acessar as páginas da *web*, o usuário tenha para si a consciência de que está sendo protegido e seus dados não estão sendo coletados indeterminadamente. Evidente que os atuais parâmetros da rede operam naturalmente com a concessão de dados pessoais, a fim de haja uma otimização da experiência na navegação. Por isso, evoca-se uma proporcionalidade, a fim de que haja

[13] A Constituição predecessora, de 1967, apenas assegurava, no artigo 150: "§ 9º - São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas. § 10 - A casa é o asilo inviolável do indivíduo. Ninguém pode penetrar nela, à noite, sem consentimento do morador, a não ser em caso de crime ou desastre, nem durante o dia, fora dos casos e na forma que a lei estabelecer." (BRASIL, 1967). Estas disposições são reproduções quase *ipsis litteris* de dois parágrafos do artigo 141, da Constituição de 1946, a saber: "§ 6º - É inviolável o sigilo da correspondência" e "§ 15 - A casa é o asilo inviolável do indivíduo. Ninguém, poderá nela penetrar à noite, sem consentimento do morador, a não ser para acudir a vítimas de crime ou desastre, nem durante o dia, fora dos casos e pela forma que a lei estabelecer." (BRASIL, 1946).

uma razoabilidade na proteção (FORTES, 2016, p. 184). Nesse sentido, verifica-se que a Lei Geral de Proteção de Dados Pessoais é suficiente.

Analogamente à navegação com privacidade na internet, a utilização dos terminais, ou seja, dos objetos que compõem a Internet das Coisas, pode operar de modo semelhante. Embora não haja a direta navegação da internet, o terminal, ao acessar a internet, o faz de modo a compartilhar dados pessoais. Assim, no caso dos brinquedos que ouvem, para que a boneca possa manter o diálogo com a criança, opera-se uma navegação na internet, com a concessão de dados pessoais, para que haja o retorno de informações necessárias à consubstanciar a a fala do brinquedo.

Como segundo direito, tem-se a prerrogativa de monitorar quem monitora, com o escopo do usuário saber quem monitora, o quê monitora, quando monitora e para quais fins o faz (BERNAL, 2014, p. 144-172). Para a Internet das Coisas, pode-se moldar essa prerrogativa a fim de que o usuário tenha o direito de saber quais dados foram coletados, por quem foram coletados, qual o tratamento está sendo dado, para que fins estão sendo usados, bem como onde estão sendo armazenados. No caso de brinquedos *online* como a Hello Barbie e My Friend Cayla, saber quem monitora os dados pessoais da criança é fundamental, principalmente aos pais, para garantir que não esteja-se operando violações desses dados, garantindo a segurança da criança, o que é imprescindível para um desenvolvimento sadio. Nesse aspecto, ainda que em menor grau, a legislação pátria também é eficiente.

O terceiro direito relaciona-se à conceder ao usuário o direito de deletar seus dados pessoais (BERNAL, 2014, p. 176-200). Cercado em grande complexidade por conta de envolver o direito ao esquecimento – *right to be forgotten* –, o direito de deletar dados pessoais operaria como uma garantia que o usuário, quando não mais quisesse manter disponível ou exposto determinadas informações pessoais, as deletasse. Evidentemente, o direito de deletar dados pessoais na internet não é analisado de modo absoluto, sendo inclusive necessárias determinadas ressalvas, a fim de garantia de direitos de individuais, coletivos e até mesmo públicos. Assim, entre as restrições, pode-se elencar como limitações as razões fiscais, eleitorais, econômicas, comunitárias, administrativas, prevenção e produção probatória de crimes, históricas, jornalística, entre outras situações sociais (FORTES, 2016, p. 185).

Diante dos objetos que constituem a Internet das Coisas, o direito de deletar dados pessoais mostra-se importante instrumento para a garantia da privacidade. Uma vez que o

usuário deixe de utilizar determinado objeto, valer-se da possibilidade de deletar seus dados pessoais armazenados conceder-lhe-á a segurança de que não continuarão sendo tratados. Permitirá, também, a garantia de que os dados que foram concedidos já não mais refletem as características atuais do usuário e, portanto, evita que possíveis contrariedades sejam suscitadas contra o sujeito.

Especialmente no caso dos brinquedos *online*, possuir a prerrogativa de deletar os dados pessoais apresenta-se como fator essencial para a garantia do desenvolvimento sadio e íntegro da criança. O princípio do melhor interesse, aplicado ao caso, direciona para esse sentido. Possibilitar a eliminação de dados pessoais de crianças é condição para que se possa estabelecer uma navegação segura, uma vez que, entende-se por "[...] navegação segura como a competência necessária para se proteger de possíveis riscos ao fazer uso da Internet: manter controle dos dados pessoais (nome completo, endereço, documentos de identificação, informações que possam prejudicar a imagem pessoal, entre outros) [...]." (DUARTE; MIGLORIA; SANTOS, 2013, p. 103). Destaca-se que, em certa medida, a Lei Geral de Proteção de Dados Pessoais também converge nesse ponto.

A criança, por sua condição peculiar de desenvolvimento, apresenta-se com maior grau de vulnerabilidade à exposição de dados pessoais na internet, gerando riscos à sua segurança e à sua privacidade (DIAS, 2016, p. 256). Nesta seara, o direito a deletar os dados pessoais da criança, principalmente após o abandono do brinquedo, é fator que maximiza o direito fundamental à privacidade da infância *online*.

Somando-se a esses, o quarto direito base faz referência à criação de uma identidade *online*, onde, a partir dela, o "indivíduo virtual" não necessite conceder todos os dados pertinentes ao "indivíduo real"[14] (BERNAL, 2014, 234-259). Assim, o usuário poderia conceder um número minimizado de informações pessoais e, portanto, reais, podendo valer-se da identidade *online* a fim de navegar e utilizar as aplicações da internet (FORTES, 2016, p. 202). Para a Internet das Coisas, especialmente os brinquedos *online*, a criação de uma identidade *online* possibilita à criança a não exposição de determinadas informações, como idade, nome, endereço, etc. É um situação que demonstra que o "anonimato *online",* em

[14] Registre-se que, "em definitivo, não existe uma "identidade real" e uma "identidade não-real"; o que existe é uma identidade física e uma identidade virtual, as quais podem ser idênticas ou não, mas ambas são reais e incessantemente relacionais." (BOLESINA, 2017, p. 129).

restritos caso como o dos brinquedos que ouvem, pode trazer benefícios ao usuário. É nesse quarto direito base que a legislação brasileira é silente.

A partir da construção teórica dos "direitos base" – ou para utilizar a expressão vernácula de Paul Bernal, *Internet Privacy Rights* –, observa-se que, esses "direitos base" da privacidade, principalmente quando inseridos na dimensão da internet, englobam a proteção dos dados pessoais.

Partindo do pressuposto de que a privacidade e dados pessoais não se confundem, mas são correlatos, no que é relativo aos brinquedos *online*, mais do que simplesmente proteger os dados da criança e das pessoais que estão à sua volta, necessita-se proceder com a respectiva proteção integral da criança. Essa mostra-se, inclusive, como uma necessidade imperiosa, seja pela condição peculiar de desenvolvimento da criança, que a coloca em uma situação de vulnerabilidade. Veja-se, também, o princípio do melhor interesse da criança, norteador de todo o sistema protetivo e assecuratório da criança e do adolescente, o qual, para o caso em tela, demanda a construção e a efetivação do sistema de direitos e garantias da criança. Nesse sentido, destaca-se que há múltiplos agentes sociais que devem estar envolvidos no processo.

Ao Estado compete assegurar, inclusive por imperativo da legislação consumerista, a regulamentação da comercialização de produtos que possam violar a segurança do consumidor também relacionada à privacidade e aos dados pessoais. Por serem os brinquedos *online* potenciais violadores privacidade, um direito constitucionalmente protegido, há que se proceder com a tomada de alguma ação protetiva, entre as quais pode-se citar: *i)* a proibição da venda de brinquedos desse gênero, com determinações também quanto à importação desses (à semelhança da Alemanha quanto ao brinquedo My Friend Cayla); *ii)* a efetivação de uma rede de proteção da privacidade *online* e dos dados pessoais de crianças e adolescentes.

À sociedade e aos pais e/ou responsáveis, em geral, recai, ainda que indiretamente, por consequência de um dever de cuidado, a cautela de verificar as potencialidades de violações de direitos que carregam os brinquedos como a Hello Barbie e My Friend Cayla. Para tanto, faz-se necessário que haja uma publicidade das informações, sendo que o próprio Código de Proteção e Defesa do Consumidor é expresso ao determinar que é direito do consumidor "a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem." (BRASIL, 1990).

A partir da facilidade de aquisição desses brinquedos por importação, questiona-se a insuficiência de uma legislação internacional que estabeleça diretrizes para a privacidade e para os dados pessoais, bem como estabeleça normas a serem observadas, em âmbito internacional, para a produção e venda de brinquedos que venham a constituir-se como potenciais violadores desses direitos de crianças e adolescentes, essencialmente no âmbito da internet. Tal máxima pode ser construída a partir da Declaração Universal dos Direitos Humanos, uma vez que esta prevê, em seu artigo 12º, que "ninguém será sujeito à interferência na sua vida privada [...]." (DECLARAÇÂO UNIVERSAL DOS DIREITOS HUMANOS, 1948).

Na seara da proteção da privacidade em âmbito internacional, o Brasil, em conjunto com Alemanha, Áustria, Liechtenstein, México e Suíça, aprovaram por consenso, durante a 34ª sessão do Conselho de Direitos Humanos das Nações Unidas (CDH), uma resolução sobre o direito à privacidade na era digital, contando com o copatrocínio de 68 países (BRASIL, 2017). Em que pese a iniciativa esteja apenas iniciando, a resolução busca reafirmar o direito à privacidade já previsto na Declaração Universal de Direitos Humanos e no Pacto Internacional de Direitos Civis e Políticos, conclamando os Estados "[...] a respeitar e proteger o direito à privacidade, a pôr fim a violações, a prover medidas efetivas de reparação e a assegurar que qualquer restrição ao direito à privacidade deverá respeitar os princípios da legalidade, necessidade e proporcionalidade." (BRASIL, 2017).

Os impactos sociais da Internet das Coisas ainda são difíceis de dimensionar. Não obstante isso, compreender o modo de funcionamento dessas tecnologias, especialmente, dos brinquedos que ouvem, podem conduzir à reflexão sobre as potencialidades de violação de direitos, como a privacidade e à proteção dos dados pessoais. A existência de normas, sejam nacionais ou internacionais, são apenas o ponto de partida para a salvaguarda desses direitos.

CONCLUSÃO

Os temas envolvendo regulação da internet são imbrincados e tendem a envolver um conjunto de variáveis extensas. Independente da dimensão da internet, os direitos e garantias fundamentais incidem sobre o território do ciberespaço. A eficácia incide de modo vertical, protegendo o cidadão de possíveis violações do Estado, tais como quebra de sigilo de

correspondências, coleta de dados pessoais em desconformidade com a lei, usurpação do poder investigativo, entre outros. De outro modo, a eficácia também deve ser horizontal, de indivíduo para indivíduo. É a partir dela que imputa-se a responsabilidade das empresas na observância das garantias e direitos constitucionais, inclusive no que diz respeito à privacidade de crianças, e também a garantia de proteção dos respectivos dados pessoais.

Observa-se, no que tange à responsabilização por eventuais violações da privacidade dos indivíduos a partir dos brinquedos que ouvem, uma dificuldade prática, na medida que a importação de *toys that listen* opera a coleta de dados pessoais em território nacional. Por outro lado, há a transferência internacional desses dados, eis que são tratados e armazenados em servidores localizados no exterior.

É certo que, no Brasil, a Lei Geral de Proteção de Dados Pessoais constitui-se como fator de profundo e significativo avanço na temática de proteção de dados pessoais e, consequentemente, na proteção da privacidade. Assim, a nível formal, pode-se equiparar a referida legislação à *General Data Protection Regulation* (GDPR) da União Europeia, bem como às legislações dos Estados Unidos da América de proteção à privacidade e aos dados pessoais.

Observa-se, portanto, que a proteção oferecida pelo ordenamento jurídico brasileiro, ainda que aprimorada, em significativo, pela Lei Geral de Proteção de Dados Pessoais, pode não ser suficiente para a garantia dos direitos de privacidade e proteção de dados pessoais, frente aos brinquedos que ouvem. Enquanto os riscos da *Internet of Toys* ainda não são precisos, pesquisas nas áreas de *privacy by design* e *privacy by default* podem apontar caminhos de inovação na área de proteção da privacidade e de dados pessoais, seja em produtos, seja em processos.

Referências

ALEMANHA. **Telekommunikationsgesetz, vom 22. Juni 2004.** Disponível em: https://www.gesetze-im-internet.de/tkg_2004/index.html#BJNR119000004BJNE009202308. Acesso em: 25 set. 2020.

AMAZON. Disponível em: https://www.amazon.com/Barbie-DKF74-Hello-Doll/dp/B012BIBAA2. Acesso em: 26 set. 2020.

BBC. **German parents told to destroy Cayla dolls over hacking fears.** Publicado em: 17 fev. 2017. Disponível em: http://www.bbc.com/news/world-europe-39002142. Acesso em: 25 set. 2020.

BERNAL, Paul. **Internet Privacy Rights:** Rights to Protect Autonomy. Cambridge (UK): Cambridge University Press, 2014.

BOLESINA, Iuri. **O direito à extimidade:** as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1967.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao67.htm. Acesso em: 26 set. 2020.

BRASIL. Ministério das Relações Exteriores. **Direito à privacidade na era digital.** 2017. Disponível em: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/15971-direito-a-privacidade-na-era-digital. Acesso em: 26 set. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 25 set. 2020.

BRASIL. **Constituição dos Estados Unidos do Brasil (de 18 de setembro de 1946).** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao46.htm. Acesso em: 26 set. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 set. 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 26 set. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 26 set. 2020.

CalOPPA (California Online Privacy Protection Act of 2003). Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC. Acesso em: 26 set. 2020.

COPPA (Children's Online Privacy Protection Act of 1998). Disponível em: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. Acesso em: 26 set. 2020.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. **ONU,** 1948. Disponível em: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 26 set. 2020.

DIAS, Felipe da Veiga. **O Direito à Informação na Infância Online.** Curitiba: Prismas, 2016.

DUARTE, Rosália; MIGLORIA, Rita; SANTOS, Emerson. Fatores associados ao uso seguro da internet entre jovens. **TIC *Kids Online* Brasil 2012:** pesquisa sobre uso da internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2013. Disponível em: http://cetic.br/media/docs/publicacoes/2/tic-kids-online-2012.pdf. Acesso em: 25 set. 2020.

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

GIBBS, Samuel. Hackers can hijack Wi-Fi Hello Barbie to spy on your children. **The Guardian.** Disponível em: https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children. Acesso em: 22 set. 2020.

GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. **Future Generation Computer Systems**, v. 29, n. 7, p. 1645-1660, 2013.

HOLLOWAY, Donell; GREEN, Lelia. The Internet of toys. **Communication Research And Practice**, [s.l.], v. 2, n. 4, p. 506-519, out. 2016. http://dx.doi.org/10.1080/22041451.2016.1266124.

LINN, Susan. Agente Barbie. *In:* **O Estado de São Paulo.** Tradução de Celso Paciornik. Publicado em: 21 mar. 2015. Disponível em: http://alias.estadao.com.br/noticias/geral,agente-barbie,1655077. Acesso em: 26 set. 2020.

MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: FGV Editora, 2018.

MIORANDI, Daniele et al. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks**, v. 10, n. 7, p. 1497-1516, 2012.

O DIA. **Alemanha proíbe venda de boneca por ser capaz de fazer espionagem.** Publicado em: 17 fev. 2017. Disponível em: https://odia.ig.com.br/mundoeciencia/2017-02-17/alemanha-proibe-venda-de-boneca-por-ser-capaz-de-fazer-espionagem.html. Acesso em: 25 set. 2020.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática. 12. ed. São Paulo: Conceito Editorial, 2011.

SMITH, Sean. **The Internet of Risky Things:** Trusting the Devices that Suround Us. Sebastopol: O'Reilly, 2017.

TEFFÉ, Chiara Spadaccini de. SOUZA, Carlos Affonso. Infância Conectada: Direitos e Educação Digital. **TIC Kids Online 2017**: pesquisa sobre uso da internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2018. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/tic_kids_online_2017_livro_eletronico.pdf. Acesso em: 26 set. 2020.