FALHAS DE SEGURANÇA EM BRINQUEDOS INTELIGENTES NA PERSPECTIVA DA LEi GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UMA REVISÃO NARRATIVA DA LITERATURA

Francisco Cavalcante de Sousa[1]
Lara Jéssica da Silva Pontes[2]

Resumo:
Este estudo apresenta uma revisão narrativa da literatura científica sobre brinquedos inteligentes na perspetiva da proteção de dados da criança e do adolescente no ordenamento jurídico brasileiro, especificamente sob a vigência da Lei Geral de Proteção de Dados Pessoais (LGPDP). Busca-se identificar quais são as falhas de segurança encontradas em brinquedos inteligentes através de estudos publicados entre 2016 e 2019 e de que maneira essas vulnerabilidades podem violar a legislação de proteção de dados no Brasil e os pilares da segurança informacional. A partir da literatura científica, identificou-se 27 artigos primários que atenderam aos critérios de seleção da presente revisão narrativa. Como resultado, verificou-se que a maioria dos estudos abordavam falhas de segurança relacionadas à confidencialidade, integridade e disponibilidade dos dados das crianças e que, no geral, as abordagens sobre brinquedos inteligentes analisadas retratam que ainda há brechas significativas relacionadas à segurança das informações dos usuários que precisam ser reparadas para efetivar o uso seguro destes dispositivos. Essas falhas de segurança tornam-se ainda mais ameaçadoras por conta da base de usuário destes brinquedos e pela falta de experiência que os pais têm em relação ao seu uso. Por último, constata-se que as leis devem acompanhar essas novas tecnologias na medida em que elas surgem, para que seja possível alinhar brinquedos inteligentes, segurança e privacidade ao público infantil.
Palavras-chave: Brinquedos Inteligentes; Criança e Adolescente; Internet das Coisas; Segurança de dados pessoais; Vulnerabilidade.

INTRODUÇÃO

De forma geral, os brinquedos desempenham importância significativa para o desenvolvimento cognitivo, motor e educacional das crianças e as acompanham durante toda fase de crescimento. Com a expansão da tecnologia e do comércio informacional, os brinquedos tradicionais tiveram que serem readaptados para atrair o público infantil que, pouco a pouco, tornou-se alvo do mercado de tecnologia, por meio de novas modalidades tecnológicas, como a Internet das Coisas, do inglês *Internet of Things* (IoT). A IoT surgiu para conectar equipamentos do cotidiano à internet em conjunto com aplicações

[1] Graduando do Curso de Direito, Universidade do Estado do Rio Grande do Norte (UERN) - Campus Central, e Técnico em Eletromecânica, Instituto Federal do Ceará (IFCE) - Campus Jaguaribe. E-mail: franciscocavalcante@alu.uern.br
[2] Graduanda do Curso de Tecnologia em Redes de Computadores. Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE) - Campus Jaguaribe. E-mail: larajdspontes@gmail.com

móveis. Nesse sentido, qualquer objeto que possa estar conectado à internet é considerado como um instrumento que pode monitorar, advertir e fiscalizar. A IoT abrange diversos dispositivos, e os brinquedos inteligentes (do inglês, *smarts toys*) estão incluídos entre eles.

Os *smart toys* surgiram por causa da necessidade de criar um brinquedo conectado à internet que pudesse atender às exigências do público infanto juvenil cada vez mais tecnológico. Comparado aos brinquedos tradicionais, os *smart toys* possuem funções extras, dentre elas destacam-se a conexão à *internet*, transferências de dados por meio de *Bluetooth* e/ou *Wi-fi*, sensores de reconhecimento facial e de voz, coleta e análise de dados em larga escala, recursos que permitem interação com o usuário, conexão com terceiros, entre outros.

Frente às novas tecnologias da informação, ordenamentos jurídicos de vários países, como Estados Unidos (EUA) e da União Europeia (UE), vêm adaptando-se para regulamentação de práticas e comportamentos envolvendo a Inteligência Artificial (IA) alinhada a IoT, objetivando impor deveres a empresas e fabricantes e, principalmente, assegurar o exercício dos direitos relativos à proteção de dados das pessoas, especialmente das crianças e adolescentes que necessitam de maior proteção devido sua vulnerabilidade.

No Brasil, a discussão acerca do chamado "direito digital" ganhou maiores proporções a partir da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann. A norma promoveu alterações no Código Penal Brasileiro para tipificar delitos e crimes informáticos, como o ocorrido com a atriz que dá nome a lei (BRASIL, 2012). Dois anos depois, foi sancionada a Lei nº 12.965/2014, denominada de Marco Civil da Internet, que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede (BRASIL, 2014).

Em 2018, foi sancionada a Lei Geral de Proteção de Dados Pessoais (LGPDP), de número 13.709, que estabeleceu direitos, obrigações e regras para coleta, tratamento e compartilhamento de dados dos cidadãos por empresas e pelo Poder Público (BRASIL, 2018). No contexto da globalização, tal legislação representou um avanço considerável do ordenamento jurídico brasileiro para coibir crimes cibernéticos e ampliar a importância da segurança informacional e privacidade virtual enquanto assuntos pertinentes tanto ao Direito Público quanto ao Privado.

Tendo em vista esse contexto jurídico-normativo, esta pesquisa busca apresentar uma abordagem sobre as falhas de segurança em brinquedos inteligentes na perspectiva da LGPDP, enfatizando os dispositivos legais voltados à regulamentação de dados pessoais de crianças e adolescentes enquanto usuários de tecnologias da informação, destacando a importância de estudos científicos sobre *smarts toys* e traçando novas perspectivas para regulamentação dos brinquedos inteligentes no Brasil. O

interesse pela temática é despertado a partir da necessidade de pesquisas na área, uma vez que, no Brasil e no mundo, os debates acerca da legislação de segurança e privacidade de dados e da aplicabilidade dos brinquedos inteligentes têm promovido novos questionamentos. Além disso, a indústria de brinquedos no Brasil vem crescendo significativamente na última década e os consumidores estão ansiosos para acompanhar as novas tendências desses dispositivos.

Tendo em vista que os brinquedos inteligentes vêm se popularizando e aperfeiçoando, as leis de proteção de dados devem acompanhar essa tendência e regulamentar lacunas que violem os direitos de segurança e privacidade dos usuários. Diante disso, este trabalho apresenta uma revisão narrativa da literatura científica sobre *smarts toys* e proteção de dados da criança e do adolescente, destacando as falhas de segurança de brinquedos inteligentes abordadas em artigos publicados entre 2016 e 2019 e a maneira como essas vulnerabilidades podem violar a lei brasileira de proteção de dados e os pilares da segurança informacional.

1 BRINQUEDOS INTELIGENTES: UMA VISÃO GERAL

Os brinquedos inteligentes são compostos por três partes: (1) brinquedo físico convencional (como um carro ou uma boneca) equipado com componentes adicionais; (2) um dispositivo móvel que fornece serviços móveis que aprimoram suas funcionalidades; e (3) uma aplicação que possibilita a interação entre o brinquedo físico e seu usuário (CARVALHO *et al.* 2018). Estas funções que são adicionadas ao brinquedo físico possuem aplicabilidades providas pela IoT, tais como eletrônicos, sensores e softwares que permitem a comunicação sem fio com outros sistemas computacionais via *Wi-Fi* ou *Bluetooth*, recursos de inteligência artificial, coleta e análise de dados, e aplicativos que permitem configurar as preferências do usuário (PRIOSTE, 2016).

Em relação aos brinquedos tradicionais, as utilidades que os brinquedos inteligentes podem oferecer aos usuários representam um grande avanço tecnológico, embora estes apresentem riscos que podem causar danos ainda maiores se comparados à outros dispositivos IoT, tendo em vista que sua base de usuários é considerada super vulnerável (FANTINATO *et al.*, 2018).

Entre os fatores preocupantes sobre a segurança dos usuários dos brinquedos inteligentes, está o fato de qualquer indivíduo que esteja compartilhando uma rede com o brinquedo poder se conectar à ele via *Bluetooth* ou *Wi-Fi* e por meio disso, ter acesso à dados dos usuários, sem o conhecimento ou intervenção de terceiros (LEAL, 2017). Durante essa conectividade com o brinquedo, é possível

descriptografar[3] comunicações entre dispositivos e também injetar áudios no brinquedo para que as crianças ouçam (VALENTE, 2017).

Também por este ângulo, estudos recentes descobriram que muitos brinquedos inteligentes ocasionaram sérios vazamentos de privacidade ou permitiram rastrear a localização física da criança por meio de GPS. Devido às essas falhas de segurança, governos em todo o mundo tomaram ação para banir alguns desses brinquedos e tratarem sobre requisitos de segurança e privacidade (SASHA *et al.*, 2018). Em consequência disso, nos últimos cinco anos as análises sobre brinquedos inteligentes têm expandido-se consideravelmente, principalmente nos Estados Unidos e nos países da União Europeia. Especialistas e consultores em segurança cibernética demonstraram a facilidade de invadir esses dispositivos e as autoridades americanas e europeias afirmam a necessidade de regulamentação estatutária para indústrias e empresas de *smarts toys*.

Por isso, novas regras e padrões de segurança estão sendo desenvolvidos nesses países para que as crianças não sejam "atacadas" por pessoas mal intencionadas, como o *Technical Regulation about Toy Safety (2009)*[4], do Conselho Internacional de Brinquedos (do inglês, *International Council of Toy Industrie*s), que estabeleceu critérios de segurança que os brinquedos fabricados devem cumprir antes de poderem ser comercializados na UE.

Em 2015, o Brasil também incorporou o *Technical Regulation about Toy Safety*, em conformidade com resoluções do Mercosul, que estabelece requisitos essenciais de segurança que devem ser cumpridos para comercialização de brinquedos em países do bloco, incluindo Argentina, Brasil, Paraguai, Uruguai e Venezuela (FANTINATO *et al.*, 2018). De forma geral, esse paradigma na América Latina impulsionou mais ainda as questões voltadas à produção e importação de brinquedos no Brasil.

---

[3] Nas comunicações digitais, a criptografia auxilia na proteção de todos os conteúdos transmitidos entre duas ou mais fontes, evitando a interceptação por parte de cibercriminosos, *hackers* e espiões, por exemplo. Quando um conteúdo é encriptado, sua informação é codificada para que seja acessada por pessoas autorizadas.

[4] A legislação da UE visa assegurar que os brinquedos cumprem os requisitos de segurança que se encontram entre os mais rigorosos do mundo, especialmente em relação ao uso de produtos químicos em brinquedos. Os brinquedos também devem cumprir qualquer outra legislação da UE aplicável a eles. Os requisitos essenciais de segurança abrangem riscos gerais quanto a saúde e segurança das crianças, bem como outras pessoas, como pais ou cuidadores; e, riscos particulares, como riscos físicos e mecânicos, de inflamabilidade, químicos, elétricos, de higiene e de radioatividade. A diretiva europeia adaptou o quadro jurídico aos desenvolvimentos tecnológicos e a questões de segurança anteriormente desconhecidas. Disponível em <https://ec.europa.eu/growth/sectors/toys/safety_en>

A indústria de brinquedos brasileira vem crescendo significativamente na última década, como apontou estatísticas da Associação Brasileira dos Fabricantes de Brinquedos (ABRINQ) em 2018[5], e os consumidores estão ansiosos para acompanhar as novas tendências dos brinquedos. Contudo, os *smarts toys* ainda não são tão populares no Brasil quanto nos EUA ou nos países da UE devido ao seu custo relativamente elevado[6]. Enquanto a expansão desses dispositivos não decola no país, eles podem ser adquiridos facilmente por meio de compras em sites de países estrangeiros.

Destarte, os brinquedos conectados à internet serão o futuro das novas gerações – e pasmem, já estão presentes no dia-a-dia de muitas crianças ao redor do mundo, pois grande parte dos jogos, videogames e outros dispositivos já contém alguma conexão com a internet (LEAL, 2017). Resta, enfim, o estabelecimento de normas que adequem esses dispositivos à segurança e à proteção que se espera quando se trata de crianças e adolescentes .

2 SEGURANÇA DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

A Constituição Federal do Brasil de 1988 elencou a inviolabilidade e o sigilo de dados dos cidadãos como uma das garantias constitucionais. Quanto ao sigilo de dados, a Carta Constitucional traz, em seu artigo 5º, XII, a seguinte redação: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial" (BRASIL, 1988).

A expansão da tecnologia com a consequente emergência da privacidade e a necessidade de segurança de dados pessoais contribuíram para a discussão hermenêutica desse dispositivo constitucional, como evidencia Ferraz Júnior (1993, p. 439), "a inviolabilidade do sigilo de dados (art. 5º, XII) é correlata ao direito fundamental à privacidade (art. 5º, X)", sendo desse modo um "direito subjetivo fundamental" com sujeito, conteúdo e objeto.

O direito ainda tem apresentado certas dificuldades em acompanhar e em criar legislação aplicável às diversas relações e conflitos antes não previstos por nossos legisladores, como as questões provenientes das novas tecnologias e do meio digital. As novas tecnologias da informação, em especial, começaram a despertar o interesse dos legisladores devido a necessidade de garantir

[5] De acordo com dados da Associação Brasileira dos Fabricantes de Brinquedos (ABRINQ), o crescimento do faturamento da produção total somado com importações de brinquedos, no Brasil, saltou de 3.460 milhões de reais em 2011, para 6.871,3 milhões de reais em 2018. Disponível em <http://www.abrinq.com.br/economia-e-estatisticas/>

[6] Pode-se citar, como exemplo, o preço da Hello Barbie, que varia entre 136 a 300 reais; o do Cognitoys Dino, variando entre 500 a 700 reais.

segurança jurídica e criar normas que tipificassem crimes cometidos por meio de computadores e outros dispositivos, principalmente por estes envolverem uma base de usuários vulneráveis, como crianças e adolescentes.

O Estatuto da Criança e do Adolescente (ECA) estabelece em seu art. 71, o direito da criança e do adolescente ao lazer e ao acesso a produtos e serviços que devem levar em conta sua condição especial de pessoa em desenvolvimento (BRASIL, 1990). Em seu artIgo 70, o ECA ainda determina como dever de todos prevenir a ocorrência de violação dos direitos da criança e do adolescente, sendo responsabilidade social o cumprimento do conjunto de normas dispostas para prevenção e proteção das crianças enquanto sujeitos de direitos no ordenamento jurídico brasileiro.

Para Leal (2017, p. 182), é importante compreender a maneira como a internet pode potencializar e projetar a vulnerabilidade da criança e do adolescente na rede, devendo-se buscar novas formas e alternativas para neutralizar os perigos que o cercam no ambiente informacional. Sob o prisma jurídico, observa-se a necessidade de um novo olhar sobre a relação entre as novas tecnologias e sua regulamentação jurídica com impactos socialmente eficazes, sejam estes no cotidiano ou até mesmo nas redes.

Algumas leis que regiam o comportamento dos usuários na internet estavam dispersas no ordenamento jurídico brasileiro e não estava posta nenhuma resolução legislativa que unificasse regulamentações específicas para controle e fiscalização de dados dos brasileiros perante o meio informacional. Por isso, observou-se a necessidade de criar de uma legislação própria para coibir crimes cibernéticos.

As discussões advindas das novas tecnologias virtuais vinculadas à expansão da Internet das Coisas deram origem, no Brasil, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, e ao Marco Civil da Internet por meio da Lei n° 12.965/2014. Com maior relevância para os fins deste estudo, o Marco Civil assegura ao usuário a inviolabilidade de sua intimidade e vida privada e prevê indenização por dano material ou moral decorrente de sua violação, além do sigilo do fluxo das comunicações privadas armazenadas, exceto por ordem judicial, bem como o direito ao não fornecimento dos dados pessoais a terceiros.

Recentemente, a legislação brasileira teve um grande avanço quanto proteção de dados por meio da Lei nº 13.709/2018, denominada de Lei Geral de Proteção de Dados Pessoais (LGPDP). Ela altera a lei do Marco Civil da Internet, tornando-se o mais recente instituto jurídico brasileiro de proteção de dados pessoais. A nova legislação estabelece direitos, obrigações e regras para coleta, tratamento e compartilhamento de dados de cidadãos brasileiros tanto por empresas como pelo Poder Público para

garantir a privacidade e segurança dos dados dos usuários e incluir tópicos que não estavam contidos na legislação anterior. Nessa regulamentação, é dedicado uma seção[7] exclusiva para o estabelecimento de regras de condutas nos casos que envolvem o tratamento de dados pessoais de crianças e adolescentes. Dentre as normas, destaca-se desde a maneira como o consentimento ao coletar informações pessoais de crianças deve ser obtido ao dever de transparência por parte dos fabricantes quanto aos dados coletados, sua utilização e seus procedimentos (art. 14), em qualquer que seja o dispositivo, incluindo os recentes e atrativos brinquedos inteligentes.

3 METODOLOGIA

Por se tratar de uma pesquisa de análise bibliográfica, optou-se por realizar uma revisão narrativa da literatura, pois esta descreve e discute o desenvolvimento ou o 'estado da arte' de um determinado assunto, sob ponto de vista teórico ou contextual. As revisões narrativas desempenham "papel fundamental para a educação continuada pois, permitem ao leitor adquirir e atualizar o conhecimento sobre uma temática específica em curto espaço de tempo", contribuindo para compreender o estado da arte de determinado tema ou linha de pesquisa (ROTHER, 2007).

Para realizar a revisão narrativa, considerou-se as seguintes etapas: identificação do tema principal e definição das informações à serem extraídas; elaboração da questão de pesquisa; estabelecimento de critérios para incluir os artigos; avaliação dos textos na íntegra; síntese dos resultados e; conclusão. Busca-se responder quais são as falhas de segurança dos brinquedos inteligentes que violam as leis de proteção de dados pessoais da criança e do adolescente e os pilares da segurança da informação no Brasil apresentados em artigos publicados entre 2016 e 2019.

Quanto aos critérios inclusivos, foram elencados as seguintes restrições: estudos publicados entre os anos de 2016 e 2019, estudos *online* disponíveis de forma gratuita; estudos relacionados à tecnologia da informação e ciências sociais; estudos que possuíam formatos de artigo; estudos não repetidos e estudos que abordassem brinquedos inteligentes. A pesquisa foi realizada na Base de Dados *Scopus*[8] no dia 8 de Janeiro de 2019. A busca dos artigos foi realizada incluindo as seguintes palavras-chaves: *smart toys*, *intelligent toys* e *smart dolls*. Os critérios de inclusão foram aplicados no

[7] Lei nº 13.709/2018, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Seção III Do Tratamento de Dados Pessoais de Crianças e de Adolescentes.* Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>

[8] "Scopus." https://www.scopus.com/. Acessado em 8 jan. 2019.

título, resumo e palavras-chaves por meio de delimitadores de pesquisa da própria base de dados e algumas ferramentas providas pelo software *EndNote X9*[9].

4 RESULTADOS E DISCUSSÃO

Nesta seção, analisa-se a literatura, o "estado da arte" e os resultados do estudo dos artigos selecionados. De uma amostra inicial de 240 trabalhos, identificou-se 27 estudos primários (11,25%) que atenderam aos critérios de seleção da presente revisão narrativa. A busca na base de dados *Scopus* resultou na Tabela 1, que apresenta o resultado da busca e os critérios utilizados para inclusão das publicações acompanhados dos quantitativos de cada item da seleção.

Tabela 1. Resultado da busca após a aplicação dos critérios de seleção

Base de dados Scopus	
Critérios inclusivos:	**Resultados:**
Estudos com acesso livre:	240
Estudos publicados entre 2016-2019	108
Estudos que sejam da área da tecnologia da informação e ciências sociais:	79
Estudos com formato de artigo:	62
Estudos não repetidos	60
Estudos que abordem brinquedos inteligentes	27

Fonte: Elaborado pelos autores.

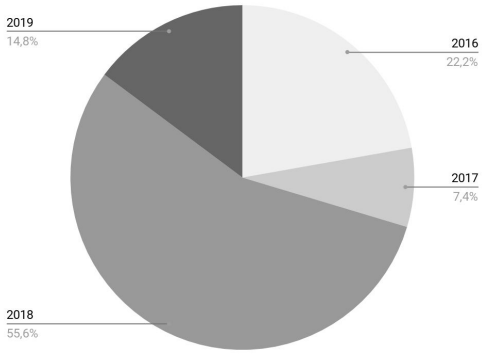
Da amostra inicial, 108 (45%) estudos foram publicados entre 2016 e 2019 e 79 (32,91%) das publicações abordavam conteúdos das áreas de tecnologia da informação e ciências sociais. Apenas dois estudos estavam repetidos na base de dados, sendo excluídos da revisão, resultando em 60. Por fim, foram selecionados apenas os estudos que abordassem brinquedos inteligentes, totalizando 27 estudos (11,25%) relevantes para este trabalho. Após os artigos passarem pelos critérios de inclusão mencionados anteriormente, verificou-se os artigos na íntegra por meio de leitura estrutural para averiguar se estes realmente respondiam à questão de pesquisa deste trabalho.

O gráfico abaixo evidencia os anos de publicação dos 27 trabalhos selecionados para esta revisão narrativa. Destes, a maioria foram veiculados no ano de 2018. Destaque também para os trabalhos

[9] "EndNote." https://endnote.com/. Acessado em 8 jan. 2019.

incluídos de 2019 que já ocupa 14,8% desta revisão, constatando a atualidade e estado da arte da pesquisa em *smarts toys*.

Gráfico 1. Publicações selecionadas para o estudo por ano.



Fonte: elaborado pelos autores

Referente ao conteúdo das publicações, verificou-se que dentre os estudos que foram analisados, a maioria deles abordavam falhas de segurança relacionadas à confidencialidade, integridade e disponibilidade dos dados das crianças registrados pelos brinquedos conectados.

Na perspectiva brasileira, a Lei Geral de Proteção de Dados Pessoais dedica sessão especial para o tratamento de dados de crianças e adolescentes. A legislação enumera direitos e obrigações visando a privacidade, proteção e segurança de dados dos usuários, desde o consentimento dos pais a transparência por parte dos fabricantes quanto a dados coletados, utilização e procedimentos nos dispositivos.

No caso dos brinquedos inteligentes, relaciona-se vários dispositivos deste instrumento jurídico que se aplicam as falhas de segurança encontradas nos artigos analisados pela presente revisão narrativa. A seguir, elencados as falhas de segurança dos brinquedos e os respectivos estudos que trouxeram como resultados os tópicos discutidos para responder a questão de pesquisa.

4.1. Coleta e armazenamento de dados pessoais em larga escala:

Os brinquedos inteligentes podem armazenar informações pessoais tanto das pais como das crianças. De acordo com os artigos, as informações das crianças que podem ser coletadas variam entre data de aniversário, nome, gênero, fotos, vídeos, áudios, entre outros. Já os dados dos pais que podem ser coletados incluem *email*, endereço, gênero, informações do cartão de crédito, número de telefone, senha do *Wi-fi*, endereço IP, senhas, dentre outros. Esses dados são coletados ao criar uma conta para utilizar o brinquedo inteligente; durante a interação com o brinquedo; e conectividade na rede *Wi-Fi.*

Pode-se dizer que todas essas informações, se acessadas pela pessoa "errada", podem servir como porta de entrada para identificar o usuário e manipular seus dados.

A LGPDP considera, no caso das crianças, que os controladores não deverão condicionar a participação dos titulares em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais *além das estritamente necessárias à atividade*. Além disso, só poderão ser coletados dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados *uma única vez* e *sem armazenamento*, ou para sua proteção.

4.2. Monitoramento de localização do usuário por meio de GPS:

Alguns artigos analisados mencionam que durante o envio e recebimento de informações do brinquedo, é possível que a empresa colete informações sobre a localização. Nesse caso, se algum atacante tiver acesso às informações do brinquedo, é possível que além dele monitorar a localização precisa da criança em tempo real, tenha informações extras sobre o ambiente que a criança se encontra.

4.3. Reconhecimento de face e voz e gravação de imagens e sons:

Com os recursos de inteligência artificial, os brinquedos inteligentes podem utilizar reconhecimento de face e voz para mapear seus usuários de acordo com as diferentes expressões e vozes, com isso, diferenciar pessoas e até mesmo se comportarem de acordo com cada usuário. Também é possível reconhecer emoções e reações por meio das expressões monitoradas, porém, a iniciativa da larga escala de armazenamento de imagens e sons por meio de câmeras sem a garantia da segurança e privacidade das informações vem sendo questionada.

4.4. Senhas padrões para todos os dispositivos:

Os estudos A2, A9, A10 mostraram que ao adquirir um brinquedo inteligente, todos esses dispositivos vêm com uma senha de acesso padrão. Embora os usuários destes brinquedos tenham a opção de alterar a senha, não há nenhum período de expiração que torne a atualização de senha como prática obrigatória. Desse modo, ao deixar que a senha padrão permaneça nas configurações do brinquedo, é possível que invasores de má fé encontrem mais facilidade para ter acesso ao brinquedo e, consequentemente, às informações armazenadas.

4.5. Ausência de consentimento dos pais ou responsáveis para controlar/gerenciar os dados e falta de esclarecimento sobre o tratamento e processamento dos dados:

No conteúdo abordado pelos artigos, a maioria dos fabricantes de brinquedos inteligentes não esclarecem exatamente em suas políticas de privacidade com que propósitos, para onde e por quem os dados armazenados serão tratados. Ainda, não há nenhum tipo de termo de consentimento que os responsáveis pelas crianças possam concordar/discordar sobre o tratamento e processamento desses dados. E tampouco, nenhuma forma dos pais ou responsáveis gerenciar, controlar ou restringir os tipos de dados que estarão disponíveis em caso de perda, roubo ou furto do brinquedo.

Conforme a legislação brasileira, no caso do tratamento que envolve crianças, deverá ser realizado o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Além disso, o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de *forma clara, adequada e ostensiva*, o que não acontece no caso dos brinquedos inteligentes analisados pelos estudos. Dentre os termos que devem ser consentidos pelo titular, estão o pleno conhecimento sobre a finalidade do tratamento, sua forma e duração, identificação do controlador e contato, informações acerca do uso compartilhado e finalidade de dados pelo controlador, responsabilidades dos agentes envolvidos e direitos previstos para o titular.

4.6. Possibilidade de exposição de informações e vinculação à terceiros sem autorização:

Os dados que são coletados durante a interação brinquedo-usuário podem ser armazenados em um banco de dados em que as empresas fabricantes dos brinquedos possui acesso, com o propósito de aperfeiçoar as funcionalidades destes brinquedos. Os artigos analisados demonstram que durante a execução de testes de invasão em brinquedos inteligentes, é possível gerar informações distorcidas/erradas e ainda descriptografar a comunicação entre dispositivos e injetar áudios nos brinquedos para que as crianças ouçam.

Os dados armazenados, *em nenhum caso poderão ser repassados a terceiro sem o consentimento* dos pais ou responsáveis pela criança e as informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível, *consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário*, usando recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

4.7. Não garantia da proteção das informações armazenadas:

Os brinquedos conectados à Internet devem cumprir as normas tradicionais de segurança dos brinquedos comuns e, como serviços online, devem também está em conformidade com as leis de

privacidade digital de seus países (SASHA *et al*, 2018). Entretanto, a maioria das empresas de brinquedos conectados à internet não é clara ou não menciona em seus documentos de política de privacidade como eles garantem a proteção e segurança dos dados de seus usuários (CHOWDHURY, 2018).

CONSIDERAÇÕES FINAIS

No geral, as abordagens sobre brinquedos inteligentes trazidas pelos artigos analisados retratam que ainda há falhas significativas relacionadas à segurança das informações dos usuários que precisam ser reparadas para efetivar o uso seguro destes dispositivos. Essas falhas de segurança se tornam ainda mais ameaçadoras por conta da base de usuário destes brinquedos, que são consideradas como vulneráveis, e pela falta de experiência que os pais têm em relação ao uso dos brinquedos.

Nessa perspectiva, as leis de privacidade e segurança devem acompanhar as tecnologias à medida que estas emergem, para que seja possível alinhar brinquedos inteligentes, segurança e privacidade ao público infantil. No caso brasileiro, a legislação teve um grande avanço quanto proteção de dados por meio da Lei Geral de Proteção de Dados Pessoais que dedica uma seção exclusiva para o estabelecimento de regras de condutas nos casos que envolvem o tratamento de dados pessoais de crianças e adolescentes, mostrando preocupação com a vulnerabilidade desses sujeitos enquanto usuários de tecnologias e detentores de proteção no ordenamento..

Com o presente estudo, compreendeu-se que a medida que a tecnologia vêm surgindo, é necessário adotar novos mecanismos legais que assegurem um crescimento seguro. quais são provedores dos pilares da segurança informacional quanto à confidencialidade, disponibilidade e integridade dos dados de crianças. Nesse sentido, o estudo permitiu refletir sobre a importância do direito enquanto agente de regulamentação do meio digital, essencialmente no que se refere às falhas de segurança encontradas em brinquedos inteligentes que podem trazer sérios problemas que repercutem no mundo jurídico.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Lei n. 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Lex: Estatuto da Criança e do Adolescente. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8069.htm> Acesso em 25 de nov. de 2019.

BRASIL. **Lei n° 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União, Brasília, 30 de Nov. 2012.
BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.
BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>
CHOI, C. **New rules to prevent children's 'smart' toys from being hacked.** ITV news. Publicado em 21 de Novembro de 2018. Disponivel em <https://www.itv.com/news/2018-11-21/new-rules-on-internet-toy-security/>. Acesso em 19 de Janeiro de 2019.
FANTINATO, M. *et al*. **A preliminary study of hello barbie in Brazil and Argentina.** Sustainable cities and society, Elsevier, v. 40, p. 83–90, 2018.
FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 88, p. 439-459, 1 jan. 1993.
GIL, A. C.. **Como elaborar projetos de pesquisa**. 2. ed. SP: Atlas, 1991.
LAKATOS, E.; MARCONI, M. **Metodologia do Trabalho Científico**. SP: Atlas, 1992.
LEAL, L. T. Internet of toys: os brinquedos conectados à internet e o direito da criança e do adolescente. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, vol. 12, p. 175-187, abr./jun. 2017.
MONTEIRO, R. L. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada.** Publicado em 14 de Julho de 2019 e disponivel em <https://www.jota.info/?pagename=paywall&redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>. Acesso em 18 de Dezembro de 2018.
PRIOSTE, C. D. **O adolescente e a internet: laços e embaraços no mundo virtual.** Tese (Doutorado) — Universidade de São Paulo, 2016
REALE, M. **Lições preliminares de Direito.**24ª ed. São Paulo: Saraiva, 1998.
ROTHER, E. T. **Revisão sistemática x revisão narrativa**. Acta Paulista de Enfermagem, São Paulo, v. 20, n. 2, p. 5-6, 2007. Disponivel em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-21002007000200001>. Acesso em 27 de Dez. de 2018.
SOUSA, J. O. F. (Org.). **Ensaios de Direito Público e Privado**. v. 2. Saraiva: São Paulo, 2014.
.

APÊNDICE I
Referências dos Artigos Selecionados para a Revisão

[A1] DELPRINO, F. et al. Abbot. In: ACM. *Advanced User Interfaces* (AVI). [S.l.], 2018. p. 1–9.
[A2] JONES, M. L.; MEURER, K. Can (and should) hello barbie keep a secret? In: IEEE. *Ethics in Engineering, Science and Technology* (ETHICS), 2016 IEEE International Symposium on . [S.l.], 2016. p. 1–6.
[A3] CECCHI, F. et al. Caretoy: An intelligent baby gym: Home-based intervention for infants at risk for neurodevelopmental disorders. *IEEE Robotics & Automation Magazine*, IEEE, v. 23, n. 4, p. 63–72, 2016.

[A4] CANO, S. et al. Design of interactive toy as support tool in stem education for children with special needs. In: SPRINGER. *Iberoamerican Workshop on Human-Computer Interaction*. [S.l.], 2018. p. 113–127.
[A5] LI, Y. et al. Design of music toy car based on smart phone via bluetooth remote control. In: IEEE. *2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*. [S.l.], 2018. p. 1976–1980.
[A6] EKIN, C. C.; CAGILTAY, K.; KARASU, N. Effectiveness of smart toy applications in teaching children with intellectual disability. *Journal of Systems Architecture*, Elsevier, v. 89, p. 41–48, 2018.
[A7] HAYNES, J. et al. A framework for preventing the exploitation of iot smart toys for reconnaissance and exfiltration. In: SPRINGER. *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage* . [S.l.], 2017. p. 581–592.
[A8] WANG, J.-H.; CHEN, C.-C.; WANG, H.-W. Grouping and time-series notifying of periodic data in a real-time streaming system for smart toy claw machine. *Journal of Systems Architecture*, Elsevier, v. 92, p. 12–22, 2019.
[A9] DRUGA, S. et al. How smart are the smart toys?: children and parents' agent interaction and intelligence attribution. In: ACM. *Proceedings of the 17th ACM Conference on Interaction Design and Children*. [S.l.], 2018. p. 231–240.
[A10] SHASHA, S. et al. Playing with danger: A taxonomy and evaluation of threats to smart toys. *IEEE Internet of Things Journal*, IEEE, 2018.
[A11] IHAMÄKI, P.; HELJAKKA, K. The internet of toys, connectedness and character-based play in early education. In: SPRINGER. *Proceedings of the Future Technologies Conference*. [S.l.], 2018. p. 1079–1096
[A12] WILLIAMS, R. et al. My doll says it's ok: a study of children's conformity to a talking doll. In: ACM. *Proceedings of the 17th ACM Conference on Interaction Design and Children*. [S.l.], 2018. p. 625–631
[A13] PLAMONDON, R. et al. Personal digital bodyguards for e-security, e-learning and e-health: A prospective survey. *Pattern Recognition*, Elsevier, v. 81, p. 633–659, 2018.
[A14] STREIFF, J. et al. Who's watching your child? exploring home security risks with smart toy bears. In: IEEE. *Internet-of-Things Design and Implementation (IoTDI), 2018 IEEE/ACM Third International Conference on.* [S.l.], 2018. p. 285–286
[A15] FANTINATO, M. et al. A preliminary study of hello barbie in brazil and argentina. *Sustainable cities and society*, Elsevier, v. 40, p. 83–90, 2018.
[A16] VALENTE, J.; CARDENAS, A. A. Security & privacy in smart toys. In: ACM. *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. [S.l.], 2017. p. 19–24.
[A17] CARVALHO, L. G. de; ELER, M. M. Security requirements and tests for smart toys. In: SPRINGER. *International Conference on Enterprise Information Systems*. [S.l.], 2017. p. 291–312
[A18] ESPINOSA-ARANDA, J. et al. Smart doll: Emotion recognition using embedded deep learning. *Symmetry*, Multidisciplinary Digital Publishing Institute, v. 10, n. 9, p. 387, 2018.
[A19] FAN, M. et al. Smart toy car localization and navigation using projected light. In: IEEE. *Multimedia (ISM), 2015 IEEE International Symposium on.* [S.l.], 2015. p. 399–402.
[A20] MIRONCIKA, S. et al. Smart toys design opportunities for measuring children's fine motor skills development. In: ACM. *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction.* [S.l.], 2018. p. 349–356.
[A21] YANG, J.; LU, Z.; WU, J. Smart-toy-edge-computing-oriented data exchange based on blockchain. *Journal of Systems Architecture*, Elsevier, v. 87, p. 36–48, 2018.
[A22] VERDOODT, V.; CLIFFORD, D.; LIEVENS, E. Toying with children's emotions, the new game in town? the legality of advergames in the eu. *Computer Law & Security Review*, Elsevier, v. 32, n. 4, p. 599–614, 2016

[A23] GOULA-DIMITRIOU, M.; DASYGENIS, M. Teddy bear upgraded with an embedded system to react on feelings. In: IEEE. *Modern Circuits and Systems Technologies (MOCAST), 2016 5th International Conference on*. [S.l.], 2016. p. 1–4
[A24] CHOWDHURY, W. Toys that talk to strangers: A look at the privacy policies of connected toys. In: SPRINGER. *Proceedings of the Future Technologies Conference*. [S.l.], 2018. p. 152–158.
[A25] EKIN, C. Ç.; ÇAĞILTAY, K.; KARASU, N. Usability study of a smart toy on students with intellectual disabilities. *Journal of Systems Architecture*, Elsevier, v. 89, p. 95–102, 2018.
[A26] WELCH, S.; SMITH, P. The user experience of disney infinity. In: SPRINGER.*International Conference on Virtual, Augmented and Mixed Reality.* [S.l.], 2016. p. 81–91.
[A27] BRITO, R.; DIAS, P.; OLIVEIRA, G. Young children, digital media and smart toys: How perceptions shape adoption and domestication. *British Journal of Educational Technology*, Wiley Online Library, v. 49, n. 5, p. 807–820, 2018.