UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ARTES, CIÊNCIAS E HUMANIDADES
PROGRAMA DE PÓS-GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

OTÁVIO DE PAULA ALBUQUERQUE

**Proposta de ferramenta de controle parental para brinquedos inteligentes
baseada em regras de privacidade**

São Paulo

2020

OTÁVIO DE PAULA ALBUQUERQUE

**Proposta de ferramenta de controle parental para brinquedos inteligentes
baseada em regras de privacidade**

Dissertação apresentada à Escola de Artes, Ciências e Humanidades da Universidade de São Paulo para obtenção do título de Mestre em Ciências pelo Programa de Pós-graduação em Sistemas de Informação.

Área de concentração: Metodologia e Técnicas da Computação

Versão corrigida contendo as alterações solicitadas pela comissão julgadora em 13 de março de 2020. A versão original encontra-se em acervo reservado na Biblioteca da EACH-USP e na Biblioteca Digital de Teses e Dissertações da USP (BDTD), de acordo com a Resolução CoPGr 6018, de 13 de outubro de 2011.

Orientador: Prof. Dr. Marcelo Fantinato

São Paulo

2020

Autorizo a reprodução e divulgação total ou parcial deste trabalho, por qualquer meio convencional ou eletrônico, para fins de estudo e pesquisa, desde que citada a fonte.

CATALOGAÇÃO-NA-PUBLICAÇÃO

(Universidade de São Paulo. Escola de Artes, Ciências e Humanidades. Biblioteca)

CRB 8 - 4936

Albuquerque, Otávio de Paula

Proposta de ferramenta de controle parental para brinquedos inteligentes baseada em regras de privacidade / Otávio de Paula Albuquerque ; orientador, Marcelo Fantinato. – 2020.

162 f : il.

Dissertação (Mestrado em Ciências) - Programa de Pós-Graduação em Sistemas de Informação, Escola de Artes, Ciências e Humanidades, Universidade de São Paulo.

Versão corrigida

1. Desenvolvimento de software. 2. Brinquedos - Programação e programas; Controle. 3. Computação aplicada. 4. Privacidade. I. Fantinato, Marcelo, orient. II. Título

CDD 22. ed. – 005.12

Dissertação de autoria de Otávio de Paula Albuquerque, sob o título “**Proposta de ferramenta de controle parental para brinquedos inteligentes baseada em regras de privacidade**”, apresentada à Escola de Artes, Ciências e Humanidades da Universidade de São Paulo, para obtenção do título de Mestre em Ciências pelo Programa de Pós-graduação em Sistemas de Informação, na área de concentração Metodologia e Técnicas da Computação, aprovada em 13 de março de 2020 pela comissão julgadora constituída pelos doutores:

Prof. Dr. Marcelo Fantinato

Instituição: Escola de Artes, Ciências e Humanidades - Universidade de São Paulo
Presidente

Prof. Dra. Renata Pontin de Mattos Fortes

Instituição: Instituto de Ciências Matemáticas e de Computação - Univerisdade de São Paulo

---

Prof. Dr. Cristiano Maciel

Instituição: Instituto de Computação - Universidade Federal do Mato Grosso

À minha avó, que não pôde ver minhas vitórias, mas que esteve comigo em minhas lutas.

Tu sempre serás minha mariposa.

Agradecimentos

Agradeço primeiramente às pessoas que estão comigo desde o começo, meu pai Emilton e minha mãe Ivoneide, obrigado por todos os ensinamentos, carinhos, conselhos, dedicação e esforço para que eu pudesse alcançar meus objetivos; sei que minhas conquistas são de vocês, e saibam que são por vocês. Vocês são meu espelho! Agradeço também ao meu irmão Caio, pela companhia e conversas e pela pessoa que é, és meu orgulho mano!

À minha noiva Lisandra por me apoiar, incentivar e sempre acreditar em mim e no meu potencial. Obrigado por esses anos de companheirismo, amor e por ser essa pessoa tão maravilhosa. Agradeço todos os dias por ter você em minha vida, és a minha inspiração e o motivo de querer ser melhor! Amo você!

À minha tia Ilza, tio Américo e primos, Sérgio, Izabela e Diana por me acolherem tão bem e me apoiarem nessa jornada de me tornar um mestre pela Universidade de São Paulo. Essa caminhada foi bem mais fácil com vocês por perto.

Agradeço aos amigos que o mestrado me deu, Leonardo, Jhonatan e Camila, obrigado pela amizade e pelo apoio dentro e fora da sala de aula. À minha dupla de trabalhos Marina por deixar as matérias um pouco mais fáceis. Aos amigos de longa data que por mais que estivessem longe nunca deixaram de apoiar.

Ao meu orientador, professor Dr. Marcelo Fantinato pela oportunidade, ensinamento, suporte e confiança - foram essenciais para que eu chegasse até aqui. Ao professor Dr. Patrick Hung pela oportunidade de poder expandir as barreiras do mestrado, adquirir mais conhecimento, e vivenciar novas experiências no Canadá. Agradeço a CAPES por ter fomentado esta pesquisa através de uma bolsa de pesquisa.

Gostaria de agradecer as pessoas que fizeram e fazem parte da minha vida, que me ajudaram direta ou indiretamente nessa caminhada. A vida não é fácil, mas é melhor quando se tem pessoas com quem se pode contar. Meu mais sincero obrigado!

“Que os vossos esforços desafiem as impossibilidades; lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível”
(Charles Chaplin)

Resumo

ALBUQUERQUE, Otávio de Paula. **Proposta de ferramenta de controle parental para brinquedos inteligentes baseada em regras de privacidade**. 2020. 162 f.

Dissertação (Mestrado em Ciências) – Escola de Artes, Ciências e Humanidades, Universidade de São Paulo, São Paulo, 2020.

Com a inserção do mundo na era digital surgiram os brinquedos inteligentes. Um brinquedo inteligente consiste em um dispositivo físico conectado com serviços móveis através de redes sem fio, proporcionando para a criança, brincadeiras mais interativas. Com os brinquedos inteligentes surgiram questionamentos de pais e pesquisadores sobre os riscos que eles podem oferecer. As maiores preocupações da área estão relacionadas a grande capacidade de coleta de dados que um brinquedo inteligente possui, e com o usuário ser uma criança que geralmente não compreende ou têm pouca preocupação com sua própria segurança e privacidade. Existem ferramentas como o controle parental em desenvolvimento pela comunidade, visam fornecer funcionalidades que auxiliem os pais na preservação da segurança e privacidade das crianças por meio do controle de acesso. No entanto, as ferramentas disponíveis no mercado não acompanharam às necessidades das recentes mudanças tecnológicas dos ambientes computacionais atuais. No ambiente de computação para brinquedos, isso torna-se mais evidente por causa da maioria dos serviços móveis vinculados aos brinquedos serem sensíveis ao contexto, ou seja, precisarem coletar dados para fornecer 100% de seus serviços. Além de funcionalidades principais de controle de acesso, há a necessidade da implementação de funcionalidades complementares que auxiliem os pais na tomada de decisão e no entendimento relacionado ao ambiente, conscientizando-os sobre as consequências do acesso a dados, os riscos que envolvem o ambiente, e disponibilizando o acesso fácil a conteúdos relacionados à proteção de dados infantis etc. Com o intuito de estabelecer uma proposta de ferramenta de controle parental para brinquedos inteligentes baseada em regras de privacidade, identificou-se um conjunto de requisitos com 19 funcionais e 18 não-funcionais, considerados desejáveis para tal tipo de ferramenta. Também se criou um modelo conceitual da ferramenta, no qual é apresentada uma visão geral das funcionalidades dela. Baseado no modelo, implementou-se então um protótipo funcional da ferramenta. Os requisitos e o protótipo foram avaliados, por meio de um questionário, quanto o grau da importância dos requisitos para uma ferramenta de controle parental e o grau de satisfação da implementação deles no protótipo. A análise dos resultados das respostas de 10 pesquisadores especialistas da área foi realizada quantitativa e qualitativamente. Na análise quantitativa confirmou-se que os requisitos são considerados importantes para compor a ferramenta, sendo os não-funcionais, em médias gerais, mais relevantes; além de demonstrar resultados expressivos relacionados a avaliação do protótipo. Para a análise qualitativa, analisou-se o conteúdo das respostas subjetivas referentes às sugestões de novas ideias de requisitos e recomendações para melhoria do protótipo. Pretende-se com isso, disponibilizar um modelo de ferramenta de controle parental para servir como base para empresas de brinquedos inteligentes desenvolverem suas ferramentas, além de contribuir para o avanço na pesquisa da área de brinquedos inteligentes, relacionados, principalmente, a temas de privacidade e segurança.

Palavras-chaves: Brinquedos inteligentes. Computação para brinquedo. Privacidade. Segurança. Controle parental.

Abstract

ALBUQUERQUE, Otávio de Paula. **Proposal of a parental control tool for smart toys based on privacy rules**. 2020. 162 p. Dissertation (Master of Science) – School of Arts, Sciences and Humanities, University of São Paulo, São Paulo, 2020.

With the insertion of the world in the digital age, intelligent toys emerged. A smart toy consists of a physical device connected with mobile services over wireless networks, providing the child with more interactive play. However, with smart toy, questions arose from parents and researchers about the risks that such toys may offer. The biggest concerns in the area are related to the great data collection capacity that a smart toy has, and to the user being a child who generally does not understand or have little concern for their own security and privacy. There are tools such as parental control being developed by the community, which aim to provide functionalities that assist parents in preserving children's security and privacy through access control. However, the tools available on the market have not kept up with the needs of recent technological changes in today's computing environments. In the toy computing environment, this becomes more evident because most mobile services linked to toys are context sensitive, that is, they need to collect data to provide 100% of their services. In addition to the main access control features, there is a need to implement complementary features that assist parents in decision-making and understanding related to the environment, making them aware of the consequences of accessing data, the risks that involve the environment, and providing easy access to content related to the protection of children's data, etc. In order to establish a proposal for a parental control tool for smart toys based on privacy rules, a set of requirements was identified with 19 functional and 18 non-functional, considered desirable for this type of tool. A conceptual model of the tool was also created, in which an overview of its functionalities is presented. Based on the model, a functional prototype of the tool was then implemented. The requirements and the prototype were assessed, through a survey, as to how important of the requirements for a parental control tool and how satisfactory with their implementation in the prototype. The analysis of the results of the responses of 10 specialist researchers in the area was carried out quantitatively and qualitatively. In the quantitative analysis it was confirmed that the requirements are considered important to compose the tool, being non-functional, in general averages, more relevant; besides demonstrating expressive results related to the evaluation of the prototype. For the qualitative analysis, the content of the subjective responses regarding the suggestions for new requirements ideas and recommendations for improving the prototype was analyzed. It is intended to provide a model of parental control tool to serve as a basis for smart toy companies to develop their tools, in addition to contributing to the advancement of research in the area of smart toys, mainly related to privacy and security issues.

Keywords: Smart toys. Toy computing. Privacy. Security. Parental control.

Lista de figuras

Figura 1 – Modelo conceitual de regras de privacidade retirado de Rafferty <i>et al.</i> (2017).	21
Figura 2 – Fluxo de processo iterativo de software	26
Figura 3 – Exemplos de brinquedos inteligentes.	30
Figura 4 – Modelo de ambiente de computação para brinquedo.	38
Figura 5 – Estrutura hierárquica do propósito.	41
Figura 6 – Tomada de decisão do controle de acesso.	44
Figura 7 – Resumo da seleção dos artigos	50
Figura 8 – Taxonomia para extração e classificação de dados	51
Figura 9 – Distribuição dos estudos primários por tipo de veículo e ano.	55
Figura 10 – Classificação de artigos pelos princípios de privacidade da ISO	55
Figura 11 – Classificação dos documentos por propriedades e requisitos de segurança (subprincípios de segurança da informação)	57
Figura 12 – Classificação de artigos por técnicas de preservação da privacidade . . .	58
Figura 13 – Análise cruzada entre riscos identificados (princípios de privacidade) e soluções propostas (técnicas de preservação da privacidade)	60
Figura 14 – Ambiente de computação para brinquedos	71
Figura 15 – Casos de uso das funcionalidades principais	83
Figura 16 – Casos de uso da criação do perfil de usuário.	85
Figura 17 – Diagrama de atividade da criação do perfil de usuário.	85
Figura 18 – Casos de uso da criação de regra de privacidade.	87
Figura 19 – Diagrama de atividade da criação de regra de privacidade.	87
Figura 20 – Casos de uso gerenciar regras de privacidade.	89
Figura 21 – Casos de uso guia de aprendizado da ferramenta.	90
Figura 22 – Casos de uso monitoramento de atividade.	90
Figura 23 – Casos de uso área de Suporte.	91
Figura 24 – Tela de apresentação da ferramenta.	94
Figura 25 – Criação do perfil de usuário.	95
Figura 26 – Telas principais da ferramenta	96
Figura 27 – Subárea guia para os pais	97

Figura 28 – Subárea monitor para os pais	98
Figura 29 – Tela Gerenciar regra	99
Figura 30 – Atualização na política de privacidade	100
Figura 31 – Funcionalidades da área de suporte	101
Figura 32 – Telas criar regra de privacidade	102
Figura 33 – Controle de acesso principal	103
Figura 34 – Controle de acesso estendido	104
Figura 35 – Revisão e confirmação da criação da regra de privacidade	105
Figura 36 – Caixa de diálogo de ajuda nas telas de controle de acesso principal . .	105
Figura 37 – Caixa de diálogo de ajuda nas telas de controle de acesso estendido para propósito e destinatário	106
Figura 38 – Caixa de diálogo de ajuda nas telas de controle de acesso estendido para obrigação e retenção	106
Figura 39 – Tela de modelos de regra de privacidade	107
Figura 40 – Nível de escolaridade	111
Figura 41 – Grau de conhecimento sobre brinquedos inteligentes	112
Figura 42 – Grau de importância dos requisitos funcionais	113
Figura 43 – Média das avaliações do grau de importância dos requisitos funcionais .	113
Figura 44 – Grau de importância dos requisitos não-funcionais	114
Figura 45 – Média das avaliações do grau de importância dos requisitos não-funcionais	115
Figura 46 – Grau de satisfação da implementação dos requisitos funcionais no protótipo	116
Figura 47 – Média das avaliações do grau de satisfação da implementação do protótipo	116

Lista de quadros

Quadro 1 – Comparação entre brinquedos tradicionais, eletrônicos e inteligente. . .	28
Quadro 2 – Propriedades genéricas de brinquedos inteligentes	29
Quadro 3 – Principais ameaças à privacidade de dados	35
Quadro 4 – Diretriz de design para integração de tecnologias de computação per- vasiva em brinquedos.	37
Quadro 5 – Fases e suas respectivas etapas de uma revisão sistemática	45
Quadro 6 – Cumprimento dos requisitos de controle parental por normas legais. .	80

Lista de tabelas

Tabela 1 – <i>String</i> de busca final*	48
Tabela 2 – Estudos primários (TV: Tipo de veículo; J – Journal; C – Conference)	54
Tabela 3 – Riscos específicos do domínio e soluções propostas (Rec. = Recomendações)	61
Tabela 4 – Requisitos funcionais para ferramentas de controle parental	73
Tabela 5 – Requisitos não-funcionais de usabilidade para ferramenta de controle parental	76
Tabela 6 – Requisito não-funcional de interoperabilidade para ferramenta de con- trole parental	76
Tabela 7 – Requisito não-funcional de implementação para ferramenta de controle parental	76
Tabela 8 – Requisitos não-funcionais de segurança para ferramenta de controle parental	77
Tabela 9 – Requisitos não-funcionais legais para ferramenta de controle parental .	78

Sumário

1	Introdução	16
1.1	<i>Motivação e justificativa . . . . .</i>	18
1.2	<i>Problema de pesquisa . . . . .</i>	19
1.3	<i>Objetivos . . . . .</i>	22
1.4	<i>Método de pesquisa . . . . .</i>	23
2	Fundamentação teórica	27
2.1	<i>Brinquedos inteligentes . . . . .</i>	27
2.2	<i>Dados de contexto de brinquedo inteligente . . . . .</i>	31
2.3	<i>Segurança, privacidade e proteção de dados infantis . . . . .</i>	32
2.3.1	Segurança infantil	32
2.3.2	Privacidade e proteção de dados infantis	33
2.4	<i>Computação para brinquedo . . . . .</i>	36
2.4.1	Modelo de computação para brinquedo	38
2.4.2	Controle de acesso	40
2.5	<i>Modelo conceitual Rafferty . . . . .</i>	41
2.6	<i>Considerações finais . . . . .</i>	44
3	Trabalhos relacionados	45
3.1	<i>Protocolo da revisão da literatura . . . . .</i>	45
3.1.1	Planejamento da revisão	46
3.1.2	Realização da revisão	49
3.2	<i>Análise de conteúdo . . . . .</i>	50
3.2.1	Análise de conteúdo quantitativa	51
3.2.2	Análise de conteúdo qualitativa	52
3.3	<i>Resultados e considerações . . . . .</i>	53
3.3.1	Riscos técnicos e soluções propostas	55
3.3.2	Riscos específicos do domínio e soluções propostas	59
3.4	<i>Discussão . . . . .</i>	63
3.4.1	Soluções para mitigar os riscos à privacidade das crianças relaciona- das ao brinquedo inteligente	63

3.5	<i>Considerações finais</i>	67
4	Requisitos da ferramenta de controle parental	69
4.1	<i>Requisitos da ferramenta</i>	70
4.2	<i>Atos e regulamentos legais</i>	79
4.3	<i>Considerações finais</i>	81
5	Modelo conceitual da ferramenta de controle parental	83
5.1	<i>Visão geral das funcionalidades</i>	83
5.2	<i>Criação do perfil de usuário</i>	84
5.3	<i>Criação da regra de privacidade</i>	86
5.4	<i>Gestão das regras de privacidade</i>	88
5.5	<i>Aprendizado e monitoramento</i>	89
5.6	<i>Suporte aos pais</i>	90
5.7	<i>Considerações finais</i>	91
6	Protótipo da ferramenta de controle parental	92
6.1	<i>Introdução da ferramenta</i>	94
6.2	<i>Criação do perfil de usuário</i>	94
6.3	<i>Áreas principais da ferramenta</i>	96
6.3.1	Área dos pais	96
6.3.2	Gerenciar regra	98
6.3.3	Área de suporte	99
6.4	<i>Criação da regra de privacidade</i>	101
6.5	<i>Considerações finais</i>	107
7	Avaliação dos requisitos e do protótipo da ferramenta	108
7.1	<i>Escopo da avaliação</i>	108
7.2	<i>Planejamento de avaliação</i>	109
7.3	<i>Execução da avaliação</i>	110
7.4	<i>Resultados e discussões</i>	111
7.4.1	Análises quantitativa	111
7.4.2	Análise qualitativa	117
7.5	<i>Considerações finais</i>	119

8	Conclusão	120
8.1	<i>Limitações . . . . .</i>	121
8.2	<i>Trabalhos futuros . . . . .</i>	121
	Referências¹	122
	Apêndice A – Questionário	130
	Apêndice B – Dados qualitativos	144
	Anexo A – Anexo	147

---

¹ De acordo com a Associação Brasileira de Normas Técnicas. NBR 6023.

1 Introdução

Desde os seus primeiros exemplares, há milhares de anos, os brinquedos fazem parte de nossa vida. Eles trazem consigo uma variedade de aplicações, incluindo educação, lazer e socialização (RAFFERTY; HUNG, 2015), proporcionando diversos benefícios para a criança, entre eles o desenvolvimento cognitivo, motor, social e linguístico (FROST; WORTHAM; REIFEL, 2001). Com o passar do tempo os brinquedos foram evoluindo em paralelo à sociedade, se adaptando aos períodos históricos e tornando-se mais atrativos em seus respectivos contextos. Por mais que tecnologias, culturas e interesses mudem, as escolhas de brinquedos e brincadeiras das crianças, dos seus jogos, das convenções e das temporadas para jogá-los, perduram, genericamente falando. (FROST, 2010).

Um dos primeiros exemplares descrito na literatura é uma boneca feita de argila e cabelos humanos, encontrada em escavações nos locais onde civilizações egípcias habitavam. Posteriormente, seguindo uma linha do tempo genérica, apareceram jogos de tabuleiro, bolas de couro, animais de pelúcia. Nessa época, os brinquedos ainda eram objetos artesanais, geralmente feitos pelos próprios pais. Após a Revolução Industrial e os avanços nas tecnologias para agilizar a fabricação, foi criada a manufatura em massa, e com isso os brinquedos se tornaram amplamente disponíveis, consolidando um novo mercado (FROST; WORTHAM; REIFEL, 2001).

Com o advento da computação, as funcionalidades de um brinquedo tradicional foram aprimoradas. O que antes eram apenas brinquedos físicos onde a imaginação era necessária para a criação das interações entre o brinquedo e a criança, agora são brinquedos com tecnologias eletrônicas embutidas (ex.: dispositivos móveis, botões, telas e sensores), resultando em novos tipos de interações e formas de brincar, emergindo assim o brinquedo eletrônico.

Com a inserção do mundo na era digital, os brinquedos também começaram a fazer parte desse contexto, surgindo então os brinquedos inteligentes. Brinquedos inteligentes são dispositivos que consistem em componentes físicos conectados a sistemas de computador com serviços de comunicação *on-line* (HUNG *et al.*, 2016). Conforme Tang e Hung (2017), um brinquedo inteligente neste contexto pode ser efetivamente considerado uma Internet das Coisas (*Internet of things* - IoT) com funcionalidades de Inteligência Artificial (*Artificial*

intelligence - AI), que pode fornecer experiências de Realidade Aumentada (*Augmented reality* - AR) aos usuários.

Junto ao surgimento dos brinquedos inteligentes surgiu a computação para brinquedo (*toy computing*), que consiste numa configuração na qual o componente de brinquedo físico interage com um dispositivo móvel que se conecta a um ou mais serviços móveis para facilitar a jogabilidade (RAFFERTY; HUNG, 2015). Exemplos de computação para brinquedo difundidos na literatura, dão-se por brinquedos inteligentes que, por meio da conexão com serviços de inteligência artificial, podem simular linguagem natural para a construção de diálogos interativos entre o brinquedo e a criança (ex: Mattel Hello Barbie¹), ou por brinquedos que juntam aspectos do mundo virtual com o real por meio de um dispositivo de câmera, assim oferecendo experiências de realidade aumentada (ex: Niantic Pokémon GO²).

No entanto, pais e responsáveis percebem os brinquedos inteligentes como um objeto complexo, tendo em vista os inúmeros dispositivos e sensores em sua estrutura conectados à rede, que implicam em potenciais riscos à privacidade e segurança, assim como a utilização de serviços móveis (FANTINATO *et al.*, 2018a). A tendência é que cada vez mais brinquedos inteligentes integrem serviços e dispositivos tecnológicos como estes.

Outro problema identificado está nos textos longos, complexos e por vezes de difícil acesso, de direitos de propriedade e de políticas de privacidade dos brinquedos inteligentes. Tais problemas dificultam a capacidade dos pais de compreenderem os potenciais riscos vinculados ao brinquedo (MAHMOUD *et al.*, 2018).

O brinquedo Hello Barbie é um caso em foco na literatura, e que tem recebido críticas a respeito de possíveis efeitos negativos em alguns aspectos de segurança e privacidade como o vazamento de dados sensíveis (SHASHA *et al.*, 2018). A criança, por exemplo, pode levar um dos seus brinquedos inteligentes para a mesa de jantar e ele, a partir do microfone conectado em sua estrutura, poderia capturar informações sensíveis de voz em qualquer parte do cômodo e transmitir a terceiros, sem o consentimento, ou até mesmo o conhecimento dos responsáveis pela criança (HAYNES *et al.*, 2017).

¹ Disponível em: <<http://hellobarbiefaq.mattel.com>>. Acesso em: 15 setembro de 2018

² Disponível em: <<https://pokemongolive.com/pt-br>>. Acesso em: 15 setembro de 2018

1.1 *Motivação e justificativa*

Como parte substancial do desenvolvimento humano, os brinquedos continuaram a manter sua presença no dia a dia de bilhões de indivíduos de todas as idades, e não está sendo diferente com os brinquedos inteligente. Uma pesquisa realizada por Juniper Research (2017), empresa especializada em pesquisas de mercados dentro do ecossistema digital, sediada no Reino Unido, informou que o brinquedo inteligente é o novo mercado chave para as empresas de brinquedos e as vendas de brinquedos inteligentes cresceriam de US\$ 2,8 bilhões em 2015 para US\$ 11,3 bilhões até 2020.

Desde o surgimento do conceito de brinquedos inteligentes à grande perspectiva de crescimento do mercado, foram surgindo questionamentos de pais e pesquisadores a respeito da proteção online da criança, principalmente relacionados à privacidade e segurança de dados. Levando em consideração que brinquedos inteligentes são capazes de coletar uma variedade de dados, como texto, imagem, vídeo, som, localização e dados de sensoriamento, o contexto se torna mais complicado do que muitos outros dispositivos inteligentes, em particular, dado que os usuários finais são, primordialmente, crianças em ambientes físicos e sociais (RAFFERTY *et al.*, 2017).

Crianças, geralmente, têm pouca compreensão e/ou cuidado com a sua privacidade, incluindo a privacidade de dados online, e por isso são mais propensas a fornecer informações privadas, o que aumenta a preocupação com possíveis riscos relacionados à privacidade e segurança (HUNG *et al.*, 2016). Por isso, as crianças são consideradas usuários vulneráveis, normalmente incapazes de tomar decisões baseadas em informações de políticas de privacidade como, por exemplo, se concorda ou não com as práticas de coleta e compartilhamento de dados de um aplicativo (CARVALHO; ELER, 2017).

A tendência é que brinquedos inteligentes integrem cada vez mais serviços e dispositivos tecnológicos em sua estrutura, aprimorando suas funcionalidades. Quanto mais componentes tecnológicos envolvidos, maior o número de riscos à privacidade e segurança e, consequentemente, maiores devem ser as precauções tomadas para a proteção virtual e física da criança. A convergência desses dispositivos e serviços móveis acabam dificultando a supervisão dos pais (ITU; UNICEF, 2014).

Por isso, pais precisam de mecanismos eficazes para entender e controlar a privacidade da criança e auxiliar na proteção de dados, sejam eles dados sensíveis ou até

mesmo informações pessoais identificáveis (*Personally Identifiable Information*-PII) (FANTINATO *et al.*, 2018b). Mecanismos computacionais como criação de senha e bloqueio de conteúdos inapropriados em tvs e navegadores de internet são os principais exemplos de funcionalidades de controle de acesso à conteúdo. No entanto, tais mecanismos não atendem à necessidade dos pais quando se trata de proteger as crianças do acesso de terceiros aos seus próprios dados.

Ferramentas que criam regras de privacidade são as mais difundidas no mercado de brinquedos inteligentes, no qual são categorias de ferramentas que habilitam os pais a decidir, de acordo com suas preferências, permitir ou negar a coleta, uso e compartilhamento de certos tipos de PIIs das crianças (RAFFERTY *et al.*, 2017).

Por meio da pesquisa empírica, notou-se que a maioria dos brinquedos inteligentes citados neste trabalho possuem ferramentas de controle de acesso como o controle parental. Entretanto, cada brinquedo possui sua própria ferramenta com diferentes funcionalidades. Até mesmo quando se trata da mesma funcionalidade como no caso da criação de regras de privacidade, os pais e responsáveis terão modelos distintos de aplicação para entender e configurar, dificultando assim o seu uso.

Os pais às vezes têm menos compreensão e conhecimento da internet e dispositivos móveis do que os seus filhos (HUNG; FANTINATO; RAFFERTY, 2016a). Em um estudo, Felt *et al.* (2012) descobriu que apenas 17% dos participantes prestaram atenção às permissões durante a instalação de aplicativos em *smartphones*, e apenas 3% puderam responder corretamente às questões de compreensão de permissão.

Esta é uma enorme desvantagem para o atual sistema de permissões, no qual elucida a necessidade de melhorar a usabilidade de tais ferramentas, considerando a interação entre o usuário e a aplicação, utilizando um conjunto de qualidades ergonômicas e navegabilidade intuitiva para as funcionalidades, facilitando a utilização e a compreensão de sistemas de proteção da privacidade como o controle parental (RAFFERTY; FANTINATO; HUNG, 2015).

1.2 Problema de pesquisa

Ferramentas de controle parental são comumente utilizadas, por exemplo, em smart tvs, navegadores de internet e smartfones, com técnicas genéricas estabelecidas como:

criação de senhas, filtros de palavras-chave e conteúdo, limitação de tempo de uso, monitoramento de atividades. No entanto, a maioria das ferramentas de controle parental não conseguiram acompanhar as novas tendências relacionadas às recentes mudanças tecnológicas e a grande busca pela coleta de dados (FUERTES *et al.*, 2015). As tecnologias utilizadas nos aparelhos eletrônicos alcançaram os brinquedos, criando novas funcionalidades e modos de brincar, mas criando também a preocupação com a privacidade de dados, refletindo na busca e uso de técnicas de controles de acessos mais atuais e complexas como a criação de regras de privacidade.

A coleta e o compartilhamento de dados se faz cada vez mais necessário para que os provedores de serviço possam desempenhar 100% da funcionalidade de suas aplicações, entregando experiências personalizadas a cada usuário. Várias empresas usam os dados coletados para atualizar e modificar os seus produtos e serviços, ou até mesmo vender para fins de *marketing* (MOINI, 2016). Com isso os ambientes atuais exigem controles de acessos mais flexíveis e adaptativos aos diferentes contextos. Isso se aplica no mercado de brinquedos inteligentes e, conseqüentemente, nas funcionalidades que uma ferramenta de controle parental deve prover aos pais, para que a criança possa ter a experiência da brincadeira e a proteção de sua privacidade ao mesmo.

A falta da padronização de um modelo de controle de acesso parental para os brinquedos inteligentes pode acarretar problemas de usabilidade, diferentes tipos de ferramenta com inúmeros modos de configuração dificultam a utilização e o entendimento; funcionalidade, as empresas de brinquedo implementam as funcionalidades que os convém, sem a verdadeira avaliação das necessidades dos pais/responsáveis; e até mesmo de segurança, com ferramentas mal implementadas, e boas práticas de segurança negligenciadas; resultando em ferramentas de controles parentais ineficientes (ITU; UNICEF, 2014).

Rafferty *et al.* (2017) propõem um modelo conceitual de regras de privacidade estendida para brinquedos inteligentes, como mostrado na figura 1. Para simplificar a leitura o modelo conceitual de regras de privacidade para brinquedos inteligentes proposto por Rafferty *et al.* (2017), será denominado como modelo Rafferty no decorrer do texto.

O modelo Rafferty estabelece entidades baseadas em privacidade para o auxílio na tomada de decisão de acesso, possibilitando flexibilizar a permissão/negação da coleta de dados se comparado aos modelos de ferramenta de controle parental tradicional. As ferramentas tradicionais tomam suas decisões de acesso (permitir/negar) a partir da

Figura 1 – Modelo conceitual de regras de privacidade retirado de Rafferty *et al.* (2017).

definição do sujeito solicitante do acesso, do objeto (dado) o qual se quer acessar e a operação que será realizada (ler/escrever).

O modelo de Rafferty *et al.* (2017) estabelece a adição de quatro entidades de privacidade (propósito, destinatário, obrigação e retenção) somadas as entidades tradicionais (sujeito, objeto e operação) para determinar sua tomada de decisão, como mostrado na figura 1.

Na solicitação de acesso, além das entidades comuns mostradas anteriormente, são acrescentadas duas entidades de privacidade: o propósito (*purposes*) no qual o solicitante deve especificar uma ou um conjunto de finalidade (por exemplo, para jogo, para *marketing* etc.) envolvida(s) na solicitação de acesso; o destinatário (*recipients*) é a entidade que determina para onde os dados coletados irão, podendo ser para o próprio sujeito solicitante, outros usuários no caso de brinquedos com funções *multiplayer* e entidades externas não pertencentes ao sistema.

Para as entidades de privacidade estabelecidas na resposta da solicitação, os pais ou responsáveis legais ficam encarregados de defini-las. As obrigações (*obligations*) são relativas aos compromissos que o solicitante precisa cumprir ao receber a permissão de acesso aos dados. Na retenção (*retention*) os pais selecionam para que e/ou por quanto tempo desejam permitir a retenção dos dados para determinada solicitação de acesso.

No entanto, o modelo Rafferty limitou seu trabalho apenas ao desenvolvimento da funcionalidade de criação de regras de privacidade para serviços móveis, que solicitam acesso a dados de localização, controlando especificamente o acesso a objetos de localização relativa e localização absoluta, para execuções de operações básicas como ler e escrever.

Tendo em vista que a coleta de dados depende dos sensores, dispositivos e serviços móveis conectados ao brinquedo, uma variedade de tipos diferentes de dados pode ser

coletada como: texto, imagem, áudio, localização, atividades e os seus subtipos como vídeo, foto, localização relativa, localização absoluta etc. Operações do tipo: enviar, aprovar, selecionar, armazenar, podem ocorrer para diferentes tipos de dados que podem ser coletados pelo sujeito solicitante de acesso vinculado ao sistema do brinquedo (FERRAILOLO *et al.*, 2016).

Por mais que a criação de regras de privacidade seja importante, é apenas um dos requisitos necessários para a criação de uma ferramenta de controle parental consistente. As atuais ferramentas de controle parental são muito limitadas, com funcionalidades inadequadas a atualidade ou simples, não atendendo mais ou atendendo apenas parcialmente às necessidades dos pais (European Commission, 2017).

Não existem requisitos predefinidos e padronizados para o desenvolvimento de ferramentas de controle parental, por isso, as empresas de brinquedo implementam os requisitos que acham necessários, o que muitas vezes geram ferramentas ineficientes e negligenciadas, com erro básicos de desenvolvimento relacionado às boas práticas de privacidade e segurança, até em práticas simples como a criptografia da camada de transporte (CHU; APTHORPE; FEAMSTER, 2019)

A funcionalidade principal exige dos pais conhecimento sobre o dispositivo, coleta de dados e os riscos envolvidos no ambiente; por isso, as ferramentas de controle parental devem ter funcionalidades que apoiem a tomada de decisão e que complementem as necessidades dos pais. Guias para aprendizado da ferramenta e para a conscientização dos potenciais riscos relacionados ao ambiente de brinquedo inteligente são exemplos de funcionalidades complementares. São desejados também, requisitos não-funcionais que ajudem no desempenho da ferramenta como em usabilidade, segurança etc.

1.3 *Objetivos*

Este trabalho tem como objetivo geral disponibilizar um modelo padrão de ferramenta de controle parental para brinquedos inteligentes baseada em regras de privacidade. A regra de privacidade é o requisito mais importante desta proposta de ferramenta, pois é a funcionalidade que trata do controle de acesso, porém, a ferramenta necessita de requisitos complementares para cobrir a necessidade dos pais no apoio a proteção dos seus filhos.

Para suprir as necessidade dos pais e alcançar o objetivo geral, foi necessário seguir os objetivos específicos listados abaixo:

- identificação e apresentação de um conjunto padronizado de requisitos, funcionais e não-funcionais levantados a partir do estudo da literatura, desejáveis para o desenvolvimento de uma ferramenta de controle parental para brinquedos inteligentes. Considerando requisitos funcionais para a identificação das funcionalidades necessárias para a ferramenta, e não-funcionais para melhorar o desempenho e robustez da aplicação, desde o planejamento à implementação.
- Integração do modelo Rafferty como base para o levantamento dos requisitos de “criar regras de privacidade” e “criar perfil dos pais”.
- Desenvolvimento de um modelo conceitual da ferramenta de controle parental para estabelecer uma visão geral das funcionalidades, mostrando os principais elementos e conceitos do domínio e sugerindo um fluxo de atividades para a implementação da ferramenta.
- Implementação de um protótipo funcional da ferramenta de controle parental baseada no modelo conceitual.

Com a ferramenta de controle parental para brinquedos inteligentes gerada, espera-se que sirva de referência para: as empresas/indústrias de brinquedos que anseiem preservar, de forma concreta, a privacidade das crianças, conscientizando e envolvendo mais os pais no processo de tomada de decisão, e principalmente considerando questões éticas e legais de atos e regulamentos que considerem a privacidade da criança como *Personal Information Protection and Electronic Documents Act* (PIPEDA), *Children’s Online Privacy Protection Rule* (COPPA) e *General Data Protection Regulation* (GDPR); para pesquisadores, contribuindo com o avanço das pesquisas na área de privacidade e segurança em brinquedos inteligentes.

1.4 Método de pesquisa

Esta seção apresenta a descrição do tipo de pesquisa científica quanto aos aspectos teóricos e conceituais nos quais foram realizados neste trabalho.

- Gênero “empírico”: a pesquisa é de gênero empírico em vista de os requisitos levantados para a construção da proposta da ferramenta de controle parental serem propostos por autores por meio da sua experiência sobre a área. Os resultados da coleta de dados foram gerados a partir da avaliação de especialistas, de acordo com os seus respectivos conhecimentos.
- Natureza “aplicada”: a proposta de ferramenta de controle parental utilizou-se de requisitos já existentes identificados na literatura para o desenvolvimento de uma solução específica da área de brinquedos inteligentes, gerando conhecimento para a aplicação prática da ciência.
- Objetivo “exploratório”: levando-se em consideração os problemas de pesquisa deste trabalho, foi realizado um levantamento bibliográfico, por meio de uma revisão sistemática, para identificar requisitos considerados importantes para uma ferramenta de controle parental para brinquedos inteligentes, com o intuito de propor uma ferramenta padrão para área. A partir dos requisitos identificados, foram desenvolvidos um modelo conceitual e um protótipo da ferramenta, nos quais foram avaliados por especialistas com conhecimento sobre a área, com a intenção de contribuir com o avanço da compreensão do tema, tão pouco explorado na literatura, proporcionando mais familiaridade com o problema, tornando-o mais explícito (GIL, 2002).
- Abordagem “Mista (qualitativa e quantitativa)”: para as etapas deste projeto: a análise dos requisitos, a criação de um modelo conceitual e o desenvolvimento do protótipo de ferramenta, foram consideradas a abordagem qualitativa face a tais etapas terem características subjetivas. Para a análise dos resultados, foi usada a abordagem quantitativa para mensurar as avaliações de importância dos requisitos e satisfação da implementação, além do uso da abordagem qualitativa, novamente, para a análise das respostas relacionadas às sugestões de novos requisitos ou recomendações de aprimoramento.

Para o presente trabalho é usado como procedimento técnico principal a ciência de projeto (*design science*). Ciência de projeto é fundamentalmente um paradigma de resoluções de problemas, no qual são criados modelos, técnicas ou implementações, denominadas de artefato, para atingir um objetivo. Esse método aborda a pesquisa por meio da construção e avaliação de artefatos projetados para atender às necessidades identificadas (HEVNER *et al.*, 2004).

Para contribuir de forma significativa com a ciência e a prática, esse artefato a ser criado deve resolver um problema ainda não solucionado ou realizar uma melhoria para uma solução já existente (HEVNER *et al.*, 2004). No caso deste trabalho, o problema que se visa solucionar é a falta de uma ferramenta padronizada de controle parental para brinquedos inteligentes, que atenda as atuais necessidades de pais/responsáveis legais. Dito isso, estabeleceu-se um conjunto padrão de requisitos funcionais e não-funcionais desejáveis para uma ferramenta de controle parental, inexistentes no contexto atual da área.

A criação de uma revisão sistemática para basear uma pesquisa em ciência de projeto faz-se necessária, por causa da importância de buscar o máximo de informação existente sobre o problema, assegurando que foram identificados o contexto, as causas e as possíveis soluções (PIMENTEL; FILIPPO; SANTORO, 2019). Para atribuir o rigor que este tipo de procedimento técnico de pesquisa necessita, foi desenvolvida uma Revisão Sistemática da Literatura, na qual são apresentados os principais riscos e soluções relacionados à computação para brinquedos (ALBUQUERQUE *et al.*, 2019). Foram selecionados então os trabalhos primários relacionados à solução de controle parental, nos quais foram usados para realizar o levantamento dos requisitos funcionais e não-funcionais importantes para a composição da ferramenta.

Como etapas da pesquisa em ciência de projeto foram realizadas:

1. Revisão sistemática da literatura.
2. Levantamento de requisitos funcionais e não-funcionais.
3. Criação do modelo conceitual
4. Prototipação da ferramenta.
5. Coleta de dados via questionário.
6. Avaliação dos dados coletados.

Para o desenvolvimento do protótipo da ferramenta de controle parental, não foi seguindo à risca um modelo formal de desenvolvimento da engenharia de software, tendo em vista que o produto final seria apenas um protótipo. No entanto, foi seguido, empiricamente, uma estratégia de desenvolvimento iterativa e incremental, nesse fluxo de processo de desenvolvimento, repete-se uma ou mais das atividades, dependendo da necessidade, antes de prosseguir para a seguinte, e após a conclusão das atividades o processo é iniciado novamente, fechando um ciclo, levando em consideração o *feedback* dos participantes do projeto, facilitando as incrementações e melhorias contínuas no produto

de software, permitindo que alterações nas atividades sejam rapidamente incorporadas no processo de desenvolvimento (PRESSMAN; MAXIM, 2016). Para a validação das atividades e *feedback* para tais melhorias, o orientador deste projeto desempenhou o papel do cliente.

A figura 2 mostra as etapas gerais do processo de desenvolvimento de software, naturalmente, usado neste trabalho. No qual foram seguidas as etapas: 1. comunicação, levantamento de requisitos ditos como desejáveis para uma ferramenta de controle parental para brinquedos inteligentes e validação dos requisitos com os *stakeholders*, nessa atividade ocorreram alterações nos requisitos iniciais; 2. planejamento, planejamento da construção do modelo conceitual e quais diagramas usar para representação da visão geral do sistema, além do planejamento do desenvolvimento do protótipo; 3. modelagem, criação do modelo conceitual da ferramenta por meio de diagramas de casos de uso e de atividades, apresentando a interação e o comportamento das funcionalidades da ferramenta e validação do modelo junto ao cliente; 4. construção, desenvolvimento do protótipo de ferramenta de controle parental para plataforma Android, com a implementação dos requisitos funcionais e testes para validação das funções do protótipo; 5. entrega, entregas periódicas para validação e obtenção de *feedback* e entrega final do protótipo para uso.

Figura 2 – Fluxo de processo iterativo de software

Fonte: Pressman e Maxim (2016).

2 Fundamentação teórica

Neste capítulo, são mostrados os principais tópicos referentes à proposta do trabalho. O primeiro tópico, trata do brinquedo inteligente, que seria o instrumento de estudo da pesquisa; seguido pelo conceito de dados de contexto, considerando o ambiente de computação para brinquedos; o próximo tópico é a descrição de segurança, privacidade e proteção de dados, sobretudo, infantil; o último conceito diz respeito à Computação para Brinquedo (*Toy Computing*), detalhando sua ferramenta de proteção à privacidade mais difundida, o controle parental. Ainda nesta seção, é detalhado o funcionamento do modelo conceitual Rafferty, devido sua importância como funcionalidade para a proposta deste trabalho.

2.1 Brinquedos inteligentes

Brinquedo inteligente é um dispositivo que consiste em um brinquedo físico que se conecta com serviços móveis por meio da rede e de tecnologias sensoriais, aprimorando a funcionalidade de um brinquedo tradicional.

Os brinquedos são adaptados ao ambiente com o intuito de se tornarem mais atrativos às crianças. Historicamente, pode-se destacar as réplicas miniaturizadas de transportes, brinquedos antropomórficos, brinquedos com *display* gráfico e botões; mais recentemente, brinquedos conectados à rede e a serviços móveis de inteligência artificial. Entre os brinquedos, podemos descrever três tipos: os brinquedos tradicionais, os eletrônicos e os inteligentes. No quadro 1, os tipos de brinquedos são comparados, apresentando as principais diferenças entre eles. Essa comparação ilustra como a computação em brinquedos evoluiu para um novo paradigma que inspira preocupações associadas ao uso pelas crianças, sobretudo, em função do direito ao sigilo de dados que, em tese, poderia ser violado (RAFFERTY; FANTINATO; HUNG, 2015).

Quadro 1 – Comparação entre brinquedos tradicionais, eletrônicos e inteligente.

Tipo	Brinquedo Tradicional	Brinquedo Eletrônico	Brinquedo Inteligente
Meios de interação	-Física: botões -Manual: movimentos	-Física: botões -Sensores: luzes, movimentos	-Física: botões, touch screen -Sensores: movimento, voz, facial etc. -Visual: câmera -Auditiva: microfone e alto-falante
Coleta de dados	-Não	-Nenhum ou limitada	-Sim
Compartilhamento de dados	-Não	-Nenhum ou limitada	-Sim
Armazenamento de dados	-Não	-Nenhum ou limitada	-Sim
Inteligência computacional	-Não	-Não	-Sim
Conectividade	-Não	-Não	-Sim
Exemplos	-Bola de futebol -Urso de pelúcia	-Tamagochi -Furby	-Mattel Hello Barbie -Cognitoys Dino

Fonte: Adaptado de Rafferty, Fantinato e Hung (2015).

Tradicionalmente, os brinquedos foram criados de forma que a criança pudesse apenas imaginar a interação com o objeto, pois os brinquedos tradicionais não têm capacidade de processamento ou de rede para manter uma comunicação com o usuário (AMANCIO, 2018). Portanto, não há manipulação de dados – coleta, compartilhamento e armazenamento –, consequentemente, não há preocupações com segurança e privacidade de dados.

Os brinquedos eletrônicos apresentam mais recurso (por exemplo, *display* gráfico e botões) oferecendo mais interatividade entre o brinquedo e a criança. No entanto, em sua maioria, suas funcionalidades não necessitam de manipulação de dados. Se caso ocorresse a coleta de dados, eles ficariam armazenados localmente no brinquedo.

Conforme Tang e Hung (2017), um brinquedo inteligente neste contexto pode ser efetivamente considerado uma Internet das Coisas (*Internet of thing* - IoT) com funcionalidades de Inteligência Artificial (*Artificial intelligence* - AI), que pode fornecer experiências de Realidade Aumentada (*Augmented reality* - AR) aos usuários.

Um brinquedo inteligente pode coletar e armazenar diferentes tipos de dados, como texto, imagem, som, localização. Assim como o estado de atividade física do usuário (ex.: caminhada, corrida etc.) e armazenar informações personalizadas (ex.: localização, padrão de atividade etc.) por meio de dispositivos vinculados ao brinquedo como câmera, microfone, sistema de posicionamento global (GPS) e vários outros sensores, como reconhecimento facial ou detecção de som (HUNG *et al.*, 2016). Além disso, é capaz de compartilhar dados entre serviços móveis e outro brinquedo inteligente.

Existem diversos modelos de brinquedos inteligentes, com interações e funcionalidades diferentes, atendendo várias idades e tipos de brincadeira. As interações e as funcionalidades de um brinquedo inteligente são determinadas pelos componentes tecnológicos que o integram; podendo ser dispositivos, sensores e serviços mobile. Em Rafferty *et al.* (2017), são identificadas três propriedades genéricas de um brinquedo inteligente como podemos ver no quadro 2.

Quadro 2 – Propriedades genéricas de brinquedos inteligentes

Propriedades	Descrição
Pervasivo	Crianças tendem a levar os seus brinquedos em atividades cotidianas.
Social	Interações sociais e multijogadores estão se tornando aspectos obrigatórios dos brinquedos inteligentes.
Conectado	Comunicação através de redes, entre brinquedos inteligentes e serviços externos.

Fonte: Traduzido de Rafferty *et al.* (2017)

Podemos destacar na literatura, dois brinquedos com funcionalidades semelhantes. Na figura 3 a (a) Hello Barbie Mattel (2016) e o (b) CogniToy Dino (2016). Ambos estão conectados a serviços de inteligência artificial para criação de diálogos interativos.

Figura 3 – Exemplos de brinquedos inteligentes.

Fonte: Adaptado de McReynolds *et al.* (2017a)

O CogniToy Dino (2016) é um dinossauro que se conecta via Wi-Fi ao serviço de inteligência artificial chamado Elemental Path, parceiro da IBM Watson, no qual é um mecanismo de diálogo, baseado em nuvem, específico para crianças. A Hello Barbie Mattel (2016) é um brinquedo inteligente que tem como brinquedo físico uma boneca, conecta-se com o serviço móvel de inteligência artificial PullString.com fornecida pela ToyTalk, empresa especializada em diálogos interativos para brinquedos.

Os brinquedos exemplificados acima têm como funcionalidade principal o diálogo interativo, no qual por meio do uso de microfone, alto-falantes e sensores de reconhecimento de voz, conectados a serviços móveis de inteligência artificial específicos para crianças, são capazes de escutar e responder perguntas, criando a interação entre o brinquedo e a criança.

Outro brinquedo inteligente que vale ressaltar é o Pokémon Go, jogo para *smartphone* baseado em localização (*Global Position System*) – tem como objetivo a captura de criaturas virtuais, os chamados Pokémons, utilizando a posição física do usuário, e indicando a posição digital do Pokémon no mundo real, por meio de serviços de localização geográfica. Pokémon Go é capaz de usar Realidade Aumentada (AR) baseado em reconhecimento de imagem (através de uma câmera) nos *smartphones* para conectar o mundo físico com conteúdo digital interativo em uma exibição visual (OLSSON; SALO, 2011).

2.2 Dados de contexto de brinquedo inteligente

Dados de contexto podem ser definidos como qualquer informação que possa ser usada para caracterizar a situação de uma entidade (ABOWD *et al.*, 1999). Em um sistema com reconhecimento de contexto, os serviços são fornecidos ao usuário com base no que é relevante para ele no cenário da aplicação. A coleta desses dados permite que os aplicativos se adaptem ao ambiente do usuário e personalizem os serviços de acordo (HUNG *et al.*, 2016).

Heurix *et al.* (2015) descrevem os dados de contexto dividindo em cinco categorias: individualidade, atividade, localização, tempo e relações. A individualidade é referente a dados pessoais; atividade está relacionada a informações de interações; localização são as informações retidas por GPS; tempo é tempo discreto e relações são as inferências feitas a partir do relacionamento de dois ou mais dados de contexto.

No geral, o modelo de dados de contexto são classificados pelo World Economic Forum (2011) em três tipos: dados voluntários (dados explicitamente fornecidos pelas crianças, podem ser informações de perfil ou preferências); dados observados (detectados pelos brinquedos inteligentes, na maioria das vezes por meio de sensores e dispositivos); dados inferidos (deduzidos com base em análise de relacionamento de dados voluntários e/ou observados).

Embora permitir que os dados de contexto sejam coletados para serviços pode ser de grande benefício para os usuários, existe um *tradeoff* entre utilidade e privacidade (CHAKRABORTY *et al.*, 2013). A quantidade de informações coletadas geralmente resulta em uma troca necessária entre a divulgação de dados confidenciais e o recebimento de serviços sensíveis ao contexto. Para fornecer os serviços mais relevantes ao usuário, informações mais pessoais e de contexto devem ser coletadas. Por esse motivo os dados de contexto estão no centro da preocupação com a privacidade (RAFFERTY; KROESE; HUNG, 2015).

Entre os dados que podem ser coletados, estão também as informações pessoais identificáveis (*Personally Identifiable Information* - PII), o Instituto Nacional de Ciência e Tecnologia (NIST) define PII como qualquer informação sobre um indivíduo mantida por uma organização que pode ser usada para distinguir ou rastrear a identidade de um indivíduo, incluindo qualquer informação vinculável a um indivíduo identificável.

Os brinquedos inteligentes usam PII por vários motivos, por exemplo, aplicativos baseados em localização, como o Pokémon GO da Niantic, coletam dados do Sistema de Posicionamento Global (GPS) para permitir a mistura do mundo digital com o virtual e proporcionar a experiência de realidade aumentada; brinquedos inteligentes como Hello Barbie da Mattel e Dino da Cognitoys, incluindo robôs de companhia como o Zenbo da Asus, visam promover a comunicação social entre o usuário e o brinquedo ou agente robótico social. As funções de conversação usam reconhecimento de fala e Inteligência Artificial (IA) para estabelecer e manter um diálogo baseado em raciocínio com a criança; assim, coletar, compartilhar e armazenar PII, como gravações de voz infantil, são práticas comuns para esses agentes sociais, a fim de oferecer uma experiência semelhante à comunicação humana (ALBUQUERQUE *et al.*, 2019).

Os brinquedos inteligentes são capazes de coletar uma variedade de dados, como texto, imagem, vídeo, som, localização, dados de detecção, sejam eles sensíveis e/ou PII com os seus diferentes componentes tecnológicos. Isso torna o cenário muito mais complicado do que muitos outros dispositivos inteligentes, especialmente porque os usuários finais são principalmente crianças em um ambiente físico e social (HUNG *et al.*, 2016).

2.3 *Segurança, privacidade e proteção de dados infantis*

Nesta seção são descritos direitos e riscos que envolvem segurança, privacidade e proteção de dados, explicando desde os conceitos gerais de cada um, até aprofundar-se no ambiente de brinquedos inteligentes, no qual o interesse está na preservação infantil.

2.3.1 *Segurança infantil*

Segurança em sua definição é o conjunto das ações e dos recursos utilizados para diminuir os riscos e perigos com o intuito de proteger algo ou alguém. Para o contexto deste trabalho, destacam-se dois tipos de segurança: da informação e física.

A segurança da informação, segundo Avizienis *et al.* (2004), tem como objetivo a proteção de dados, e pode ser definida como o composto da confidencialidade, integridade e disponibilidade. Confidencialidade significa que o acesso aos dados é restrito apenas às partes pretendidas. A integridade é a precisão e consistência dos dados, indicando autenti-

cidade. Disponibilidade indica que os dados permanecem disponíveis quando necessário pelas partes legítimas.

Silva *et al.* (2018) diz que segurança da informação, na literatura, constantemente vem atrelada à privacidade, embora em alguns casos as definições pareçam semelhantes, são termos com abordagens diferentes. Segurança pode ser definida como a proteção de dados contra acessos não autorizados, concentrando-se em ataques e roubos de dados. A privacidade trata a capacidade de proteção de informações confidenciais e sigilosas, podendo se concentrar no controle de dados pessoais.

A segurança física trata dos riscos reais que problemas de segurança da informação podem ocasionar, tendo em vista que por meio da captura de dados sensíveis, por exemplo, localização e tempo, pode-se inferir um cronograma de atividades diárias. Portanto, facilitando a localização física, e consequentemente a possível ação de predadores infantis.

Considerando que os usuários finais dos brinquedos inteligentes ainda são crianças, que têm geralmente pouca compreensão e preocupação com a sua segurança e privacidade de dados, e considerando o Art. 2º da Lei Nº 8.069/90 (Estatuto da Criança e do Adolescente do Brasil, 1990), no qual se considera criança a pessoa até 13 anos de idade incompletos, aumenta a possibilidade de ocorrerem riscos relacionados à segurança, tanto da informação como, na pior das hipóteses, físicas. Nesses casos, embora a segurança seja vital para proteção de dados, ela é insuficiente para abordar questões de privacidade (SILVA *et al.*, 2018).

2.3.2 Privacidade e proteção de dados infantis

Privacidade de dados pode ser considerada como o direito de um indivíduo determinar como, quando e até que ponto as informações sobre si serão liberadas para outra pessoa ou para uma organização (HUNG; CHENG, 2009). A privacidade não é apenas uma questão pessoal, mas uma questão de segurança em geral, é preciso confiar nas partes a quem são confiadas as informações pessoais (HEURIX *et al.*, 2015).

O surgimento e os avanços das tecnologias de processamento de informações, a mudança de um mundo análogo ao digital centrado em dados e a tendência de coletar e armazenar dados pessoais sobre todos, levaram à compreensão de que a preservação da privacidade é, hoje em dia, mais importante do que nunca (HEURIX *et al.*, 2015).

Por esse motivo, mecanismos foram desenvolvidos para o auxílio na preservação da privacidade de dados. Entre eles a política de privacidade.

A política de privacidade descreve como é realizada a manipulação dos dados por uma empresa. Cada brinquedo inteligente e serviço móvel deve ter sua própria política de privacidade, que descreve as informações, incluindo como será realizada a coleta, armazenamento e compartilhamento dos dados pessoais do usuário (HUNG *et al.*, 2016).

A ferramenta de controle parental também auxilia na proteção da privacidade, por meio da criação de regras de privacidade, na qual o usuário (geralmente o usuário da ferramenta são os pais, e o usuário do brinquedo é a criança) define como os dados serão manipulados, de acordo com suas preferências.

Conhecer quais são os principais riscos à privacidade, assim como sua forma de ocorrência, é uma forma de ajudar a mitigá-los. No quadro 3 são descritos os principais riscos à privacidade de dados (RAFFERTY; FANTINATO; HUNG, 2015).

Quadro 3 – Principais ameaças à privacidade de dados

Ameaças	Descrição
Conectividade	Um invasor é capaz de distinguir se dois ou mais itens de interesse (por exemplo, sujeitos, mensagens, ações etc.) estão relacionados ou não no sistema.
Identificabilidade	Um invasor pode identificar suficientemente um sujeitos associado a um item de interesse, por exemplo, o remetente de uma mensagem. Geralmente, identificabilidade refere-se a um conjunto de sujeitos em potencial. Este é um caso especial de vinculação entre um sujeito e os seus atributos. Identificabilidade é uma ameaça ao anonimato e à pseudonimidade.
Não repudiabilidade	Isso permite que um invasor colete evidências para contrariar as alegações da parte de repúdio e para provar que um usuário sabe, fez ou disse algo.
Detectabilidade	Um invasor pode distinguir suficientemente se um item existe ou não (por exemplo, mensagens são suficientemente discerníveis de ruído aleatório)
Divulgação de Informações	Informações pessoais são expostas a indivíduos que não deveriam ter acesso a elas.
Desconhecimento do conteúdo	Um usuário não tem conhecimento das informações divulgadas ao sistema. O usuário fornece informações em excesso que permitem que um invasor recupere facilmente a identidade do usuário ou informações imprecisas que podem causar decisões ou ações erradas.
Inconformidade na Política e Consentimento	Isso significa que, embora o sistema mostre suas políticas de privacidade a seus usuários, não há garantia de que o sistema realmente esteja em conformidade com as políticas anunciadas. Portanto, os dados pessoais do usuário ainda podem ser revelados.

Fonte: Traduzido de Rafferty, Fantinato e Hung (2015)

Países, como os Estados Unidos da América, criaram leis e regras para a preservação da privacidade individual. Como é o caso da *Children's Online Privacy Protection Rule* (COPPA), uma lei de proteção online para crianças, que impõe a organizações restrições associadas à coleta de dados de crianças com menos de 13 anos (HERTZEL, 1999). Essa é uma razão pela qual muitos serviços on-line, por exemplo, o Facebook, têm 13 como idade mínima para criação da conta (HOLLOWAY; GREEN, 2016). De acordo com a idade considerada pela COPPA, uma criança não tem noção do perigo ao relatar os seus dados pessoais, prejudicando, dessa forma, sua privacidade e abrindo espaço para que pessoas mal-intencionadas possam coletar seus dados (HERTZEL, 1999).

O direito à proteção de dados pessoais é entendido como uma garantia de outros direitos fundamentais, um direito mais específico dentro do direito mais geral da privacidade pessoal (REIGADA, 2011).

O conceito de proteção de dados segue, conforme descrito por Martín-Ruíz *et al.* (2017): (1) Toda pessoa tem direito à proteção de dados pessoais que lhe digam respeito. (2) Tais dados devem ser processados de forma justa para fins específicos e com base no consentimento da pessoa envolvida ou em alguma outra base legítima estabelecida por lei. Todos têm o direito de acessar os dados coletados e o direito de retificá-los. (3) O cumprimento destas regras está sujeito ao controle de uma autoridade independente.

As diferentes dimensões dos direitos de proteção de dados são: minimização de dados, qualidade de dados, especificação de propósitos, limitação de uso, confidencialidade, segurança, transparência, participação individual e acesso a dados e anonimato (WRIGHT, 2011).

2.4 Computação para brinquedo

Com o campo de pesquisa de brinquedos inteligentes surgiu a Computação para Brinquedo (*Toy computing*), que é uma configuração na qual o componente de brinquedo físico interage com um dispositivo móvel que se conecta a um ou mais serviços móveis para facilitar a jogabilidade (RAFFERTY; HUNG, 2015). Com isso os brinquedos ganharam a capacidade de coletar e armazenar dados sobre as interações do usuário (RAFFERTY; FANTINATO; HUNG, 2015).

A computação para brinquedo é composta por dois tópicos principais em ciência da computação: a computação física e os serviços móveis (RAFFERTY; HUNG, 2015). A computação física é a interação entre o usuário e o brinquedo, através dos dispositivos sensoriais integrados em sua estrutura, que permitem a captação e manipulação de dados referentes a objetos e espaços reais por meio de sistemas mecânicos e/ou eletrônicos (CAMARATA; GROSS; DO, 2003).

Juntamente com a computação física, onde é peça chave para a composição de uma computação para brinquedo, é utilizada a computação pervasiva. A distinção entre computação física e pervasiva é que a computação física tem mais foco nos objetos físicos envolvidos, em vez da interação “transparente”, quase imperceptíveis.

Hinske, Langheinrich e Lampe (2008) propoem uma diretriz de *design* para integrar a tecnologia de computação pervasiva nos Brinquedos como mostrado no quadro 4. Tais diretrizes indicam os cuidados necessários para a criação de uma integração perfeita entre os componentes do brinquedo inteligente. No entanto, isso introduz a necessidade de uma estrutura de preservação da privacidade que proteja a criança das ameaças contra a privacidade, ao mesmo tempo que não se afaste da experiência de brincar, introduzindo políticas intrusivas (RAFFERTY; KROESE; HUNG, 2015).

Quadro 4 – Diretriz de design para integração de tecnologias de computação pervasiva em brinquedos.

Descrição
1. O aprimoramento tecnológico deve ter um valor agregado.
2. Especifique quais ações / tarefas devem ser suportadas.
3. Deixe o foco permanecer no brinquedo e na interação em si, não na tecnologia.
4. Integrar a tecnologia de forma que seja discreta, se não completamente invisível.
5. Os brinquedos ainda devem ser usados (de maneira “tradicional”) mesmo que a tecnologia esteja desligada ou não esteja funcionando.
6. Estreitamente entrelaçar design e implementação.
7. A tecnologia deve ser confiável, durável e segura.
8. Oferecer <i>feedback</i> imediato e contínuo.
9. A tecnologia adicionada deve suportar a alta dinâmica dos ambientes de jogo.
10. Empregue um processo de desenvolvimento iterativo, incluindo prototipagem rápida e testes.

Fonte: Traduzido de Hinske, Langheinrich e Lampe (2008)

Tecnologias da computação para brinquedo que englobam recursos sensoriais e de rede abrem novas ameaças à privacidade, estimulam novos requisitos do usuário e estabelece um caso exclusivo para leis e regulamentações existentes (RAFFERTY; FANTINATO; HUNG, 2015). Por mais que a computação herde as leis e regulamento dos seus componentes (serviços, dispositivos, brinquedo), não existem leis específicas para o ambiente de computação em brinquedos.

A figura 4 apresenta um modelo de ambiente de computação para brinquedo, destacando-se três entidades: o componente de brinquedo físico, dispositivo móvel e o serviço móvel (RAFFERTY; HUNG, 2015).

2.4.1 Modelo de computação para brinquedo

Figura 4 – Modelo de ambiente de computação para brinquedo.

Fonte: Traduzido de Rafferty e Hung (2015).

O brinquedo inteligente pode assumir vários formatos e modelos, brinquedos antropomórficos como bonecas e animais, armas, réplicas de transporte etc. A parte física do modelo é denominada de componente de brinquedo físico. Esse componente pode interagir com vários dispositivos móveis, sendo eles vinculados à sua estrutura ou externos. Com isso podem ser gerados vários tipos diferentes de interação.

As interações podem ocorrer por meio da interação física, na qual são usados movimentos articulados, botões ou até mesmo telas sensíveis ao toque, interação visual pelo uso de câmera no dispositivo móvel, interações auditivas com o uso de microfones e auto-falantes, ou até mesmo interações de rede sem fio como no caso do Wi-Fi, bluetooth, RFID (RAFFERTY; KROESE; HUNG, 2015). As interações também podem ocorrer por meio de tecnologias sensoriais, que coletam e enviam dados sensoriais para dispositivos móveis, como no caso do sensor de reconhecimento de voz que interage junto ao microfone, reconhecimento facial com a câmera etc.

A computação física tem como foco principal a interação realizada a partir de objetos físicos integrantes no brinquedo, já a computação pervasiva tenta obter interações “naturais”, tornando a interação entre usuários e máquina o mais invisível possível. Na computação para brinquedo, o componente de brinquedo físico é uma parte ativa da experiência do usuário, enquanto na computação pervasiva haveria pouco ou nenhum componente físico, e o sistema funcionaria perfeitamente com as atividades cotidianas

(RAFFERTY; KROESE; HUNG, 2015). Uma das principais características dos dispositivos de computação pervasiva e física é a capacidade de perceber informações de contexto sobre o ambiente circundante, a fim de reagir de acordo (SAHA; MUKHERJEE, 2003).

As outras entidades, a plataforma móvel e o serviço móvel, podem ser denominados componentes móveis. A plataforma móvel intermedia as restrições de acesso entre os serviços móveis e os dados locais coletados pelos dispositivos móveis (RAFFERTY; HUNG, 2015). Os serviços móveis são serviços acessíveis por meio de redes móveis. São geralmente sensíveis ao contexto (*context aware*), reunindo informações de contexto do dispositivo móvel e fornecendo serviços personalizados relevantes com base no contexto (RAFFERTY; KROESE; HUNG, 2015).

O ambiente de computação em brinquedo incorpora o conceito de *Bring your own device* (BYOD), significando que os serviços são executados no próprio dispositivo do usuário. Portanto, os serviços móveis devem considerar a grande variedade de dispositivos, com tipos diferentes de processamento, armazenamento e segurança.

Em um ambiente de computação para brinquedo, a preocupação é com a privacidade do usuário e que o acesso a recursos que podem revelar dados de contexto é limitado ao aplicativo de serviço de brinquedo, e usado apenas para fins que cumprem as políticas de privacidade e são aceitáveis para o usuário (RAFFERTY; KROESE; HUNG, 2015). Por isso, é necessário adotar mecanismos de preservação da privacidade.

Walled Garden tem esse nome devido ser um modelo de área restrita que permite que o processamento de dados ocorra em aplicações seguras, no qual os operadores controlam o acesso aos dados do cliente e fornecem acesso apenas a provedores de conteúdo selecionados, separando dos dados pessoais (JAOKAR; FISH, 2004). A relação com estes prestadores de serviços é regulada pelos operadores, que podem tomar decisões de controle de acesso, aplicando barreiras tecnológicas, regulamentos de pagamento e políticas de uso (REUVER, 2011). Portanto, a segurança e o suporte ao cliente são centralizados no operador, reduzindo a complexidade para os usuários finais e tornando a plataforma mais confiável. Em ferramentas de controle de acesso, as restrições criadas são armazenadas no *walled Garden*, no qual, posteriormente, servirão de instrumento para as tomadas de decisão.

2.4.2 Controle de acesso

A ferramenta de computação para brinquedo mais difundida na literatura é o controle de acesso. O controle de acesso é um conceito de segurança e privacidade que visa proteger o acesso a recursos ou dados (RAFFERTY; KROESE; HUNG, 2015). O objetivo do controle de acesso é limitar as ações ou operações que um usuário legítimo pode executar (SANDHU; SAMARATI, 1994).

Tal ferramenta busca, basicamente, inibir ameaças à privacidade ditas leves, como a divulgação de informações, que é a exposição de dados para indivíduos que não deveriam ter acesso a elas, e o desconhecimento de conteúdo, onde o usuário não tem conhecimento das informações divulgadas aos sistemas.

No contexto de brinquedos inteligentes, o controle de acesso dá lugar ao controle parental. Essa ferramenta permite que os pais criem regras de privacidade para impedir que os seus filhos autorizem que os seus dados sejam coletados por serviços e componentes tecnológicos vinculados aos brinquedos, de acordo com suas preferências (HUNG; FANTINATO; RAFFERTY, 2016a).

ITU e UNICEF (2014) recomendam que os controles parentais não transfiram a responsabilidade pelo uso de tecnologias da informação e comunicação (TIC) de crianças apenas aos pais, mas reconheça que os pais estão em melhor posição para decidir o que é apropriado para os seus filhos e devem estar cientes de todos os riscos, com o intuito de proteger melhor os seus filhos e capacitá-los a agir.

A ferramenta de controle parental, além de basear-se nas preferências dos pais, utiliza de políticas de segurança e privacidade para a tomada de decisão de acesso. Enquanto as políticas de segurança estão focadas na manutenção dos seus conceitos fundamentais como confidencialidade, integridade e disponibilidade, as políticas de privacidade estão relacionadas a por que, por quem e como os dados são coletados, armazenados e compartilhados (RAFFERTY; KROESE; HUNG, 2015).

O controle parental pode ser avaliado levando em consideração alguns itens relevantes como usabilidade, funcionalidade, eficácia e segurança (European Union Safer Internet Program, 2012). Seguindo a definição da ISO/IEC 25010:2011 (2011) para todos os itens. A usabilidade é definida como a capacidade do *software* ou produto de ser compreendido, aprendido, usado e atraente para o usuário, quando usado sob condições especificadas. A

funcionalidade é a capacidade do produto de *software* de prover funções que atendam às necessidades explícitas e implícitas, quando o software estiver sendo utilizado sob condições especificadas. A eficácia se refere à capacidade do produto de *software* de permitir que usuários atinjam metas especificadas com acurácia e completitude, em um contexto de uso especificado. E a segurança como a capacidade do produto de software de apresentar níveis aceitáveis de riscos de danos a pessoas, negócios, software, propriedades ou ao ambiente, em um contexto de uso especificado.

2.5 Modelo conceitual Rafferty

As ferramentas de controle parental tradicionais tomam suas decisões de acesso (permitir/negar) a partir da definição das entidades: sujeito solicitante do acesso, objeto ao qual se quer ter acesso e a operação que será realizada (ler/escrever).

No modelo conceitual Rafferty *et al.* (2017) de regras de privacidade para brinquedos inteligentes, a tomada de decisão de acesso, além das entidades presentes em um modelo de ferramenta tradicional, baseia-se em entidades de privacidade: propósito (*purpose*), destinatário (*recipient*), retenção (*retention*) e obrigação (*obligation*). Essas entidades são baseadas na plataforma para projeto de preferências de privacidade (p3p) (WENNING, 2007).

O propósito é um ou um conjunto de finalidades as quais determinada solicitação de acesso se propõe a seguir. Um propósito pode ser descrito como sub-propósitos diferentes ou combinados em um propósito “geral” em uma estrutura hierárquica (HE, 2003) como podemos visualizar na figura 5.

Figura 5 – Estrutura hierárquica do propósito.

Fonte: Traduzido de Rafferty e Hung (2015).

Propósitos diferentes podem ser unificados criando conjuntos genéricos como no caso do *Any Purpose*, ou podem ser classificados individualmente como propósitos de

marketing, pessoa, administrativo e jogo, que ainda podem ser sub-classificados criando propósitos mais específicos.

O destinatário é um conjunto de n destinatários do(s) objeto(s) coletado(s) pertencentes aos sujeitos ou aos usuários no sistema, no qual cada objeto coletado tem um conjunto correspondente de destinatários (RAFFERTY *et al.*, 2017). Os destinatários, levando em consideração o ambiente de computação para brinquedo no qual o modelo está submetido, são definidos como:

- Individual: o sujeito que fez a solicitação de acesso.
- Grupo: um grupo de usuários (ex.: jogos *multiplayers*).
- Terceiros: entidades externas não pertencentes ao sistema.
- Qualquer pessoa: qualquer sujeito ou entidade externa.

As obrigações são as regras que um sujeito solicitante concorda em cumprir após a permissão de acesso. Essas obrigações, geralmente, estão relacionadas às legislações como o COPPA ou a uma política de obrigação personalizada pelos pais ou responsáveis legais.

A retenção trata-se da imposição de um tempo de duração que um objeto pode ser usado ou coletado pelo sujeito solicitante do acesso. Os pais podem selecionar por quanto tempo desejam permitir que os dados dos seus filhos sejam retidos. A retenção pode ser dividida nas seguintes categorias:

- Não retenção: Não existe armazenamento de dados, o objeto solicitado é retido por um curto período de tempo.
- Objetivo declarado: Como forma de alcançar o objetivo declarado, o objeto solicitado é retido pelo tempo necessário para a conclusão do objetivo, sendo descartado após isso.
- Requisito legal: o objeto solicitado é retido para atender requisitos legais conforme exigido por leis ou diretrizes.
- Práticas de negócio: o objeto solicitado é retido de acordo com as práticas comerciais declaradas.

Levando em consideração a definição das entidades comuns entre as ferramentas de controle parental, e as entidades de privacidade adotadas para ambientes de computação para brinquedos, Rafferty *et al.* (2017) descreve uma regra de privacidade como:

Um sujeito tem acesso a um objeto, somente se o acesso for autorizado pelo controle de acesso principal. Além disso, o sujeito precisa especificar a(s) finalidade(s) do acesso e do(s) destinatário(s) do resultado da operação de acesso. O(s) propósitos(s) e o(s) destinatário(s) devem ser legítimos de acordo com o acesso do objeto definido pelo proprietário ou por uma autoridade como o governo. Assim, as obrigações e uma política de retenção serão retornadas como uma mensagem de resposta se o acesso for permitido. O sujeito deve também cumprir as obrigações e a política de retenção. A solicitação de acesso será negada de outra forma.

A tomada de decisão no modelo de regras de privacidade para brinquedos inteligentes é feita da seguinte maneira conforme explica Rafferty *et al.* (2017), mostrado também na figura 6: no primeiro passo, o sujeito solicita permissão a acesso aos dados de um usuário por meio da especificação do sujeito, objeto, operação, propósito e destinatário no corpo da solicitação. Após o recebimento da solicitação de acesso, é iniciado o processo da solicitação; primeiramente é verificado o proprietário do objeto do pedido de acesso, são recuperadas as regras e políticas de privacidade ativas no sistema, por último verifica-se o canal de comunicação de confirmação para o responsável pela solicitação.

No passo três a decisão de acesso é tomada; são verificadas a permissão do modelo, os propósitos permitidos e os destinatários com acesso permitido. Como último passo, a decisão final é tomada e a confirmação contendo o sujeito da solicitação e o respectivo evento é enviada para o usuário da ferramenta (pais ou responsáveis legais). Caso a decisão final seja a permissão, é enviada ao sujeito uma resposta contendo as obrigações que o sujeito deve cumprir para continuar tendo permissão de acesso ao objeto, e a política de retenção para aquele determinado acesso. O modelo registra todos os itens acima nos logs de auditoria.

Figura 6 – Tomada de decisão do controle de acesso.

Fonte: Traduzido de Rafferty e Hung (2015).

2.6 Considerações finais

Este capítulo tem como fim esclarecer os tópicos mais importantes neste trabalho. Na seção 2.1 de brinquedos inteligentes, aprofunda-se o conhecimento sobre esse tipo de brinquedo, comparando-o aos outros tipos, esclarecendo as diferenças entre eles e definindo o que é e como funciona um brinquedo inteligente. Na próxima seção 2.2 é apresentado o dado de contexto, tópico importante para o entendimento sobre o prejuízo e benefício que a coleta de dados pode causar.

Na seção 2.3.1 são descritos os conceitos de segurança, dividindo-se em dois tipos, segurança da informação e física. Ainda nesta seção, uma descrição sobre a privacidade e a proteção de dados, onde são expostos os principais riscos à privacidade. Na última seção 2.4 é enfatizado o tipo de computação por trás do brinquedo inteligente, descrevendo a estrutura do modelo de computação para brinquedo, assim como descrevendo sobre sua ferramenta mais difundida referente à proteção da privacidade, o controle parental.

3 Trabalhos relacionados

Com o objetivo de encontrar o maior número possível de trabalhos primários com assuntos similares ao tema deste em questão, uma revisão da literatura baseada nos princípios da revisão sistemática foi realizada. Uma revisão sistemática da literatura é um meio de identificar, avaliar e interpretar toda a pesquisa disponível relevante para uma questão de pesquisa em particular, área temática, ou fenômeno de interesse (KITCHENHAM; CHARTERS, 2007). A revisão sistemática foi realizada nos meses de janeiro e fevereiro de 2019, retornando estudos primários publicados até essa data.

A revisão sistemática da literatura (RSL) desenvolvida para este trabalho, foi aprofundada para a submissão de um artigo, e junto a um grupo de especialistas na área de brinquedo inteligente, submeteu-se o primeiro artigo intitulado: “*Privacy in smart toys: Risks and proposed solutions*”, aceito no *Journal: Electronic Commerce Research and Applications* (ALBUQUERQUE *et al.*, 2019). Posteriormente, em vista do grande conteúdo da RSL, foi desenvolvido e submetido outro artigo: “*A Literature Survey on Smart Toy-related Children’s Privacy Risks*”, aceito na *Hawaii International Conference on System Sciences* (2020).

3.1 Protocolo da revisão da literatura

A realização da revisão da literatura com princípios sistemáticos baseou-se no método proposto por Kitchenham e Charters (2007). Nesse método é sugerida uma sequência de etapas distintas, seguindo um determinado protocolo de pesquisa. Para o planejamento da revisão são seguidos as determinadas etapas apresentadas no quadro 5.

Quadro 5 – Fases e suas respectivas etapas de uma revisão sistemática

Planejamento	• Identificação da necessidade de uma revisão; • Comissionando uma revisão; • Especificando a(s) pergunta(s) de pesquisa; • Desenvolver um protocolo de revisão; • Avaliar o protocolo de revisão;

Fonte: Traduzido de Kitchenham e Charters (2007)

Além da realização da revisão sistemática da literatura, usou-se a análise de conteúdo. Com a análise de conteúdo, foram analisadas as evidências existentes encontradas por meio da revisão sistemática, e foram sintetizados os achados que as relacionam às diferentes categorias de riscos e soluções de privacidade das crianças para abordá-las (ALBUQUERQUE *et al.*, 2019).

3.1.1 Planejamento da revisão

O planejamento da revisão sistemática da literatura para este trabalho, foi seguindo todos os cinco passos do planejamento apresentados acima:

a) Necessidade da pesquisa

Novos brinquedos e maneiras de brincar surgem com o passar do tempo, acompanhando o avanço da indústria e tecnologia. As empresas de brinquedos começaram a integrar dispositivos tecnológicos na estrutura de brinquedos, criando novos tipos de interações e jogabilidades, emergindo uma nova categoria chamada de brinquedo inteligente (ALBUQUERQUE *et al.*, 2019). Os brinquedos ganharam a capacidade de se conectar à internet, coletar e processar diferentes tipos de dados (por exemplo, texto, imagem, voz, localização), o que pode incluir dados pessoais identificáveis (PII).

Tendo em vista que os usuários finais são crianças que, geralmente, não compreendem ou se preocupam com a própria proteção de dados, garantir a privacidade das informações coletadas é um desafio crítico para os brinquedos inteligentes, considerando as inúmeras consequências que podem ocorrer, incluindo ameaças à integridade física da criança (HUNG; FANTINATO; ROA, 2019).

Privacidade e segurança, sobretudo, em brinquedos inteligentes, é um campo de pesquisa importante, que vem ganhando amplitude, mas que ainda necessita ser explorado. Faltam estudos capazes de mostrar uma visão geral dos possíveis riscos que cercam um brinquedo inteligente. Embora haja significativo número de pesquisas relacionadas às técnicas de segurança e privacidade em ambientes de Internet das Coisas (*Internet of Thing* - IoT), não há trabalhos especificamente para a subárea de brinquedos inteligentes nesse paradigma (HUNG *et al.*, 2016).

Esclarecer pais e pesquisadores a respeito dos possíveis riscos à privacidade e segurança, e das ferramentas utilizadas disponíveis atualmente, identificando os prós e contras, faz-se necessário para o avanço do conhecimento e na pesquisa deste tema.

b) Comissionamento da revisão

O autor deste trabalho aproveitou o desenvolvimento desta revisão sistemática para usá-la na submissão de artigos científicos, no qual houve outros coautores, especialistas e doutores especializados na área de brinquedo inteligente que auxiliaram no desenvolvimento da estratégia da revisão e análise dos resultados.

c) Questões de pesquisa

Foram definidas duas questões de pesquisa com a intenção de selecionar os estudos relacionados ao escopo da revisão da literatura.

Q1. Quais são os principais riscos para a privacidade das crianças ao usar brinquedos inteligentes?

Considerando que, dependendo da área do conhecimento, autores utilizam-se de diferentes nomenclaturas para termos relacionados a riscos, ameaças e vulnerabilidades em privacidade e segurança, usamos o “risco” como um termo genérico para referenciar todos esses termos relativos, desconsiderando significados específicos que tais termos podem ter em diferentes campos.

Esta questão de pesquisa teve como objetivo identificar quais os principais riscos pertinentes ao uso dos brinquedos inteligentes por crianças.

Q2. É possível mitigar os riscos à privacidade das crianças ao usar brinquedos inteligentes?

Ao responder essa questão de pesquisa, foi possível identificar técnicas, metodologias ou tecnologias que estão sendo utilizadas para prevenir a ocorrência de riscos, ou ao menos planejar respostas. São demonstrados como os recursos ajudam a combater tais problemas de privacidade e segurança.

d) Protocolo da revisão

Um protocolo especifica os métodos que serão utilizados para realizar uma revisão sistemática. Um protocolo predefinido é necessário para reduzir a possibilidade de viés do pesquisador (KITCHENHAM; CHARTERS, 2007).

São expostos os passos realizados, desde a criação de uma *string* de busca para encontrar os estudos primários que fariam parte do escopo da pesquisa, selecionar os estudos que respondem às questões de pesquisa, até a extração dos dados necessários para a realização da revisão sistemática.

Para a pesquisa dos estudos primários que integraram a revisão, foram utilizadas as bases de dados de pesquisa Scopus e Web of Science (WoS). A Scopus é considerado o maior banco de dados de literatura revisada por pares, incluindo revistas científicas, livros e anais de conferências, com títulos de mais de 5000 editores internacionais, incluindo grandes editores como Elsevier, IEEE, Springer, Wiley, Taylor & Francis, World Scientific, SAGE, Emerald e InderScience (ELSEVIER, 2017). A Web of Science também foi utilizada, pois, em revisões anteriores conduzidas pelo grupo de pesquisa, ela foi útil ao encontrar artigos adicionais não encontrados pela Scopus, mesmo em casos muito raros.

No que diz respeito à pesquisa dos estudos primários viáveis para o escopo da revisão criou-se uma *string* de busca, com palavras-chave relacionadas ao tema principal do trabalho: brinquedos inteligentes, privacidade e segurança. Foi incrementalmente refinada a partir de pesquisas exploratórias piloto anteriormente realizadas. A tabela 1 abaixo representa a *string* final de busca.

Tabela 1 – *String* de busca final*

(privacy OR private OR security OR secret OR safety OR vulnerable OR protect OR preserve OR confidential OR sensitive OR reliability) AND ((smart OR connected OR clever OR intelligent OR anthropomorphic OR humanoid OR humanlike OR interactive OR cognitive OR social OR educational OR internet OR IoT OR online) W/5 (toys OR playthings OR dolls OR barbie))

Fonte: Otávio de Paula Albuquerque, 2020

Para guiar a seleção dos estudos primários da revisão, definiram-se critérios de inclusão e exclusão

- A.1) Critérios de Inclusão:

- CI-1 Estudos que identificam riscos em brinquedos inteligentes.
- CI-2 Estudos que abordam artifícios como técnicas, metodologias e tecnologias para planejar respostas e soluções para riscos em brinquedos inteligentes.
- A.2) Critérios de Exclusão:
  - CE-1 Artigo não disponível para leitura.
  - CE-2 Artigo publicado como resumo.
  - CE-3 Artigo que não estiver escrito totalmente em inglês.
  - CE-4 Artigo não avaliado por especialistas.

e) Avaliação do protocolo

A avaliação foi realizada a partir do grupo de coautores envolvidos no desenvolvimento do artigo científico baseado nesta revisão sistemática da literatura. O grupo integrou um estudante de mestrado, uma estudante de doutorado e dois doutores, com trabalhos consolidados no tema de brinquedos inteligentes.

3.1.2 Realização da revisão

O objetivo de uma revisão sistemática é encontrar o maior número possível de estudos primários relacionados à pergunta de pesquisa, usando uma estratégia de busca imparcial (KITCHENHAM; CHARTERS, 2007). Para que a estratégia cumpra com o seu objetivo, é necessário que alguns passos sejam seguidos.

Estratégia de pesquisa

Foram identificadas as palavras-chave relacionadas ao conteúdo proposto para revisão, com a finalidade de criar uma *string* de busca.

Após identificar as palavras-chave principais, foram usados alguns artifícios para deixar a *string* mais eficiente na busca. Foram incluídos sinônimos, abreviaturas, plurais e outros termos encontrados na literatura referentes as palavras-chave já disponíveis. Após a criação da *string* piloto, foram realizadas buscas experimentais, utilizando o banco de dados Scopus e Web of Science, primeiramente para avaliar o volume de estudos potencialmente

relevantes. No entanto, as primeiras buscas serviram para identificar outras palavras-chave utilizadas em estudos primários retornados que poderiam ser incorporadas na *string*.

Com a *string* final concluída, submeteu-se a pesquisa, e analisando títulos, resumos e palavras-chave, foram retornados 194 documentos. Do total, foram retirados 39 artigos duplicados, e em seguida foram adicionados os critérios de inclusão e exclusão. Com a primeira análise, por meio de uma leitura dinâmica dos documentos, foram selecionados 65 artigos. Ao fazer uma análise mais detalhada, aplicando novamente os critérios de inclusão e exclusão, mas agora para o texto completo, foram selecionados 22 artigos. Para reforçar a sistematização da revisão, foram analisadas as referências dos 22 artigos selecionados, resultando na adição de mais 4 artigos ao escopo, concluindo em um total de 26 estudos para a análise de conteúdo, como apresentado na figura 7.

Figura 7 – Resumo da seleção dos artigos

Fonte: Otávio de Paula Albuquerque, 2020

3.2 Análise de conteúdo

Para responder às questões de pesquisa baseadas nos estudos primários identificados como resultado de nosso procedimento sistemático de pesquisa, foram combinados: análise de conteúdo quantitativa e qualitativa. A análise de conteúdo refere-se à análise de textos e à existência de categorias específicas de termos (BRYMAN, 2012). A análise quantitativa de conteúdo é uma abordagem orientada positivamente, com base em categorias precedentes. A análise qualitativa de conteúdo, por outro lado, requer a inferência de categorias de forma interpretativa.

3.2.1 Análise de conteúdo quantitativa

Para a análise quantitativa, utilizou-se a taxonomia proposta por Loukil *et al.* (2017), usada em sua revisão sistemática sobre o reconhecimento de privacidade em aplicações IoT. Considerando brinquedo inteligente como um tipo de IoT, essa taxonomia foi considerada a mais relacionada a revisão sistemática. Foram utilizadas quatro facetas das sete classificadas originalmente, pois este trabalho tem um objetivo mais específico. Enquanto Loukil *et al.* (2017) estavam interessados em várias análises (incluindo também: domínio do aplicativo, tipos de arquitetura e fases do ciclo de vida), esta RSL particularmente preocupa-se com os tipos de riscos e soluções relacionados à segurança e privacidade.

A figura 8 apresenta a taxonomia adaptada usada aqui. Além de não usar algumas facetas, agruparam-se as propriedades de segurança e os requisitos de segurança como uma única sub-faceta de Segurança da informação para tornar a taxonomia mais adequada para os propósitos da RSL.

Figura 8 – Taxonomia para extração e classificação de dados

Fonte: Adaptado e traduzido de (LOUKIL *et al.*, 2017).

Como resultado, a classificação usada na análise quantitativa possui apenas duas facetas. O primeiro *princípios de privacidade ISO* está relacionado à nossa primeira pergunta de pesquisa: os riscos de privacidade envolvidos no uso de brinquedos inteligentes, incluindo ameaças e vulnerabilidades. O último *técnicas de preservação da privacidade* está relacionado à nossa segunda questão de pesquisa: soluções para mitigar os riscos de privacidade envolvidos no uso de brinquedos inteligentes. Loukil *et al.* (2017) confiaram em

uma ampla norma ISO/IEC (2011) para definir os princípios de privacidade usados em sua classificação.

Assumiu-se que os fabricantes de brinquedos inteligentes deveriam aderir a esse conjunto de princípios de privacidade para não representar riscos para as crianças usuárias. Assim, foram avaliados os estudos primários, com o intuito de identificar quais apresentavam preocupações e quais dos princípios estavam relacionados às respectivas preocupações.

Existem 11 princípios de privacidade, um dos quais — *segurança da informação* — está dividido em seis outros princípios especificamente relacionados à segurança, mencionados como propriedades e requisitos de segurança. Esse segundo nível de classificação é importante, pois a *segurança das informações* é geralmente um dos aspectos mais importantes para garantir a privacidade das informações. Quanto à *preservação da privacidade*, Loukil *et al.* (2017) consideraram cinco técnicas principais: duas do tipo “perturbação de dados” (*proteção contra adição de ruído* e *anonimização*) e três do tipo “restrição de dados” (*controle de acesso*, *proteção criptográfica* e baseada em *blockchain*).

Para a análise quantitativa dos dados, todos os 26 estudos primários foram analisados usando palavras-chave que pudessem mostrar a preocupação dos autores em relação a cada princípio na figura 8. Como análise quantitativa, cada termo era contabilizado na extração de dados de um determinado artigo somente quando uma manifestação de preocupação direta (clara e explícita) foi encontrada no artigo sobre o princípio correspondente.

3.2.2 Análise de conteúdo qualitativa

A classificação levantada por meio da análise quantitativa de conteúdo é direcionada a riscos e soluções técnicas, efeito proporcionado pela taxonomia adotada. Embora importante para o estudo, essa contribuição parcial está focada em aspectos voltados ao público especializado em segurança e privacidade da informação. A taxonomia usada, embora aplicável ao contexto do brinquedo inteligente, baseia-se em conceitos técnicos de segurança e privacidade, que são usados para identificar riscos e abordar possíveis soluções de mitigação.

Foi realizada uma análise qualitativa do conteúdo para produzir também uma classificação de riscos e soluções mais alinhadas à área de aplicação. A intenção foi identificar riscos de privacidade e possíveis soluções mais representativas para o contexto de

brinquedos inteligentes. Procurou-se encontrar riscos mais tangíveis para crianças usuárias do brinquedo, bem como soluções mais direcionadas para esse tipo de usuário.

Para este caso, foi necessária uma análise qualitativa do conteúdo, pois nenhuma taxonomia adequada foi previamente identificada especificamente para esse fim. Assim, essa classificação teve que emergir da análise dos 26 estudos primários. Para isso, foi feita uma leitura cuidadosa de todos os estudos, para que tais riscos e soluções pudessem ser identificados. Primeiro, um conjunto amplo foi identificado, incluindo uma série de sinônimos e expressões semelhantes. Em seguida, trabalhou-se em um conjunto inicial, através de várias iterações, até reduzi-lo a um conjunto menor, que refletia genericamente todos os estudos primários.

3.3 Resultados e considerações

A tabela 2 mostra uma descrição dos 26 estudos primários resultantes do nosso procedimento sistemático de pesquisa. Acredita-se que esses trabalhos representam a grande maioria dos estudos publicados até o início de 2019 que abordam os riscos envolvidos na privacidade das crianças associados ao uso de brinquedos inteligentes, bem como as possíveis soluções discutidas até agora para esses riscos. Considerando a sistematização seguida em nossa busca por artigos, há apenas uma pequena chance de falta de artigos relevantes.

A figura 9 mostra graficamente a evolução temporal dos estudos primários encontrados. Embora o primeiro artigo mencionado nesse problema tenha sido publicado em 2009, a grande maioria dos artigos foi publicada a partir de 2016 (cerca de 88% deles), com destaque para 2018 (com 35% dos artigos). De fato, é notório que o conceito de brinquedos inteligentes começou a se tornar mais conhecido por volta de 2015, especialmente após o lançamento da Hello Barbie, seguido de várias reportagens da mídia sobre suas características e riscos que envolvem a privacidade das crianças. Os números ainda são baixos para 2019, provavelmente porque a pesquisa foi realizada nos primeiros meses do ano.

Em relação ao tipo de veículo, a maioria dos trabalhos foram publicados em anais de conferências, o que é comum nos campos de tecnologia e computação. No entanto, ocorreu um aumento no número de artigos publicados em periódicos em 2018, o que pode mostrar

Tabela 2 – Estudos primários (TV: Tipo de veículo; J – Journal; C – Conference)

ID	Título	Autores-Ano	TV
1	Security and privacy analyses of internet of things children's toys	Chu, Apthorpe e Feamster (2019)	J
2	Modeling Privacy Preservation in Smart Connected Toys by Petri-Nets	Yankson <i>et al.</i> (2019)	C
3	Playing with danger: A taxonomy and evaluation of threats to smart toys	Shasha <i>et al.</i> (2018)	J
4	Children's digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture	Smith e Shade (2018)	J
5	Toys that talk to strangers: A look at the privacy policies of connected toys	Chowdhury (2018)	C
6	Smart doll: Emotion recognition using embedded deep learning	Espinosa-Aranda <i>et al.</i> (2018)	J
7	Cyberthreats under the bed	Kshetri e Voas (2018)	J
8	A preliminary study of Hello Barbie in Brazil and Argentina	Fantinato <i>et al.</i> (2018b)	J
9	Smart bears don't talk to strangers: Analysing privacy concerns and technical solutions in smart toys for children	Demetrou, Böck e Hanteer (2018)	C
10	Security tests for smart toys	Carvalho e Eler (2018b)	C
11	Security requirements and tests for smart toys	Carvalho e Eler (2018a)	C
12	A framework for preventing the exploitation of IoT smart toys for reconnaissance and exfiltration	Haynes <i>et al.</i> (2017)	C
13	Towards a comprehensive analytical framework for smart toy privacy practices	Mahmoud <i>et al.</i> (2017)	C
14	Security& privacy in smart toys	Valente e Cardenas (2017)	C
15	Protecting privacy in the era of smart toys: Does Hello Barbie have a duty to report	Moini (2017)	J
16	Security requirements for smart toys	Carvalho e Eler (2017)	C
17	Toys that listen: A study of parents, children, and internet-connected toys	McReynolds <i>et al.</i> (2017a)	C
18	Towards a privacy rule conceptual model for smart toys	Rafferty <i>et al.</i> (2017)	C
19	A study of privacy requirements for smart toys	Hung, Fantinato e Rafferty (2016a)	C
20	A glance of child's play privacy in smart toys	Hung <i>et al.</i> (2016)	C
21	The Internet of toys	Holloway e Green (2016)	J
22	Your New Best Frenemy: Hello Barbie and Privacy Without Screens	Jones (2016)	J
23	Can (and should) Hello Barbie keep a secret?	Jones e Meurer (2016a)	C
24	Hacking and securing the AR.Drone 2.0 quadcopter: Investigations for improving the security of a toy	Pleban, Band e Creutzburg (2014)	C
25	Risk mitigation strategies for mobile Wi-Fi robot toys from online pedophiles	Yong <i>et al.</i> (2011)	C
26	A spotlight on security and privacy risks with future household robots: Attacks and lessons	Denning <i>et al.</i> (2009)	C

Fonte: Albuquerque *et al.* (2019).

um ganho de maturidade das pesquisas nessa área. Não há foco em nenhuma conferência ou periódico, exceto uma conferência que publicou três artigos e uma conferência e um periódico com dois artigos cada.

Figura 9 – Distribuição dos estudos primários por tipo de veículo e ano.

Fonte: Albuquerque *et al.* (2019).

3.3.1 Riscos técnicos e soluções propostas

a) Riscos técnicos identificados — Princípios de privacidade e segurança da informação

A figura 10 mostra a classificação dos 26 estudos primários de acordo com as preocupações expressas pelos autores sobre os 11 princípios de privacidade. Os dados apresentados neste gráfico refletem as principais preocupações dos pesquisadores sobre os riscos à privacidade das crianças no uso de brinquedos inteligentes. Alguns desses riscos são mencionados apenas brevemente em alguns documentos, com cobertura superficial, enquanto outros têm uma cobertura profunda. Assim, para uma melhor caracterização, a extração de dados considerou se o artigo trata um risco específico de maneira profunda ou superficial.

Figura 10 – Classificação de artigos pelos princípios de privacidade da ISO

Fonte: Albuquerque *et al.* (2019).

Na figura 10, pode-se observar diferentes níveis de interesse e preocupação nos estudos primários. Os três riscos mais frequentemente encontrados estão relacionados a: (1) a maneira que os dados são usados (incluindo sua retenção e, especialmente, sua divulgação); (2) a necessidade de consentimento para qualquer tipo de operação de dados

a ser executada (inclusive fornecendo opções diferentes); e (3) a necessidade de ampla transparência por parte do fabricante de brinquedos inteligentes, para que o responsável pela criança tenha um amplo conhecimento do que está envolvido nas operações com os dados da criança. Esses riscos estão relacionados aos três primeiros princípios da figura 10: *limitação de uso, retenção e divulgação; consentimento e escolha; e abertura, transparência e notificação*. Esses três princípios foram abordados no mínimo superficialmente em pelo menos 20 dos 26 estudos primários e profundamente cobertos por pelo menos 11 artigos.

Ao analisar esses estudos, percebe-se facilmente esse padrão de preocupação dos autores, que manifestam um claro interesse nesses riscos básicos à privacidade de brinquedos inteligentes, no qual algumas dessas preocupações recorrentes estão relacionadas a problemas como: se pais sabem exatamente quais dados da criança são coletados; se os pais são devidamente notificados; se existe transparência nas políticas de privacidade dos fabricantes de brinquedos inteligentes; se as ações de consentimento funcionam como esperado; o que exatamente é feito com as PIIs da criança; se os dados são mantidos armazenados após o uso ou removidos; e se existe o risco de divulgação inadequada de informações pessoais de identificação das crianças.

O quarto princípio na figura 10 é a *segurança da informação*, que é, de fato, uma média dos seis subprincípios apresentados na figura 11. Os seis subprincípios da figura 11 apresentaram diferentes níveis de ocorrência em cada um dos 26 estudos primários; o que aparece na figura 10 é um valor médio considerando todos eles para cada estudo primário. Um dos seis subprincípios — *confidencialidade* — é a preocupação mais presente nos 26 estudos primários, profundamente abordados em 16 deles. Por outro lado, as preocupações relacionadas à *integridade* aparecem em apenas sete artigos, a maioria coberta apenas superficialmente.

Esses seis princípios relacionados à segurança de dados são abordados nos 26 estudos primários também como um reflexo do modo como os autores se posicionaram sobre os riscos referentes à privacidade de crianças relacionadas a brinquedos inteligentes. A maioria expressou preocupação com o risco mais latente, a *confidencialidade* dos dados da criança. Isso mostra que mesmo os princípios mais básicos não foram abordados adequadamente pelos fabricantes de brinquedos inteligentes. As preocupações mais mencionadas a seguir estão relacionadas diretamente à manutenção da confidencialidade, ou seja, *autorização* e *autenticação*. Por outro lado, os riscos relacionados a *integridade*, *disponibilidade* e *accountability* ainda não fazem parte das principais preocupações dos pesquisadores, talvez

Figura 11 – Classificação dos documentos por propriedades e requisitos de segurança (subprincípios de segurança da informação)

Fonte: Albuquerque *et al.* (2019).

porque a confidencialidade e a privacidade dos dados não estejam diretamente conectadas a esses três princípios. No entanto, todos os princípios de *segurança da informação* estão interconectados com importância semelhante para garantir a privacidade. Por exemplo, a falta de integridade nos dados armazenados por uma empresa de brinquedos pode facilitar indiretamente o vazamento de dados. Mesmo a *accountability* que aparece com um número maior de ocorrências pelos autores ainda se refere a manifestações superficiais em cada artigo em que elas aparecem.

Após os quatro primeiros princípios de privacidade (cf. figura 10), os sete posteriores não tiveram muitas ocorrências nos estudos primários. O princípio *limitação na coleta* se destaca com oito manifestações profundas. Um número razoável de autores manifestou preocupação com a quantidade de dados coletados maiores que o necessário pelas empresas de brinquedos. Por outro lado, *minimização de dados*, o extremo do princípio de *limitação na coleta*, foi o menos mencionado. Minimizar dados significa que deve haver uma limitação no processamento de dados, não apenas na coleta de dados. Em geral, questões de privacidade mais específicas, que geralmente não são óbvias, ainda não foram abordadas. Por exemplo, enquanto muitos autores lidaram com *limitação de uso*, *consentimento* e *transparência*, poucos abordaram *participação e acesso individual*, que se refere a dar aos usuários o direito de revisar, alterar e remover os seus dados de maneira simples, sempre que desejado.

b) Soluções técnicas propostas — Técnicas de preservação da privacidade

Embora existam muitos riscos à privacidade (consulte a figura 8), apenas cinco técnicas de preservação da privacidade estão claramente definidas na taxonomia básica usada por este estudo. Na figura 12, apenas duas técnicas do tipo *restrição de dados* receberam um número razoável de menções — *criptografia* e *controle de acesso*. O alto número de soluções relacionadas a criptografia reflete uma das maiores preocupações dos pesquisadores - o risco de violação da confidencialidade. Vários pesquisadores trataram nos seus artigos a necessidade de criptografar as informações pessoais identificáveis (PII) das crianças e, possivelmente, dados relacionados ao uso do brinquedo inteligente. Os pesquisadores também estão muito interessados em propor maneiras de controlar o acesso aos brinquedos. O controle de acesso pode ser tratado com níveis e objetivos específicos. Uma forma de controle de acesso específica ao contexto de brinquedos inteligentes é por meio de ferramentas de controle parental, abordadas em alguns desses documentos como uma solução proposta para reduzir os riscos à privacidade das crianças.

Figura 12 – Classificação de artigos por técnicas de preservação da privacidade

Fonte: Albuquerque *et al.* (2019).

Técnicas relacionadas a *anonimização* e *adição de ruído* foram meramente mencionadas como soluções apenas em alguns estudos primários. Resta ver se essas técnicas do tipo *perturbação de dados* não são apropriadas para brinquedos inteligentes ou se ainda não foram consideradas pelos pesquisadores nesse contexto. Pelo menos no contexto geral da IoT, de acordo com a revisão sistemática realizada por Loukil *et al.* (2017), o número de soluções encontradas relacionadas ao anonimato foi cerca de 60% maior do que o controle de acesso. Esse cenário é muito diferente daquele encontrado para brinquedos inteligentes.

Finalmente, soluções relacionadas à *blockchain* não foram mencionadas em nenhum artigo. No entanto, este poderia ser um resultado esperado, pois *blockchain* é uma técnica muito recente. Mesmo para o contexto mais geral da IoT, pouquíssimos documentos mencionaram ela como uma possível solução para os riscos à privacidade na revisão sistemática realizada por (LOUKIL *et al.*, 2017).

c) Análise cruzada entre os riscos e as soluções propostas

A figura 13 mostra uma análise cruzada entre os dados apresentados nas figuras 10, 11 e os dados apresentados na figura 12, ou seja, uma análise cruzada entre os riscos identificados e os tipos de soluções propostas nos estudos primários. Os dados da figura 13 mostram mais claramente o que poderia ter sido inferido a partir de dados anteriores: quais são as principais preocupações abordadas pelos pesquisadores em termos de riscos à privacidade das crianças e que tipos de soluções podem ser usadas para mitigar esses riscos. O gráfico mostra o número de artigos para os quais ocorre um determinado par de princípios. Por exemplo, os princípios de *minimização de dados* e *anonimização* estão presentes no mesmo artigo em apenas 3 dos 26 estudos primários.

Algumas análises importantes podem ser realizadas como pode-se ver em outros exemplos, pelo menos 14 artigos mencionam os riscos associados a *consentimento e escolha, limitação de uso, retenção e divulgação, abertura, transparência e notificação, segurança da informação — confidencialidade — e segurança da informação — autorização —*, além de possíveis soluções associadas a *controle de acesso e criptografia*. Isso não significa que esses tópicos estejam necessariamente conectados nesses documentos. No entanto, alguns sinais fortes obtidos são que os riscos de consentimento são vistos como possivelmente abordados pelas técnicas de controle de acesso ou que os riscos de autorização devem ser tratados através de técnicas criptográficas.

3.3.2 Riscos específicos do domínio e soluções propostas

A tabela 3 mostra os resultados da análise qualitativa de conteúdo dos estudos primários. Por meio da análise qualitativa, foi levantada uma nova classificação de riscos e soluções propostas, além da apresentada na figura 8. Embora esse tenha sido conduzido

Figura 13 – Análise cruzada entre riscos identificados (princípios de privacidade) e soluções propostas (técnicas de preservação da privacidade)

Fonte: Albuquerque *et al.* (2019).

por riscos técnicos do ambiente de IoT em geral, este é voltado para riscos mais próximos do domínio específico que está sendo tratado, ou seja, brinquedos inteligentes e usuários infantis.

Nem todos os estudos primários abordam algum risco específico do domínio. Em vez disso, alguns naturalmente enfatizam os riscos técnicos, conforme explorado nas figuras 10 e 11. Outros mencionam riscos específicos de domínio, mas superficialmente, apenas como motivação básica para o seu trabalho técnico. Por outro lado, alguns trabalhos buscam uma vertente de impacto social e exploram os riscos que podem afetar diretamente as crianças que usam brinquedos inteligentes.

A tabela 3 apresenta a categorização realizada nesta RSL, resultante desses riscos específicos do domínio. O risco mais comum apontado pelos autores é *violação de dados*, encontrado em quase todos os artigos. Diferentes tipos e níveis de violação de dados são agrupados nessa categoria, incluindo: divulgação ilegal ou inadequada de dados, vazamento de dados, dados roubados e uso indevido de dados. De fato, esse tipo de risco não é

Tabela 3 – Riscos específicos do domínio e soluções propostas (Rec. = Recomendações)

ID	Riscos específicos do domínio	Soluções propostas específicas do domínio
1	Violação de dados; segurança física	Compartilhar lições aprendidas; quadro de avaliação
2	Violação de dados; segurança física	Rec. para fabricantes de brinquedos
3	Violação de dados; segurança física; segurança psicológica	Quadro de avaliação
4	Vigilância de dados; violação dos direitos éticos da privacidade das crianças; propaganda infantil	Compartilhar lições aprendidas
5	Violação de dados	Rec. para melhorar a política de privacidade
6	Violação de dados	Rec. para fabricantes de brinquedos
7	Violação de dados	Compartilhar lições aprendidas
8	Violação de dados; segurança física	Controle parental
9	Violação de dados; segurança física; violação dos direitos éticos da privacidade das crianças	Rec. para fabricantes de brinquedos
10	Violação de dados	Rec. para fabricantes de brinquedos; controle parental
11	Violação de dados	Rec. para fabricantes de brinquedos; controle parental
12	Segurança física; segurança psicológica	Quadro de avaliação
13	Violação de dados	Quadro de avaliação
14	Segurança física; segurança psicológica	Rec. para fabricantes de brinquedos
15	Violação dos direitos éticos da privacidade das crianças	Rec. para legisladores
16	Violação de dados	Rec. para fabricantes de brinquedos; controle parental
17	Violação de dados; violação dos direitos éticos da privacidade das crianças	Rec. para fabricantes de brinquedos; rec. para legisladores; controle parental
18	Violação de dados; segurança física	Rec. para fabricantes de brinquedos; controle parental
19	Violação de dados; segurança física	Rec. para fabricantes de brinquedos; rec. para legisladores; controle parental
20	Violação de dados; segurança física	Rec. para fabricantes de brinquedos; controle parental
21	Violação de dados; Vigilância de dados; controle remoto não autorizado	Rec. para legisladores
22	Violação de dados; violação dos direitos éticos da privacidade das crianças; segurança psicológica	Rec. para fabricantes de brinquedos; rec. para melhorar a política de privacidade
23	Violação de dados; segurança psicológica	Rec. para fabricantes de brinquedos
24	Violação de dados; controle remoto não autorizado	Rec. para fabricantes de brinquedos
25	Segurança física	Rec. para fabricantes de brinquedos; rec. para pais ou responsáveis legais
26	Espionagem; controle remoto não autorizado; segurança psicológica	Rec. para fabricantes de brinquedos

Fonte: Albuquerque *et al.* (2019).

totalmente específico do domínio, como os outros apresentados na tabela 3; no entanto, a maioria dos autores destaca as especificidades dos dados da criança, portanto, da violação de dados da criança.

Considerando riscos mais tangíveis, muitos autores levantaram preocupações sobre a *segurança física* de crianças usuárias. As crianças podem enfrentar problemas relacionados a assédio, perseguição, aliciamento, abuso sexual, exploração, sequestro, pedofilia e outros

tipos de violência. Semelhante a isso, existem preocupações com *segurança psicológica*, pois as crianças podem enfrentar problemas relacionados a chantagem, insultos, perda de confiança, e *bullying*.

Um risco menos proeminente é o *dataveillance*, isto é, a vigilância de dados, que pode ser realizada pela própria empresa de brinquedos, pelo governo ou por terceiros não autorizados. Também não muito proeminente, existe o risco de *controle remoto não autorizado* do brinquedo, o que pode ser feito, por exemplo, por vandalismo ou roubo do brinquedo. Existe também o risco de *campanhas inadequadas de publicidade direcionadas a crianças* mencionadas apenas uma vez.

Por fim, o risco de *espionagem* (vigilância), o que pode ser feito até pelos próprios pais. No entanto, neste último caso, há controvérsia sobre se isso deve ser considerado um risco ou uma solução. De qualquer forma, isso é indicado na tabela 3 como *violação dos direitos éticos da privacidade das crianças*.

As categorias de risco específicas do domínio na tabela 3 não são mutuamente exclusivas. Existem riscos inter-relacionados, por exemplo, muitos riscos de *violação de dados* são motivadores para riscos de *segurança física*. O *controle remoto não autorizado* de um brinquedo pode levar a riscos de *segurança física ou psicológica*. A complexidade dos riscos envolvidos é tal que não conseguimos produzir uma taxonomia mutuamente exclusiva ou um modelo de relacionamento entre as categorias.

Do ponto de vista das soluções (tabela 3), nem todos os estudos principais visam apresentar soluções específicas de domínio. Alguns trabalhos pretendem apresentar apenas contribuições analíticas e soluções não concretas. Nesses casos, são esperadas apenas algumas recomendações gerais possíveis, indicadas na tabela 3 como *compartilhar lições aprendidas*.

Outros trabalhos naturalmente se concentram em soluções mais técnicas, relacionadas aos princípios resumidos nas figuras 10 e 11. No entanto, a tabela 3 procura classificar todos os trabalhos do ponto de vista das soluções propostas específicas para o domínio de brinquedos inteligentes e usuários infantis. As soluções propostas diferem bastante umas das outras. O objetivo deste trabalho era agregar as soluções propostas em grandes categorias, a maioria relacionada a recomendações: *recomendações para fabricantes de brinquedos*, incluindo técnicas, métodos, modelos, estruturas, melhores práticas, diretrizes úteis para desenvolvedores produzirem brinquedos inteligentes sob regulamentos de segurança e privacidade; *recomendações para legisladores*, incluindo sugestões e recomendações

para melhorias relacionadas a leis, legislação e regulamentos associados a este contexto; *recomendações para melhorar as políticas de privacidade*, incluindo sugestões para empresas de brinquedos para melhorar a comunicação sobre suas políticas de privacidade, como aumentar sua transparência; e *recomendações para pais*, mencionado apenas uma vez e tem como objetivo listar as ações que os pais podem executar para evitar problemas.

Outro tipo importante de solução são os *quadros de avaliação* propostos para apoiar a análise de brinquedos inteligentes e, possivelmente, sua classificação com base no cumprimento das normas de segurança e privacidade. Finalmente, uma solução muito específica para esse domínio, e mencionada por muitos autores, é a necessidade e a importância de ferramentas adequadas de *controle parental*.

3.4 Discussão

De modo a direcionar o assunto da discussão para apenas o objetivo deste trabalho, tratou-se aqui especificamente da parte sobre as soluções identificadas para a área de brinquedos inteligentes. Para a leitura completa da discussão, na qual envolve, também, os riscos relacionados ao brinquedo inteligente, está disponível em anexo (anexo A) o artigo completo referente a esta revisão sistemática da literatura.

3.4.1 Soluções para mitigar os riscos à privacidade das crianças relacionadas ao brinquedo inteligente

Há um cenário ameaçador em termos de riscos de privacidade e segurança relacionados a brinquedos inteligentes, de acordo com os pesquisadores. No entanto, apesar de seu impacto potencialmente sério, a maioria das vulnerabilidades existentes é facilmente corrigível (CHU; APTHORPE; FEAMSTER, 2019). Elas provavelmente são causadas por erro substancial do desenvolvedor, apatia ou ignorância das práticas recomendadas de privacidade e segurança. Talvez os fabricantes de brinquedos não estejam muito preocupados com questões de segurança e privacidade, pois são apenas brinquedos, quando deveria ser exatamente o oposto, tendo em vista quem são os seus principais usuários. Para resolver adequadamente esses problemas, os fabricantes de brinquedos precisam incluir essa preocupação nos estágios iniciais do ciclo de vida do desenvolvimento de brinquedos inteligentes. Por exemplo, Yankson *et al.* (2019) mostra a importância de abordar os

elementos do descritor de privacidade ao modelar o fluxo de dados durante a análise de requisitos e modelagem de sistema.

No entanto, o cenário atual mostra que, ao considerar as soluções de privacidade das crianças para desenvolver novos brinquedos inteligentes, os desenvolvedores precisam entender que a segurança dos dados das crianças exige ir além do paradigma básico de privacidade de dados *opt-in-opt-out* (HOLLOWAY; GREEN, 2016). Os produtos de brinquedos inteligentes podem ser ainda mais vulneráveis a ataques cibernéticos do que outros dispositivos de IoT, fornecendo para hackers um ponto de entrada frequentemente esquecido (KSHETRI; VOAS, 2018), mostrando que cuidados extras devem ser tomados.

Muitas soluções técnicas foram apresentadas pelos pesquisadores, algumas muito pontuais para questões muito específicas. Esses casos geralmente são o resultado de estudos experimentais em que falhas e vulnerabilidades concretas foram demonstradas, enquanto suas correções também foram apresentadas quando possível. Conforme advertido por alguns pesquisadores, muitas das ferramentas técnicas necessárias já existem, pois são genéricas para o domínio da IoT e precisam ser usadas corretamente apenas. As soluções técnicas relacionadas à criptografia e controle de acesso foram mais mencionadas até agora, ambos do tipo de restrição de dados. Técnicas do tipo de perturbação de dados não foram muito mencionadas pelos pesquisadores (isto é, anonimização e adição de ruído), o que difere da IoT em geral.

Considerando soluções específicas de domínio, em nível social, várias recomendações foram apresentadas. Essas recomendações são derivadas de diferentes métodos de pesquisa; algumas são meramente lições aprendidas ou coleções de ideias, outras resultam de estudos mais sistemáticos, como estudos de caso e experimentos, enquanto outras são derivadas de análises detalhadas da legislação e das políticas de privacidade de certos brinquedos inteligentes. Além disso, existem recomendações voltadas especificamente para desenvolvedores de brinquedos inteligentes, outros para legisladores, enquanto outros para empresas de brinquedos como responsáveis pelo desenvolvimento de políticas de privacidade. Alguns autores propuseram estruturas de avaliação para apoiar a análise de brinquedos inteligentes e, possivelmente, sua classificação com base no cumprimento das normas de segurança e privacidade, que podem ser úteis para desenvolvedores, empresas e legisladores. Finalmente, autores mostram a necessidade de ferramentas de controle parental como a solução mais específica do domínio.

A maioria das recomendações para desenvolvedores, ou seja, fabricantes de brinquedos, são compostas de recomendações técnicas, no formato de melhores práticas, requisitos, estruturas etc., como as apresentadas por (DENNING *et al.*, 2009; YONG *et al.*, 2011; PLEBAN; BAND; CREUTZBURG, 2014; HUNG; FANTINATO; RAFFERTY, 2016a; VALENTE; CARDENAS, 2017; CARVALHO; ELER, 2017; CARVALHO; ELER, 2018a; CARVALHO; ELER, 2018b; SHASHA *et al.*, 2018; DEMETZOU; BÖCK; HANTEER, 2018). Fantinato *et al.* (2018b) são exemplos de autores que não recomendam uma solução estritamente técnica, pois sugerem que os fabricantes de brinquedos reduzam os problemas de privacidade, melhorando as ferramentas de controle parental usando a mineração de dados, parte de uma solução mais estratégica.

Carvalho e Eler (2018a) argumentam que os fabricantes de brinquedos inteligentes devem fornecer aos pais informações sobre quais ações eles devem tomar para garantir a segurança dos filhos. A solução mais completa proposta até agora para esse fim é de Rafferty *et al.* (2017), que propôs um modelo conceitual para permitir que os pais (ou responsáveis legais) forneçam consentimento por meio de regras de acesso que definem que os dados dos seus filhos sejam compartilhados de acordo com suas preferências de privacidade. O modelo permite que os pais criem sistematicamente regras de privacidade e tomem conhecimento em relação à manipulação de dados sensíveis à privacidade dos seus filhos. Esse modelo conceitual é, de fato, uma base poderosa para criar ferramentas de controle parental muito mais apropriadas do que as ferramentas de configuração simples oferecidas atualmente (FANTINATO *et al.*, 2018b). Vários pesquisadores lamentam o quão medíocre são as atuais ferramentas de controle parental, ao mesmo tempo em que destacam o potencial que esse tipo de solução apresenta para resolver muitos dos riscos indicados na forma de uma solução abrangente.

Considerando que os riscos existem por causa da alta conectividade dos brinquedos inteligentes, Espinosa-Aranda *et al.* (2018) argumentam que seria possível evitar o envio de tanto processamento para a nuvem. Eles mostram que é possível realizar o reconhecimento de emoções através do processamento local no brinquedo usando *deep learning*. Embora não seja razoável tratar todo o processamento como local, o que iria na direção oposta à onipresença do mundo moderno, isso corrobora diretamente com o princípio de privacidade ISO de minimizar o processamento de dados.

Chowdhury (2018) recomendou que os fabricantes de brinquedos explicitassem suas políticas de privacidade, para que os pais tenham mais transparência para decidir

se comprem brinquedos inteligentes para os seus filhos, por exemplo, as perguntas frequentes (FAQ) com itens de privacidade devem acompanhar os documentos da política de privacidade para facilitar a visualização de como as informações são coletadas, usadas e divulgadas.

De acordo com Fantinato *et al.* (2018b), as diretrizes de segurança de brinquedos, como os requisitos de segurança da *Health Canada's Safety Requirements for Children's Toys and Related Products*, estão desatualizados com as inovações atuais na tecnologia de brinquedos inteligentes. Essas diretrizes concentram-se na segurança física relacionada aos brinquedos tradicionais e não consideram os desenvolvimentos recentes nas tecnologias de brinquedos, que agora possuem uma ampla gama de recursos sensoriais e de rede, criando novos riscos à segurança. Espera-se que as contribuições apresentadas pelos pesquisadores sejam utilizadas pelo interesse público. Moini (2017), por exemplo, propôs uma emenda à COPPA para incluir a obrigação do brinquedo inteligente (de fato, a empresa responsável por ele, incluindo analistas de sistema e prestadores de serviços) de monitorar e rastrear gravações suspeitas em assuntos críticos como abuso sexual, para alertar os pais.

É provável que os IoToys se tornem um tópico cada vez mais importante para preocupação e discussão do público nos próximos anos (HOLLOWAY; GREEN, 2016). O desenvolvimento de políticas já está em andamento no domínio mais amplo da IoT na Austrália, Europa e EUA, no entanto, espera-se que ocorram mais declarações e iniciativas de políticas (HOLLOWAY; GREEN, 2016). Os legisladores devem ajudar as crianças, os pais e os fabricantes de brinquedos a se conscientizarem dos problemas de privacidade, fortalecer as proteções de privacidade das crianças existentes, como a COPPA, e resolver os mesmos problemas com outros dispositivos conectados à Internet que não são brinquedos, mas também são usados por crianças como a Siri, Amazon Echo e Alexa (MCREYNOLDS *et al.*, 2017a). Apesar da incompletude desses regulamentos, muito já está coberto por eles. Por exemplo, a *minimização de dados*, uma etapa importante para reduzir os riscos à privacidade, é um princípio de processamento de dados mencionado no artigo 5(1p) do GDPR que obriga o controlador de dados a processar apenas dados pessoais *adequados, relevantes e limitados ao que é necessário em relação às finalidades para as quais eles são processados* (DEMETZOU; BÖCK; HANTEER, 2018).

Alguns autores contribuíram de maneira importante ao propor estruturas de avaliação (MAHMOUD *et al.*, 2017; HAYNES *et al.*, 2017; SHASHA *et al.*, 2018; CHU; APTHORPE; FEAMSTER, 2019). Cada um com os seus detalhes específicos, eles têm

objetivos comuns: permitir às partes interessadas avaliar e comparar brinquedos inteligentes a partir de um determinado conjunto de critérios. Essas estruturas são muito importantes porque permitem que as partes interessadas tenham uma visão abrangente dos conjuntos de riscos existentes e da qualidade de determinados brinquedos inteligentes. Haynes *et al.* (2017) sugeriu que o brinquedo pode ser acompanhado por uma etiqueta, classificado como A+, A, B+, B ou C, dependendo do número de critérios atendidos.

3.5 Considerações finais

Se a tendência for confirmada e os brinquedos inteligentes se tornarem mais atraentes para as crianças e suas vendas futuras aumentarem, como espera-se, os fabricantes de brinquedos e os regulamentos de privacidade precisarão ser ágeis, tendo em vista que atualmente não estão prontos para lidar com os riscos à privacidade das crianças. Embora os brinquedos inteligentes ainda não sejam amplamente utilizados por crianças em todo o mundo, as crianças ainda encontrarão os brinquedos inteligentes como uma importante oportunidade de entretenimento porque são excluídos de muitas plataformas de mídia social em vista da idade, pelos regulamentos adotados (por exemplo, Facebook, Twitter, Snapchat etc.).

Os brinquedos inteligentes devem-se tornar cada vez mais populares à medida que adquirem mais recursos tecnológicos com o poder de atrair as crianças do mundo de hoje. Esses mesmos recursos tecnológicos devem aumentar suas vulnerabilidades em relação aos riscos de privacidade. As crianças são muito mais receptivas à adoção e ao uso de novas tecnologias do que as gerações anteriores e expressam pouca ou nenhuma preocupação com as implicações de privacidade associadas ao uso dessas tecnologias e dispositivos. Se hoje o problema não é tão grande porque há poucas crianças que usam brinquedos inteligentes, ele pode se tornar muito maior em breve. Isso dependerá de como os brinquedos inteligentes evoluirão para realmente atrair as crianças e permear suas vidas e como os seus fabricantes estarão preparados para oferecer soluções seguras.

Como contribuição direta do estudo, propôs-se uma classificação de dois níveis de riscos e soluções: um nível técnico (baseado em questões gerais de IoT) e um nível específico de domínio (alvo no domínio de brinquedos inteligentes). Dos 26 estudos primários selecionados, o risco técnico mais mencionado é a divulgação de dados, enquanto, de

uma perspectiva específica do domínio, há muita preocupação com a segurança física e psicológica das crianças. Do ponto de vista da mitigação, muitas recomendações e soluções foram propostas; não há um tipo de contribuição mais comum, embora as agrupemos em categorias para promover nossa análise. Como trabalho futuro, pode ser proposta uma nova estrutura de avaliação, com objetivo semelhante aos encontrados, porém mais sistemático e abrangente, envolvendo toda a classificação adotada neste estudo.

4 Requisitos da ferramenta de controle parental

Este capítulo trata do levantamento de requisitos, funcionais e não-funcionais, identificados para a criação da proposta de ferramenta de controle parental para brinquedos inteligentes, desenvolvida neste trabalho. São apresentados os requisitos e suas descrições, além de mostrar a cobertura dos atos e regulamentos sobre esses eles.

Coletar, armazenar e compartilhar informações pessoais identificáveis (*personally identifiable information* - PII), como gravações de voz, são práticas comuns para brinquedos inteligentes, de modo a oferecer uma experiência semelhante à comunicação humana. As PII são usadas por vários motivos. Por exemplo, o Dino da Cognitoys e o Hello Barbie da Mattel, bem como robôs de companhia como o Zenbo da Asus, visam promover a comunicação social, através de conversas de voz entre o usuário e o brinquedo ou agente robótico social. As funções de conversação usam reconhecimento de fala e Inteligência Artificial (IA) para estabelecer e manter um diálogo com a criança.

Como outros produtos da Internet das Coisas (IoT), garantir a privacidade das informações coletadas é um desafio crítico para os brinquedos inteligentes (HUNG *et al.*, 2016). A preocupação é ainda maior nesse caso, pois as PII são coletadas de usuários menores de idade. As soluções inteligentes de brinquedos podem ser oportunidades para muitos riscos à privacidade das crianças, com as PII se tornando um alvo para coleta, armazenamento ou divulgação não autorizada de dados (SHASHA *et al.*, 2018). Os fabricantes de brinquedos inteligentes devem considerar ameaças e vulnerabilidades para mitigar os riscos à privacidade antes de comercializar novos produtos que possam comprometer a privacidade das crianças. As soluções de brinquedos inteligentes devem pelo menos garantir a conformidade com os regulamentos de privacidade e segurança das informações relacionadas aos dados de usuários infantis.

As ferramentas de controle de acesso fornecidas pelas empresas de brinquedos, como as ferramentas de controle dos pais, são possíveis soluções para ajudar a proteger a privacidade dos dados das crianças (RAFFERTY; KROESE; HUNG, 2015). Esse tipo de ferramenta deve permitir que os pais decidam, de acordo com suas preferências, permitir ou negar a coleta, o uso e o compartilhamento de certos tipos de dados dos seus filhos (RAFFERTY *et al.*, 2017). No entanto, as atuais ferramentas de controle parental são muito limitadas, atendendo apenas parcialmente às necessidades dos pais (European Commission,

2017). Embora existam técnicas gerais bem estabelecidas para ferramentas de controle parental (FUERTES *et al.*, 2015), elas não seguiram as tendências emergentes trazidas pelas recentes mudanças tecnológicas. Em termos de brinquedos inteligentes, embora diferentes estudos tenham abordado a necessidade de controle dos pais (RAFFERTY; KROESE; HUNG, 2015; RAFFERTY *et al.*, 2017; RAFFERTY; FANTINATO; HUNG, 2015; HUNG; FANTINATO; RAFFERTY, 2016b; MCREYNOLDS *et al.*, 2017b), ainda não há convergência para um modelo padronizado para esse tipo de ferramenta.

Os requisitos da ferramenta de controle parental aqui apresentados são direcionados ao desenvolvimento de ferramentas para ajudar os pais a controlar as atividades das crianças ao usar brinquedos inteligentes, especialmente com relação à manipulação das informações pessoais identificáveis (*personally identifiable information* - PII) das crianças. Tais requisitos devem servir de referência para os fabricantes de brinquedos que realmente desejam preservar a privacidade das crianças, envolvendo os pais no processo, especialmente considerando questões legais e éticas.

4.1 *Requisitos da ferramenta*

A ferramenta de controle parental é peça chave para a proteção de dados em um ambiente de computação para brinquedos (representado na figura 14). A ferramenta é executada pelos pais da criança geralmente em um dispositivo móvel, podendo ter recursos acessados por um computador pessoal. A ferramenta em execução no dispositivo móvel deve se comunicar com outros aplicativos possivelmente em execução no mesmo dispositivo, com o brinquedo físico e com os possíveis serviços em nuvem; logo, os requisitos de uma ferramenta de controle parental devem abordar todo esse contexto de comunicação.

Figura 14 – Ambiente de computação para brinquedos

Fonte: Otávio de Paula Albuquerque, 2020.

Tendo em vista os possíveis riscos que um brinquedo inteligente pode causar para a criança, a pesquisa sobre requisitos e estratégias de implementação de ferramentas de controle parental estão se tornando mais frequentes, devido a grande projeção desse mercado, e a falta de ferramentas efetivas para essa área.

Hung, Fantinato e Rafferty (2016a) discutem em sua pesquisa sobre requisitos de privacidade em computação para brinquedos, dividindo-as em 5 categorias, levando em consideração alguns aspectos locais: requisito de usuário final (*end user requirements for children*), controle parental (*parental control*), regulações e leis de privacidade (*privacy laws and regulations*), requisitos de segurança do Health Canada para brinquedos infantis e produtos relacionados (*health Canada's safety requirements for children's toys and related products*), Guia e boas práticas para indústria (*industry guidelines and best practices*). Os autores afirmam a necessidade de ferramentas padronizadas e funcionais para auxiliar os pais na proteção dos seus filhos.

Para este trabalho, foi levantado um conjunto de requisitos funcionais e não-funcionais ditos como desejáveis para a composição de uma ferramenta de controle parental para brinquedos inteligentes. Os requisitos foram obtidos por meio da leitura detalhada de artigos selecionados na seção 3. Dos 26 artigos selecionados na última etapa da revisão sistemática, 13 discutiam sobre mecanismos para responder ou mitigar riscos relacionados a ferramentas de controle parental para brinquedos inteligentes, apresentando requisitos para tais soluções. Após a leitura das referências dos 13 trabalhos, foram adicionados 7 artigos ao escopo, incluindo os relatórios dos atos PIPEDA (*Personal Information Protection and Electronic Documents Act*), COPPA (*Children's Online Privacy Protection*

Act), GDPR (Regulamento Geral sobre a Proteção de Dados), e do relatório SIP-BENCH III (relatório para avaliação de ferramentas de controle parental), totalizando 20 artigos que apresentavam ao menos um requisito para uma ferramenta de controle parental.

Como resultado, 37 requisitos foram identificados: 19 requisitos funcionais e 18 requisitos não-funcionais, dos quais 4 de usabilidade, 1 de interoperabilidade, 1 de implementação, 8 de segurança e 4 legais, apresentados nas respectivas tabelas 4, 5, 6, 7, 8 e 9.

Tabela 4 – Requisitos funcionais para ferramentas de controle parental

ID	Req. Funcional	Descrição	Fonte
F01	Criar perfil dos pais	Cadastrar dados básicos de contato do usuário da ferramenta (ou seja, Rafferty <i>et al.</i> (2017), Lic-dos pais ou responsável legal) tais como nome e e-mail, para permitir a cardi <i>et al.</i> (2014) comunicação entre o usuário e a empresa do brinquedo inteligente.	
F02	Obter consentimento dos pais	Obter o consentimento dos pais, no qual eles assumem a propriedade dos Carvalho e Eler (2017), Car-dados em nome da criança e concordam com a política de privacidade da valho e Eler (2018a), Carva-empresa de brinquedo, garantindo o direito à coleta de dados da criança lho e Eler (2018b) por parte da empresa, desde que não fira as regras de privacidade a serem definidas pelos pais por meio dessa ferramenta.	
F03	Notificar mudanças na política de privacidade da empresa	Notificar os pais sobre alterações na política de privacidade da empresa de Liccardi <i>et al.</i> (2014), Carva-brinquedos em relação às regras gerais de coleta, uso, compartilhamento e lho e Eler (2017), Carvalho divulgação de dados da criança com os quais os pais haviam concordado e Eler (2018a), Carvalho e antes e solicitar uma nova concordância dos pais. Eler (2018b)	
F04	Apresentar a política de privacidade da empresa	Apresentar e facilitar o acesso à política de privacidade da empresa Carvalho e Eler (2017), Car-privacidade da empresa do brinquedo, que define as regras básicas sobre as quais a empresa se valho e Eler (2018a), Carva-compromete a lidar com os dados que ela terá acesso. lho e Eler (2018b)	
F05	Garantir autenticidade de acesso	Verificar se o usuário cadastrado na ferramenta é realmente os pais da Rafferty <i>et al.</i> (2017), Lic-criança por meio de algum mecanismo de verificação, como confirmação cardi <i>et al.</i> (2014), More e de acesso por e-mail, formulário assinado e enviado digitalmente, cartão Chatterjee (2017) de crédito com débito reembolsado etc.	
F06	Criar regras de privacidade	Permitir que os pais criem “regras de privacidade” para definir como os Rafferty, Fantinato e Hung dados manipulados pelo brinquedo (incluindo informações de identificação (2015), Hung <i>et al.</i> (2016), pessoal da criança) deverão ser coletados, manipulados, compartilhados, Rafferty <i>et al.</i> (2017), Hung, divulgados e enviados, permitindo ou negando acesso aos dados de acordo Fantinato e Rafferty (2016a) com as preferências do usuário.	

- F07 Disponibilizar modelos de Auxiliar os pais na criação de “regras de privacidade” por meio da disponibilização de modelos (ou seja, templates) de regras de privacidade, tino, Ferrari e Perego (2010) incluindo modelos externos. Esses modelos devem funcionar como regras de privacidade predefinidas que podem ser alteradas posteriormente para atender exatamente o desejo do usuário.
- F08 Definir data de validade Permitir que os pais definam uma data de validade para as regras de Rafferty *et al.* (2017) de regra de privacidade privacidades criadas, incluindo períodos pré-determinados ou indeterminados.
- F09 Consultar descrição de re- Permitir que pais verifiquem, a qualquer momento, todos os detalhes de Rafferty *et al.* (2017), Lic- gra de privacidade uma regra de privacidade já criada anteriormente por eles. cardi *et al.* (2014)
- F10 Desabilitar regra de pri- Permitir que os pais possam, a qualquer momento, desabilitar uma regra McReynolds *et al.* (2017a) vacidade de privacidade criada anteriormente por eles. Uma regra de privacidade desabilitada deixa de funcionar, mas não é apagada, podendo ser habilitada novamente posteriormente.
- F11 Disponibilizar diretrizes Fornecer aos pais materiais informativos contendo orientações sobre riscos European Commission para os pais de privacidade online para crianças que usam brinquedos inteligentes (2017), Hung, Fantinato e assim como conteúdos para facilitar o aprendizado de uso da ferramenta, Rafferty (2016a), Fantinato destacando a importância dos pais usarem os recursos fornecidos pela *et al.* (2018b) ferramenta de controle parental.
- F12 Disponibilizar links úteis Disponibilizar para os pais links para conteúdos importantes relacionados Canada (2018) para os pais a privacidade online infantil, facilitando o acesso a, por exemplo, atos, leis, políticas de privacidade da empresa de brinquedos etc.
- F13 Informar sobre con- Explicar aos pais sobre restrições que algumas funcionalidades do brin- Rafferty *et al.* (2017), Lic- seqüências da criação de quedo poderão apresentar se determinados tipos de regras de privacidade cardi *et al.* (2014) regras de privacidade muito restritivas forem criadas.
- F14 Classificar riscos de priva- Classificar riscos de privacidade infantil para ajudar os pais em suas Hung, Fantinato e Rafferty cidade online infantil tomadas de decisão na criação de regras de privacidade. Essa classificação (2016a) pode ser realizada com base em técnicas estatísticas ou de aprendizado de máquina, como modelos probabilísticos generativos. Os riscos de privacidade podem, por exemplo, ser listados por frequência de ocorrência ou grau de ameaça.

- F15 Disponibilizar acesso a Fornecer aos pais respostas para as perguntas mais frequentes e relevantes USA (2002) “Dúvidas Comuns” (FAQ) relacionadas ao uso do brinquedo inteligente e da ferramenta de controle parental.
- F16 Disponibilizar canal de Proporcionar um canal de comunicação rápido e fácil para que os pais Hung *et al.* (2016), Rafferty, fácil comunicação (Chat) possam resolver dúvidas, registrar reclamações e enviar sugestões perante Fantinato e Hung (2015) à empresa de brinquedos.
- F17 Remover dados sensíveis Permitir que os pais solicitem que a empresa do brinquedo exclua todas Rafferty *et al.* (2017), Hung e/ou PII os dados sensíveis e/ou de “Informações Pessoais identificáveis” (Personally *et al.* (2016), Rafferty, Fanti- Identifiable Information - PII) coletadas da criança durante suas interações nato e Hung (2015) com o brinquedo até o momento.
- F18 Manter histórico de ativi- Registrar o histórico de todas as atividades realizadas pela criança ao Hung *et al.* (2016), Rafferty, dades da criança usar o brinquedo inteligente, incluindo a gravação de conversas com o Fantinato e Hung (2015), Fu- brinquedo (se o brinquedo possuir microfone) e disponibilizar esse histórico ertes *et al.* (2015), Tenna- de atividades para acesso pelos pais (incluindo das conversas gravadas). koon, Saridakis e Moham- med (2018)
- F19 Monitorar e alertar sobre Aplicar técnicas de processamento de língua natural e reconhecimento de Hung *et al.* (2016), Euro- assuntos suspeitos menci- padrões nos diálogos entre a criança e o brinquedo inteligente para alertar pean Commission (2017), onados pela criança imediatamente os pais caso sejam identificados assuntos suspeitos falados Fantinato *et al.* (2018b), pela criança, se desejado pelos pais. Por exemplo, palavras como drogas, Moini (2017) arma, morte, assédio, sangue, sexo etc.

Fonte: Otávio de Paula Albuquerque, 2020

Tabela 5 – Requisitos não-funcionais de usabilidade para ferramenta de controle parental

ID	Req. Usabilidade	Descrição	Fonte
U01	Multipлатформа	Os pais devem poder usar a ferramenta de controle parental no seu ambiente tecnológico conhecido, considerando, por exemplo, diferentes tipos de dispositivos móveis e sistemas operacionais.	European Commission (2017)
U02	Multiplos usuários	A ferramenta de controle parental deve permitir diferentes pais ou responsáveis legais criarem regras de privacidade para diferentes crianças.	Hung, Fantinato e Rafferty (2016a)
U03	Fácil de instalar	Os pais devem ser capazes de entender e gerenciar facilmente o processo de instalação da ferramenta de controle parental.	European Commission (2017)
U04	Fácil uso	A empresa desenvolvedora da ferramenta de controle parental deve seguir os princípios de usabilidade de software, para oferecer aos pais uma ferramenta fácil de entender e de usar, de forma rápida e intuitiva.	European Commission (2017)

Fonte: Otávio de Paula Albuquerque, 2020

Tabela 6 – Requisito não-funcional de interoperabilidade para ferramenta de controle parental

ID	Req. Interoperabilidade	Descrição	Fonte
I01	Interoperabilidade semântica	A ferramenta de controle parental deve poder trocar informações de forma clara e correta com serviços móveis.	Bertino, Ferrari e Perego (2010)

Fonte: Otávio de Paula Albuquerque, 2020

Tabela 7 – Requisito não-funcional de implementação para ferramenta de controle parental

ID	Req. Implementação	Descrição	Fonte
IM01	Implementar seguindo o <i>Privacy by Design</i>	A empresa desenvolvedora da ferramenta de controle parental deve implementar efetivamente ações técnicas e organizacionais apropriadas para atender aos requisitos de privacidade dos regulamentos legais e proteger os direitos dos proprietários dos dados.	EU (2016)

Fonte: Otávio de Paula Albuquerque, 2020

Tabela 8 – Requisitos não-funcionais de segurança para ferramenta de controle parental

ID	Req. Segurança	Descrição	Fonte
S01	Autenticar usuários	A ferramenta de controle parental deve autenticar todos os seus usuários para garantir que apenas os pais ou responsáveis legais estejam desempenhando o papel de guardião da criança.	Bertino, Ferrari e Perego (2010), Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b)
S02	Criptografar “Informações Pessoais Identificáveis” (PII)	A ferramenta de controle parental deve criptografar as “Informações Pessoais Identificáveis” (PII) a serem acessadas por outros aplicativos, mesmo que o acesso seja por outros aplicativos sendo executados no memo dispositivo móvel.	Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b)
S03	Autenticar e autorizar comunicações	A comunicação entre a ferramenta de controle parental e o ambiente de computação para brinquedos deve usar protocolos de comunicação que permitam mecanismos de autenticação e autorização.	Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b)
S04	Criptografar comunicação	A comunicação entre a ferramenta de controle parental e o ambiente de computação para brinquedos deve usar mecanismos criptográficos.	Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b)
S05	Garantir a integridade do arquivo de configuração	A integridade do arquivo de configuração deve ser verificada e mantida para cada sessão de uso da ferramenta de controle parental no dispositivo móvel.	Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b)
S06	Exigir certificado digital para serviços móveis	A ferramenta de controle parental deve garantir que as “Informações Pessoais Identificáveis” (PII) da criança sejam enviadas ou compartilhadas apenas com serviços móveis que possuem certificados digitais que permitem a verificação de identidade digital.	Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b)
S07	Notificar violações de segurança	A ferramenta de controle parental deve notificar os pais sobre qualquer violação de segurança detectada em relação ao seu uso.	Liccardi <i>et al.</i> (2014), Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b)
S08	Seguir boas práticas de segurança de software	A empresa desenvolvedora da ferramenta de controle parental deve seguir princípios de segurança de software conhecidos.	CARVALHO; ELER, 2017; CARVALHO; ELER, 2018a; CARVALHO; ELER, 2018b)

Fonte: Otávio de Paula Albuquerque, 2020

Tabela 9 – Requisitos não-funcionais legais para ferramenta de controle parental

ID	Req. Legal	Descrição	Fonte
L01	Cumprir com o consentimento dos pais	A ferramenta de controle parental deve garantir que as “Informações Pessoais Identificáveis” (PII) da criança não sejam coletadas, usadas, compartilhadas ou divulgadas com terceiros sem o consentimento dos pais, considerando suas preferências manifestadas pelas regras de privacidade criadas.	Fantinato, Hung, e Rafferty (2016a)
L02	Cumprir com as normas legais	As operações realizadas, apoiadas e permitidas pela ferramenta de controle parental devem estar em conformidade com as normas legais definidas por leis e regulamentos gerais aplicáveis.	Rafferty <i>et al.</i> (2017), Hung, Fantinato e Rafferty (2016a), Holway e Green (2016)
L03	Cumprir com o direito à privacidade das crianças	As operações realizadas, apoiadas e permitidas pela ferramenta de controle parental devem respeitar os direitos de privacidade das crianças cumprindo as normas e atos específicos para esse fim.	USA (2002), Canada (2018)
L04	Clareza nas informações e manipulação dos dados	“Informações Pessoais Identificáveis” (PII) da criança estão sendo coletadas, como são usadas e compartilhadas com terceiros e práticas adicionais de divulgação.	EU (2016), USA (2002), Liccardi <i>et al.</i> (2014), Bertino, Ferrari e Perego (2010), Carvalho e Eler (2017), Carvalho e Eler (2018a), Carvalho e Eler (2018b), Zimbeck <i>et al.</i> (2017), Canada (2018)

Fonte: Otávio de Paula Albuquerque, 2020

Requisitos encontrados em diferentes fontes que se assemelhavam em sua descrição, foram agrupados em um único requisito, com o intuito de criar um conjunto de requisitos mais compacto e estável. Alguns requisitos se sobrepõem, especialmente os requisitos funcionais. Embora tenham ocorrido tentativas de evitar a sobreposição, nem sempre foi possível tendo em vista que esses requisitos em específico, geralmente, apresentavam diferentes níveis de granularidade.

Alguns requisitos podem se anular, como o caso do requisito funcional de *monitoramento de atividades*, e o requisito não-funcional legal que está relacionado à privacidade da criança. Embora as crianças devam ter privacidade, inclusive dos seus pais, esses sistemas de monitoramento dos pais são populares e vistos como uma maneira de proteger as crianças online e offline (JONES; MEURER, 2016a).

Por mais que alguns dos requisitos aqui apresentados possam ser vistos como sobrepostos aos requisitos gerais de privacidade e segurança de brinquedos inteligentes, eles de fato se referem especificamente apenas às ferramentas de controle parental. Por exemplo, os requisitos de segurança não-funcionais referem-se apenas à segurança necessária para uma ferramenta de controle parental, e não ao brinquedo inteligente na totalidade.

Ainda existem requisitos não-funcionais relevantes não mencionados aqui, como de desempenho, por exemplo. No entanto, eles são genéricos para a maioria dos aplicativos móveis, sem detalhes específicos para o contexto do controle parental para brinquedos inteligentes, portanto, não são destacados no material consultado; por isso, também não estão listados aqui.

4.2 *Atos e regulamentos legais*

Embora este trabalho contemple 20 trabalhos de pesquisa e leis sobre privacidade, a completude deste conjunto de requisitos apresentados não é garantida, tendo em vista possíveis ocasiões particulares que não foram cobertas pela literatura atual. Entretanto, entende-se que todos os requisitos básicos foram levantados aqui, além de requisitos avançados relevantes, identificados em trabalhos complexos e bem classificados. Além disso, uma comparação entre os requisitos propostos e as recomendações sobre controle parental e proteção à privacidade feita pelos atos e regulamentos citados anteriormente,

foi realizada e apresentada na tabela 6, mostrando a amplitude do conjunto de requisitos identificados.

Quadro 6 – Cumprimento dos requisitos de controle parental por normas legais.

ID Req.	COPPA	PIPEDA	GDPR	SIP-BENCH
F01				
F02	X		X	
F03	X			
F04	X		X	
F05	X			
F06		X		
F07				
F08				
F09		X		
F10				X
F11		X		
F12		X		
F13				
F14				
F15	X			
F16	X			
F17	X			
F18		X		
F19	X			
U01				X
U02				X
U03				X
U04				X
I01				
IM01			X	
S01	X	X		
S02				
S03				
S04				
S05	X			
S06				
S07	X		X	
S08	X			
L01	X	X	X	
L02	X	X	X	
L03	X	X	X	
L04	X	X	X	

Fonte: Otávio de Paula Albuquerque, 2020

As referências que os fabricantes de brinquedos têm atualmente para apoiar o desenvolvimento de ferramentas de controle parental são normas legais como COPPA,

PIPEDA e GDPR, apresentadas anteriormente. No entanto, como essas normas são gerais, pouca ênfase é colocada especificamente para o controle parental, como pode ser visto na análise apresentada na tabela 6. Pode-se verificar que nenhuma das três normas internacionais conhecidas que coordenam a proteção de privacidade de dados atende à maioria dos requisitos levantados. De fato, a COPPA, que cobre o maior número deles, responde por apenas 43%. O PIPEDA atende apenas 27%, enquanto o GDPR apenas 21%. Mesmo o SIP-BENCH III, que é uma referência criada especificamente para ferramentas de controle parental, atende somente por 13%. Se apenas os requisitos funcionais forem considerados, os níveis de cobertura são de 21%, 13%, 5% e 2%, respectivamente.

Além de apresentar pouca cobertura geral, cada norma se concentra em diferentes aspectos desses requisitos. Por exemplo, apenas os requisitos não-funcionais legais (L1, L2, L3 E L4) são atendidos por três normas, o que parece mais natural. Por outro lado, existem nove requisitos não atendidos por nenhuma norma, incluindo cinco requisitos funcionais. Como resultado, duas principais conclusões podem ser destacadas: (1) essas normas são limitadas em geral para ajudar a desenvolver ferramentas de controle dos pais para brinquedos inteligentes, mostrando que é necessário algum padrão específico adicional; e (2) o conjunto de requisitos aqui apresentados tem um escopo bastante amplo, tornando-o muito relevante para sua finalidade.

4.3 *Considerações finais*

Como principal contribuição, 37 requisitos de controle parental foram identificados e organizados em: 19 requisitos funcionais e 18 não funcionais (4 usabilidade, 1 interoperabilidade, 1 implementação, 8 requisitos de segurança e 4 requisitos legais), representando um conjunto robusto de requisitos para o desenvolvimento de ferramentas de controle parental para brinquedos inteligentes. A análise mostrou que as normas gerais de proteção de privacidade de dados são limitadas para atingir o objetivo, portanto, os requisitos sistematizados neste trabalho devem ser relevantes para esta área de pesquisa.

Existem atualmente leis internacionais que abordam parcialmente a privacidade e segurança online da criança como a PIPEDA e a GDPR, ou que são específicas para o tema como o COPPA, no entanto ainda não existem leis e regulamentos que tratam das áreas mais atuais como a de brinquedos inteligentes. No Brasil, pelo fato do brinquedo inteligente

ainda não ser uma realidade no mercado infantil, não existem leis ou regulamentos voltados para a preservação da privacidade de crianças, no qual é regida apenas pelo Regulamento Geral sobre a Proteção de Dados (GDPR), em vigor no território nacional também.

5 Modelo conceitual da ferramenta de controle parental

Apresenta-se neste capítulo de Diagramas de Casos de Uso (UCD) e Diagramas de Atividades (AD), que organizam os requisitos funcionais apresentados na tabela 4 em modelos conceituais da ferramenta de controle parental. São apresentados os elementos importantes do domínio da ferramenta e suas relações para a implementação, sem demonstrar os detalhes técnicos, que foram abordados no capítulo seguinte.

5.1 Visão geral das funcionalidades

O modelo conceitual apresenta as funcionalidades da ferramenta de controle parental por meio dos requisitos funcionais expostos no capítulo 4. A figura 15 demonstra uma visão geral das funcionalidades desejadas para a composição da ferramenta, apresentada através de um diagrama de Casos de Uso. Os requisitos estão representados em suas respectivas funcionalidades por seus códigos de identificação. As funcionalidades do modelo indicadas nos diagramas são apresentadas no decorrer dessa seção, algumas delas estão contraídas, representadas pelo “*” ao lado de seu código de identificação (por exemplo [F01*]), ou foram agrupadas por terem finalidades semelhantes e estão representadas pela identificação “[...]”, no qual serão apresentadas de forma expandida.

Figura 15 – Casos de uso das funcionalidades principais

O modelo conceitual tem como funcionalidade inicial *criar perfil de usuário*, na qual permite que pais ou responsáveis legais possam criar um perfil de usuário da ferramenta, e assim ter acesso as outras funcionalidades.

5.2 Criação do perfil de usuário

A figura 16 detalha a funcionalidade da *criação do perfil de usuário*, que no caso dessa ferramenta podem ser os pais (pai ou mãe) ou o responsável legal da criança. É necessária a criação do perfil para estabelecer um canal de comunicação entre o responsável pela criança e a empresa do brinquedo, assegurando de que é o responsável de fato que está no controle da ferramenta.

A figura 17 sugere um possível procedimento para executar essas funcionalidades: primeiramente, os pais/responsáveis devem inserir alguns dados de contato para o cadastro do perfil de usuário, criando um canal de comunicação com a empresa, além de determinarem se aceitam ou não receber notificações de mudanças na política de privacidade da empresa do brinquedo inteligente; após essa etapa, os pais inserem o dado da criança, no qual é requisitado apenas o primeiro nome para fins de personalização e formalidades, assim a ferramenta, ao necessitar encaminhar para o pai algo relacionado à criança, refere-se especificamente ao nome inserido, tornando a abordagem mais pessoal, além disto, os pais devem consentir com a licença de acordo de usuário final (*End User License Agreement* - EULA), no qual os pais tornam-se proprietários dos dados do seu filho; a ferramenta então apresenta aos pais a política de privacidade da empresa de brinquedos, em formato de texto estruturado por tópicos, com a qual os pais devem concordar, ou não, antes de finalizar o cadastro do perfil de usuário. A clareza na política de privacidade é de suma importância para que haja um julgamento consciente dos pais sobre se concordam ou não com tal política.

Há a necessidade de a ferramenta verificar a autenticidade das informações: a legitimidade dos dados relatados e os consentimentos fornecidos. No entanto, existem alguns diferentes mecanismos para realizar a autenticação do usuário, que podem ser usados em diferentes momentos do cadastro de usuário. A ferramenta deve dedicar esforços razoáveis para verificar se o consentimento é dado ou autorizado pelo detentor da responsabilidade de pai/responsável sobre a criança, considerando a tecnologia disponível (EU, 2016).

Finalmente finalizada e verificada a autenticidade do cadastro do perfil de usuário da ferramenta, as demais funcionalidades são habilitadas.

Figura 16 – Casos de uso da criação do perfil de usuário.

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 17 – Diagrama de atividade da criação do perfil de usuário.

Fonte: Otávio de Paula Albuquerque, 2020.

5.3 Criação da regra de privacidade

A figura 18 detalha a criação das regras de privacidade, a principal funcionalidade da ferramenta e a que executa o controle de acesso. As regras de privacidade são criadas para permitir ou restringir a coleta, o uso, o compartilhamento ou a divulgação das informações pessoais da criança, de acordo com as preferências selecionadas por pais/responsáveis.

A figura 19 sugere um fluxo de atividade para executar essa funcionalidade. Para a criação da regra de privacidade, primeiramente, o pai/responsável deve escolher entre as duas opções de criação: usar um modelo de regra de privacidade existente com as suas configurações predefinidas ou criar uma regra de privacidade desde o começo.

Para o uso de modelo de regra de privacidade predefinido, a ferramenta deve fornecer regras distintas com opções para diferentes cenários, apresentando suas descrições e suas finalidades. Essa opção de criação de regra é considerada para os cenários mais comuns.

Para a *criação da regra de privacidade desde o começo*, o primeiro passo é configurar as definições gerais da regra, preenchendo seus dados de identificação. No segundo passo configura-se o controle de acesso principal, onde são definidas às três entidades básicas de um controle de acesso simples: o sujeito solicitante do acesso que é caracterizado como uma entidade tripla, composto por um brinquedo, um dispositivo e um serviço móvel, no qual são as principais entidades que compõem um sistema de computação para brinquedos (RAFFERTY *et al.*, 2017); a operação que o sujeito deseja executar, podendo ser enviar, capturar, armazenar etc.; e os objetos que poderão ser manipulados (coletados, armazenados, compartilhados) pelo solicitante do acesso. O passo seguinte trata o controle de acesso estendido, proposto por Rafferty *et al.* (2017), no qual são incluídas mais quatro entidades de privacidade, sendo elas: o propósito, o destinatário, a obrigação e a retenção. Como último passo desta funcionalidade, os pais/responsáveis devem revisar os dados definidos no decorrer das etapas e confirmá-los, concluindo a criação da regra de privacidade.

O sistema de computação para brinquedos consiste em um brinquedo físico com dispositivos móveis em sua estrutura, que executam um ou mais serviços móveis, consequentes da interação entre o brinquedo e a criança. Para o serviço móvel ter acesso aos dados: (1) ele precisa solicitar acesso ao dispositivo, que por sua vez encaminha a solicitação para o módulo de tomada de decisão; (2) o módulo irá checar as regras de

privacidade salvas no banco de dados, e realizar a comparação entre elas e a política de privacidade do serviço móvel, e com isso tomar a decisão de acesso. As regras, por sua vez, são baseadas em tais serviços móveis, que a partir da sua configuração personalizada, irá prover as preferências escolhidas de forma genérica, no qual servirá de referência para qualquer sujeito que solicitar acesso àquele determinado tipo de serviço móvel.

Figura 18 – Casos de uso da criação de regra de privacidade.

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 19 – Diagrama de atividade da criação de regra de privacidade.

Fonte: Otávio de Paula Albuquerque, 2020.

As duas funcionalidades descritas anteriormente (*criar perfil de usuário* e *criar regra de privacidade*), baseiam-se na estrutura e fluxo de atividades do modelo Rafferty. O modelo Rafferty toma sua decisão de acesso apoiado nas entidades básicas (sujeito, operação e objeto), somadas as entidades de privacidade (propósito (*purpose*), destinatário (*recipient*), retenção (*retention*) e obrigação (*obligation*)), nos quais são entidades provindas de projetos da Plataforma de Preferências de Privacidade (P3P), elaboradas para auxiliar na criação de ferramentas de controle de acesso mais finas (*fine grained*), garantindo maior flexibilidade entre a coleta de dados de contexto, importante para a utilização eficiente dos serviços no brinquedo, e a proteção e privacidade dos dados da criança.

Considerando as limitações do modelo Rafferty, a intenção deste trabalho é desenvolver um modelo que contemple todos os tipos de dados/objetos e operações envolvidas no uso dos dispositivos e sensores na estrutura do brinquedo inteligente, tendo em vista a crescente evolução tecnológica desses brinquedos.

5.4 Gestão das regras de privacidade

A partir da criação da primeira regra de privacidade, a ferramenta habilita a gestão das regras de privacidade. No caso de uso da figura 20, são apresentadas as funcionalidades relacionadas a gerência das regras, desde as funcionalidades mais básicas como: criar, editar e apagar a regra de privacidade, até a visualização da descrição da regra e desabilitação da mesma, na qual retira a permissão de acesso do serviço móvel sem precisar apagar a regra criada para o acesso.

Figura 20 – Casos de uso gerenciar regras de privacidade.

Fonte: Otávio de Paula Albuquerque, 2020.

5.5 Aprendizado e monitoramento

Na figura 21 está representado o diagrama de caso de uso do *guia para aprendizado da ferramenta*, no qual estão as funcionalidades relacionadas ao aprendizado dos pais frente ao ambiente de computação para brinquedos e a ferramenta. Devido à dificuldade dos pais com novas tecnologias, criar mecanismos e apresentar conteúdos de fácil acesso para ensinar sobre o uso da ferramenta e sobre o seu contexto é imprescindível. Disponibilizar funcionalidades que apresentem aos pais/responsáveis a ferramenta de forma eficiente, bem como conscientizá-los sobre como usá-la, e esclarecer, por meio do apoio didático, sobre a estrutura do ambiente de brinquedos e os riscos que o envolvem, ajudam os pais a tomarem decisões de acesso mais conscientes.

Ferramentas que auxiliem os pais a monitorar as atividades dos seus filhos no uso do brinquedo também são apresentadas na figura 22. *Visualizar histórico de atividades* é a funcionalidade que apresenta aos pais o histórico de interações da criança com o brinquedo, indicando suas datas e horas, *verificar alerta de assuntos sensíveis* é um mecanismo de monitoramento contínuo feito pela própria ferramenta para brinquedos que tem como funcionalidade o diálogo interativo, no qual relata aos pais quando algum assunto como: sexo, assédio, abuso, sangue, morte etc., for falado pela criança. Embora as crianças devam ter privacidade, inclusive dos seus pais, essas funcionalidades de monitoramento

são populares e vistas como uma maneira de proteger as crianças online e offline (JONES; MEURER, 2016b).

Figura 21 – Casos de uso guia de aprendizado da ferramenta.

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 22 – Casos de uso monitoramento de atividade.

Fonte: Otávio de Paula Albuquerque, 2020.

5.6 Suporte aos pais

As demais funcionalidades foram agrupadas no mesmo diagrama por se tratar de funcionalidades com finalidades similares de suporte técnico, onde a empresa proporciona um apoio direto ao usuário (pais ou responsáveis legais) da ferramenta. São criados canais de comunicação com a empresa do brinquedo inteligente, no qual os pais podem receber notificações de atualizações na política de privacidade, tirar dúvidas, fazer recomendações

e sugestões imediatas, ou até mesmo solicitar a remoção dos dados sensíveis coletados da criança, via ferramenta de controle parental.

Visualizar atualizações na política de privacidade, acessar chat e visualizar FAQ são funcionalidades que basicamente facilitam o acesso a informações específicas sobre a empresa, o brinquedo e sua política de privacidade, mas não se prendem somente a esse tipo de informação. A ferramenta deve disponibilizar uma funcionalidade como *solicitar remoção de dados sensíveis*, para os pais poderem solicitar a remoção dos dados sensíveis coletados até aquele momento, sem a necessidade de intermediários.

Figura 23 – Casos de uso área de Suporte.

Fonte: Otávio de Paula Albuquerque, 2020.

5.7 Considerações finais

O modelo conceitual visou delimitar uma estrutura com base na análise dos requisitos funcionais para o posterior desenvolvimento da ferramenta, identificando as funcionalidades e entidades que fariam parte do escopo, e criando a relação entre elas.

Para o desenvolvimento do modelo conceitual, levou-se em consideração apenas os requisitos funcionais, nos quais foram dispostos em diagramas de casos de uso, descrevendo o conjunto de funcionalidades e suas interações na ferramenta.

As funcionalidades *criar perfil de usuário* e *criar regra de privacidade* são consideradas mais complexas, exigindo a criação de diagramas de atividade para a apresentação do fluxo de atividades, baseados no modelo Rafferty.

6 Protótipo da ferramenta de controle parental

Como citado anteriormente em 1.1, os pais, geralmente, possuem pouco conhecimento das novas tecnologias e técnicas de controle de acesso como a criação de regras de privacidade. A necessidade de ensinar o passo a passo da ferramenta e proporcionar um ambiente funcional e propício ao aprendizado é primordial, tendo em vista o uso eficiente da ferramenta.

Considerando o modelo conceitual e suas funcionalidades, foi implementado um protótipo da ferramenta de controle parental para brinquedos inteligentes. Foi usado um processo de desenvolvimento iterativo e incremental, no qual o autor deste projeto e o seu orientador assumiram os papéis dos *stakeholders* do projeto, sendo o orientador o cliente, onde após a conclusão de uma iteração sugeria os *feedbacks* para os eventuais incrementos e alterações.

O desenvolvimento do protótipo durou 8 meses, no qual o 1º ciclo de iteração teve início em Junho de 2019, com duração de quatro meses, esse foi o ciclo mais longo por se tratar do primeiro, no qual os requisitos estavam sendo identificados e levantados, e o planejamento do escopo do protótipo ainda sendo definido, com tudo, a alternância entre as primeiras etapas da iteração – comunicação e planejamento –, foram recorrentes até a definição do escopo do protótipo, das tecnologias e ferramentas que seriam usadas e do roteiro apropriado, e assim seguir para as próximas etapas.

Ainda na etapa de planejamento do processo de desenvolvimento, definiu-se que a ferramenta seria desenvolvida apenas para a plataforma Android, por se tratar de um sistema de código aberto, mais usado ao redor do mundo (statcounter Globalstats, 2020); além do autor deste projeto ter familiaridade com a linguagem de programação Java, linguagem base para programação Android.

Para o desenvolvimento, foi usado o Ambiente de Desenvolvimento Integrado (Integrated Development Environment - IDE) Android studio, ferramenta especificamente configurada para desenvolvimento de aplicações Android. Foi usado na programação, bibliotecas e APIs (*Application Programming Interface*) nativas do Android, com exceção de apenas uma API externa, denominada *AppIntro* para a implementação das telas de introdução do protótipo, apresentadas na seção a seguir.

Nas etapas restantes da 1ª iteração, foram então construído o modelo conceitual e posteriormente desenvolvida primeira versão do protótipo, contendo apenas as funcionalidades principais: *criar perfil dos pais* e *criar regras de privacidade*, dispostas em uma única tela principal. Para a implementação de tais funcionalidades, foram seguidos os passos apresentados por Rafferty, Fantinato e Hung (2015), em suas demonstrações de modelos de interface para as funcionalidades.

O 2º, 3º e 4º ciclo de iteração tiveram duração de um mês cada, no qual tiveram um grande número de alterações/incrementos, principalmente na etapa da construção do protótipo, onde foram implementadas as demais funcionalidades, e definidos os modelos de interface e navegação que seriam usados.

Para a construção e estruturação das interfaces, foram usadas ConstraintLayout para o desenvolvimento de *users interfaces* responsivas, tendo em vista a grande variedade de dimensões entre os *smartphones* atuais. As cores principais usadas nos *layouts* do protótipo (verde e branco), são cores disponibilizadas pela própria IDE, sendo o branco a cor *default* empregada nas interfaces e o verde uma cor pré-definida denominada *colorPrimary*. Bem como foi usada a fonte *default* disponibilizada pela IDE, a *sans serif*.

Para a navegação principal, foi usado o tipo *bottom navigation menu*. Tal tipo de navegação para menu foi escolhida tendo em vista sua adequação de navegação para o que pretendia-se seguir, no qual seria o acesso direto e fácil às funcionalidades da ferramenta, agrupadas em três principais áreas: gerenciar regra, área dos pais e área de suporte. Além disso, é o tipo de navegação de menu comumente usado em aplicações móveis conhecidas como: Facebook, Twitter, Instagram, LinkedIn etc.

Os últimos ciclos de iteração (5º, 6º e 7º) foram mais curtos, com duração de aproximadamente 10 dias cada, no qual foram realizados os ajustes finais, principalmente no conteúdo textual da ferramenta, para a entrega da última versão da ferramenta, e assim, realizar o próximo passo do projeto, a avaliação dos requisitos e do protótipo.

Apesar da implementação ter seguido os principais padrões de design de programação disponibilizados pelo Android, por se tratar de um protótipo, não se levou em consideração a implementação explícita dos modelos de usabilidade e acessibilidade, ou mesmo dos modelos de testes para tais aspectos, no qual foram abordados intuitivamente, levando em consideração a experiência dos desenvolvedores relacionados a engenharia de software.

6.1 Introdução da ferramenta

Considerando a necessidade de guiar os pais em todos os passos da ferramenta, foram criadas as telas de introdução (figura 24). Ao iniciar o protótipo são apresentadas as telas que visam descrever sucintamente a ferramenta, contendo informações iniciais do primeiro acesso. É apresentado de modo geral: qual a finalidade da ferramenta; como funciona a principal funcionalidade, a *criação de regras de privacidade*; a *área dos pais*, onde os pais podem consultar materiais e aprender sobre a ferramenta e o ambiente de computação para brinquedos; por último apresenta-se o próximo passo, a *criação do perfil de usuário*, direcionando o usuário para a funcionalidade, a primeira da ferramenta.

Figura 24 – Tela de apresentação da ferramenta.

Fonte: Otávio de Paula Albuquerque, 2020.

6.2 Criação do perfil de usuário

Cria perfil de usuário é o primeiro passo da ferramenta (figura 25). Baseada no modelo Rafferty, essa funcionalidade é separada em três seções: dados do pai ou responsável, dados da criança e política de privacidade.

Na tela de *dados do pai ou responsável*, o pai/responsável preenche os seus dados de contato, com o intuito de criar um canal de comunicação com a empresa do brinquedo. O pai, então, decide se deseja receber notificações de mudanças na política de privacidade do brinquedo (é fortemente recomendado que os pais sempre selecionem a caixa de diálogo para receber tais atualizações).

Em *dados da criança*, é solicitado o preenchimento do primeiro nome da criança, essa informação é usada apenas para formalidades de gestão; além disso, o pai/responsável deve aceitar o acordo de licença do usuário final (*End-user license agreement* - EULA), criando um acordo legal para o uso da aplicação e tornando-se proprietário dos dados da criança.

Na *política de privacidade*, é apresentado ao pai a política de privacidade da empresa do brinquedo, a qual deve ser revisada, e de acordo com a preferência, ter os termos aceito ou rejeitado. Caso aceito, o pai consente que está ciente dos termos relatados pela empresa, incluindo suas políticas de manipulação de dados (coleta, armazenamento, compartilhamento etc.), que servirão de informações para futuras criações de regras de privacidade. Por isso, há a necessidade das políticas de privacidade serem apresentadas de forma clara e objetiva. Após concordar e finalizar a criação do perfil, são habilitadas as outras funcionalidades da ferramenta. A política de privacidade usada no protótipo foi adaptada e traduzida da empresa de brinquedos Toymail Co.

Figura 25 – Criação do perfil de usuário.

Dados do pai ou responsável	Dados da criança	Política de privacidade	Dados do pai ou responsável	Dados da criança	Política de privacidade	Dados do pai ou responsável	Dados da criança	Política de privacidade
Primeiro nome: ____ Último nome: ____ E-mail: ____ Você opta por receber e-mails e notificações de atualização na política de privacidade? Por favor, indique abaixo caso você queira recebê-los. ☐ Sim, eu desejo receber e-mails e notificações. As notificações de atualização serão exibidas em: "Área de suporte > Atualização na política".	Informe o nome da criança, apenas para fins formais de comunicação. ____ Primeiro nome Marcando a caixa abaixo, você concorda que o usuário é uma criança menor de 13 anos; que você é o pai/guardião legal e o responsável pela privacidade da criança; que você reivindica a propriedade dos dados da criança que são coletados por meio do dispositivo móvel; e que você está agindo em nome da criança para proteger seus dados.	☐ Eu concordo.	VOLTAR	PRÓXIMO	Política de privacidade do brinquedo SEGURANÇA A Empresa é segura? A Empresa Sa leva a segurança a sério e se preocupa com a integridade de suas informações pessoais. Os brinquedos da Empresa são certificados pelo Programa de Selo iKeepSafe. Para saber mais, visite ikeepSAFE.org . Os brinquedos são construídos sobre uma plataforma certificada no padrão UL-2900-2-2 para segurança cibernética.	☐ Eu li e concordo com os termos.	VOLTAR	FINALIZAR
CANCELAR	PRÓXIMO							

Fonte: Otávio de Paula Albuquerque, 2020.

Apesar do protótipo da ferramenta não ter implementado um mecanismo de autenticação de usuário, é necessário que uma ferramenta de controle parental verifique a autenticidade das informações preenchidas no decorrer da funcionalidade, confirmando se a função de pai é realmente desempenhada pelo responsável legal da criança. Pode-se verificar a autenticidade das informações por meio de algum mecanismo de verificação/autenticação

como a confirmação de acesso por e-mail, formulário assinado, cartão de crédito com débito reembolsado etc.

6.3 Áreas principais da ferramenta

Após o cadastro de usuário realizado pelo pai/responsável, são habilitadas as telas principais da ferramenta e suas funcionalidades como demonstrado na figura 26, sendo elas: gerenciar regras, área dos pais, área de suporte, selecionáveis a partir do menu inferior.

6.3.1 Área dos pais

A tela 2 da figura 26 apresenta a *área dos pais*, a qual está dividida em duas subáreas. Em *guias para os pais* estão selecionadas as funcionalidades referentes ao aprendizado e auxílio à tomada de decisão dos pais, apresentando suas respectivas funcionalidades na figura 27.

Figura 26 – Telas principais da ferramenta

Fonte: Otávio de Paula Albuquerque, 2020.

Em *restrições de uso*, o intuito é mostrar as restrições de desempenho e/ou funcionalidade que a criação de regras de privacidade pode causar, e como pode afetar os serviços e interações no brinquedo. Por exemplo, Pokémon GO da Niantic, coleta dados do Sistema

de Posicionamento Global (GPS) para jogabilidades ao ar livre, sem a coleta de dados de localização, o jogo não conseguirá prover os serviços necessários para a jogabilidade.

A *classificação de riscos*, visa apresentar uma lista de prováveis riscos relacionados ao uso do brinquedo, levando em consideração os dispositivos e sensores integrados nele. A classificação dos riscos será realizada com base em técnicas estatísticas ou de aprendizado de máquina como modelos probabilísticos generativos, auxiliando na tomada de decisão dos pais. Essa funcionalidade e a anterior não foram implementadas no protótipo, onde foram criadas suas respectivas interfaces, e foram apresentadas suas descrições.

Em *guia para aprendizado*, são disponibilizados pela empresa do brinquedo, conteúdos educativos como vídeos, textos, imagens etc. (para o protótipo foram usados apenas vídeos sobre brinquedos inteligentes), que auxiliem no aprendizado dos pais relacionados tanto à utilização da ferramenta, quanto aos aspectos que envolvem o ambiente de computação para brinquedo. Essa funcionalidade visa conscientizar os pais/responsáveis para os riscos que envolvem o ambiente e as formas de preservação e proteção de dados.

Nos *links úteis* são disponibilizados os links considerados importantes para o apoio externo à ferramenta como link dos atos, regulamentos, leis, políticas de privacidade etc. Em *links úteis* pode-se disponibilizar também links para *sites* e conteúdos de terceiros referentes ao aprendizado sobre o ambiente de brinquedos inteligentes, oferecendo alternavas ao *guia para aprendizado*.

Figura 27 – Subárea guia para os pais

Fonte: Otávio de Paula Albuquerque, 2020.

Na subárea de *monitor dos pais* (figura 28) é estabelecida duas funcionalidades de monitoramento: *monitoramento de atividades*, a qual refere-se à funcionalidade que registra e apresenta o histórico de todas as atividades realizadas pela criança ao usar o

brinquedo inteligente, incluindo a gravação das conversas (quando esta funcionalidade é disponibilizada pelo brinquedo), identificadas por data e hora da interação; *alerta de assuntos sensíveis*, recomenda-se que as empresas de brinquedo apliquem técnicas de processamento de linguagem natural nos diálogos entre a criança e o brinquedo inteligente para alertar imediatamente os pais, caso sejam identificados assuntos suspeitos como: sexo, sangue, abuso, assédio, morte etc., se desejado pelos pais. Nenhuma das duas funcionalidades de monitoramento foram implementadas neste primeiro momento, por causa de suas complexidades.

Figura 28 – Subárea monitor para os pais

Fonte: Otávio de Paula Albuquerque, 2020.

Na *área dos pais* há a possibilidade de editar o perfil de usuário ao clicar na figura de perfil, ao lado da saudação no canto superior esquerdo, no entanto, caso queira editar algum dado cadastral, será necessário realizar a autenticação dos dados novamente.

6.3.2 Gerenciar regra

Nas telas de *gerenciar regra* representadas na figura 29, são observadas as funcionalidades que envolvem a gestão da regra de privacidade. Entre elas, destaca-se a principal funcionalidade, *criar regra de privacidade*. Ao criar uma regra de privacidade, ela ficará

listada na tabela *regras de privacidade*, e habilitará automaticamente duas funcionalidades: *visualizar descrição da regra*, os detalhes da regra podem ser visualizados a qualquer momento após ela já ter sido criada; *desabilitar regra*, desabilita a permissão de acesso da regra específica, esta função não apaga a regra criada, apenas a inativa, permanecendo na lista de regras até ser utilizada novamente ou apagada definitivamente. Tal funcionalidade foi baseada no modelo Rafferty, e será mais detalhada a seguir, na seção 6.4.

Junto com a criação da regra, foram implementadas funcionalidades complementares de gestão, *editar* e *apagar* regra de privacidade. Por se tratar de funcionalidades genéricas, *editar* e *apagar* não foram consideradas para o conjunto de requisitos levantados neste trabalho, apesar de suas implementações no protótipo em vista da necessidade de gerir a regra.

Figura 29 – Tela Gerenciar regra

Fonte: Otávio de Paula Albuquerque, 2020.

6.3.3 Área de suporte

A *área de suporte* (figura 30 e 31) estão as funcionalidades de suporte oferecidas pela empresa do brinquedo aos pais, de forma a facilitar o acesso e a comunicação entre ambos. Como primeira parte da área, são apresentadas as atualizações na política de privacidade, quando houver. Caso o pai aceite receber notificações ao realizar o seu cadastro de perfil de

usuário, além de receber via e-mail, as notificações de atualização serão exibidas e listadas na tabela de *atualização na política de privacidade*, na qual são descritas especificamente a parte atualizada, e podem ser visualizadas por completo quando selecionada a opção.

Figura 30 – Atualização na política de privacidade

Fonte: Otávio de Paula Albuquerque, 2020.

Duas funcionalidades que estabelecem uma comunicação direta com a empresa de brinquedos: o *chat* (tela 1 da figura 31), foi implementado para comunicações mais dinâmicas, para dúvidas mais complexas, fazer sugestões e reclamações, inclusive como opção para solicitar a remoção de dados sensíveis, no qual seleciona-se o assunto desejado para o acesso ao chat; o *dúvidas comuns - Faq* (tela 2 da figura 31), serve para o acesso a dúvidas mais simples e imediatas, mas que são frequentemente feitas à empresa de brinquedo.

Em *remover dados sensíveis* (tela 3 da figura 31), caso o pai sinta a necessidade de excluir todos os dados sensíveis coletados por meio da interação da criança com o brinquedo, até o momento, o pai pode solicitar a remoção dos dados perante a empresa, e para isso deve escrever uma justificativa para solicitação. A empresa receberá a solicitação, irá analisar a justificativa, e enviar uma resposta ao pai com o parecer, caso aceito os dados serão excluídos, caso contrário, a empresa enviará um e-mail apresentando o seu contra ponto e agendando uma data para contato formal.

Desativar a conta de usuário (tela 4 da figura 31), consiste da exclusão de todos os dados e desativação da ferramenta, caso o pai queira encerrar as atividades da ferramenta (motivo, por exemplo, o brinquedo não está mais sendo usado). Essa funcionalidade não foi considerada para o conjunto de requisitos funcionais por causa de ser considerada genérica.

Figura 31 – Funcionalidades da área de suporte

Fonte: Otávio de Paula Albuquerque, 2020.

Os links para os textos de *termos de serviço*, documento responsável por conter as condições e regras de uso dos serviços da ferramenta, no qual as empresas delimitam suas responsabilidades a fim de se resguardarem juridicamente; e a *política de privacidade* que trata das informações de práticas e processos relacionados a manipulação de dados adotada pela ferramenta de controle parental, também estão disponibilizados na *área de suporte*.

6.4 Criação da regra de privacidade

A *criação da regra de privacidade* (figura 32) é a funcionalidade mais importante do protótipo da ferramenta, seguindo como base o modelo Rafferty. Como primeiro passo para a criação de uma regra de privacidade o pai/responsável seleciona entre criar as opções de criação: *do início*, criando uma regra nova desde o começo; ou *baseado em modelo*, no qual usa-se um modelo existente de regra de privacidade com as configurações já predefinidas.

Figura 32 – Telas criar regra de privacidade

Fonte: Otávio de Paula Albuquerque, 2020.

Caso selecionada a opção *do início*, o pai é direcionado para a tela de criação da regra de privacidade (figura 33): os primeiros passos para a criação da regra são as *configurações gerais*, onde são preenchidos o nome e a descrição da regra para identificação na ferramenta; posteriormente é configurado o *controle de acesso*, constituído pela seleção do *sujeito solicitante do acesso*, pelo sujeito se tratar de uma entidade tripla (brinquedo físico, dispositivo e serviço móvel), optou-se por representá-lo pelo serviço móvel, para melhorar o entendimento sobre quem solicita os dados; as *operações* e os *objetos* que o serviço móvel poderá executar e coletar respectivamente. No primeiro momento foram implementadas apenas as operações básicas de capturar (ler) e enviar (escrever), para facilitar o uso da ferramenta.

Os serviços móveis, geralmente, são sensíveis ao contexto, ou seja, necessitam da coleta de dados para fornecer serviços personalizados e relevantes com base nos dados de contexto. Para a implementação do protótipo, apresentaram-se três exemplos distintos de serviço móvel (figura 33) para a configuração do *controle de acesso*, no qual requisitam operações e objetos diferentes, simulando um brinquedo real que possui serviços e dispositivos diferentes em sua estrutura.

Figura 33 – Controle de acesso principal

The figure displays four sequential screenshots of a web form titled 'Criar nova regra' (Create new rule). Each screenshot shows the same form structure with the following fields and options:

- Nome da regra:** A text input field.
- Descrição da regra:** A text input field.
- Escolha o serviço móvel:** A dropdown menu with a question mark icon. The selected option varies across the screenshots:
  - Screenshot 1: 'Escolha...' (placeholder)
  - Screenshot 2: 'Serviço de localização'
  - Screenshot 3: 'Serviço de imagem'
  - Screenshot 4: 'Serviço de voz'
- Acesso o(s) objeto(s):** A section with checkboxes:
  - For 'Serviço de localização': 'Localizacao absoluta' and 'Localizacao relativa'.
  - For 'Serviço de imagem': 'Foto' and 'Video'.
  - For 'Serviço de voz': 'Audio'.
- Com as seguintes operações:** A section with checkboxes 'Capturar' and 'Enviar'.
- Progress indicator:** '1/4' is shown at the bottom of each form.
- Buttons:** 'CANCELAR' (white) and 'PRÓXIMO' (green) are at the bottom.

Fonte: Otávio de Paula Albuquerque, 2020.

O 2º passo é configurar o *controle de acesso estendido*, representado na figura 34. Na 1ª tela, são apresentadas duas entidades de privacidade para escolha. No *propósito*, pode ser selecionada uma ou um conjunto de propósitos no qual os sujeitos vinculados ao brinquedo poderão fazer uso dos dados coletados, caso escolhida a opção *qualquer um*, todas as opções serão selecionadas. No *destinatário*, onde são selecionados os sujeitos que irão ter permissão de acesso aos dados, podem ser: 1- individual, um usuário individual ou um serviço vinculado ao sistema do brinquedo; 2- grupo: um grupo de usuários (ex: brinquedos com função multi-jogador); 3- terceiros, serviço móvel que não está diretamente vinculado ao sistema do brinquedo, mas é restrito e responsabilizado pelo detentor dos objetos (sujeito), inclui serviços externos.

Na 2ª tela da figura 34 é apresentada a parte seguinte do *controle de acesso estendido*. São selecionadas então as *obrigações* e as *retenções*. As *obrigações* descrevem as regras e regulamentos que o sujeito concorda em cumprir após obter a permissão de acesso. Para o presente protótipo, foram utilizadas duas leis relacionadas à privacidade: Lei de proteção de informações pessoais e documentos eletrônicos (PIPEDA) e Lei de proteção à privacidade online das crianças (COPPA). A *Retenção* é o tempo no qual os dados ficarão retidos: 1- sem retenção, o objeto solicitado não é retido por mais de um breve período de tempo, ou seja, após o seu processamento será destruído sem armazenamento; 2- propósito definido, o objeto solicitado é retido pelo tempo necessário para atender a finalidade declarada no *propósito* e será descartado assim que finalizado; 3- requisito legal, o objeto solicitado é retido para atender a um objetivo declarado (conforme exigido por lei ou responsabilidade de acordo com a lei aplicável); 4- práticas de negócio, o objeto solicitado é retido de acordo

com as práticas comerciais declaradas nos termos de serviço; 5- indefinidamente, o objeto solicitado é retido por um período indeterminado de tempo; 6- personalizado, retido pelo tempo determinado pelo usuário, usado para criar um prazo de validade para a regra (tela 3 da figura 34), que é por si só uma funcionalidade.

Figura 34 – Controle de acesso estendido

The figure displays three panels of a privacy rule configuration interface, each with a progress indicator (2/4, 3/4, 3/4) and navigation buttons (VOLTAR, PRÓXIMO).

Panel 1 (2/4):

- Propósitos ?**
  - ☐ Jogos
  - ☐ Pessoal
  - ☐ Marketing
  - ☐ Administrativo
  - ☐ Pesquisa
  - ☐ Qualquer um
- Destinatários ?**
  - ☐ Individual
  - ☐ Grupo
  - ☐ Terceiro
  - ☐ Qualquer um

Panel 2 (3/4):

- Obrigações ?**
  - ☐ PIPEDA ☐ COPPA
- Retenção ?**
  - ☐ Sem retenção
  - ☐ Propósito definido
  - ☐ Requisito legal
  - ☐ Práticas de negócio
  - ☐ Indefinido
  - ☐ Personalizado

Panel 3 (3/4):

- Obrigações ?**
  - ☐ PIPEDA ☐ COPPA
- Retenção ?**
  - ☐ Sem retenção
  - ☐ Propósito definido
  - ☐ Requisito legal
  - ☐ Práticas de negócio
  - ☐ Indefinido
  - ☒ Personalizado
- 1 ▼ dia(s) ▼

Fonte: Otávio de Paula Albuquerque, 2020.

Como último passo para a criação da regra de privacidade, é exibida aos pais ou responsáveis legais a descrição da regra, apresentando todos os dados selecionados no decorrer do processo de criação da regra para a revisão (figura 35). Caso os dados estiverem de acordo com as escolhas, a confirmação da criação da regra deverá ser realizada. Após a confirmação, o protótipo retorna para a tela *gerenciar regras* com a regra já listada em sua tabela de *regras de privacidade*.

Figura 35 – Revisão e confirmação da criação da regra de privacidade

Revisar e adicionar regra

Você está criando a regra de privacidade REGRA 1. Por favor, revise cuidadosamente todos os dados informados:

A regra de privacidade REGRA 1 permitirá que o serviço móvel SERVIÇO DE LOCALIZAÇÃO realize a(s) operação(ões) LER no(s) objeto(s) LOCALIZACAO ABSOLUTA, com o(s) propósito(s) de uso JOGOS, podendo ser compartilhado(s) de forma GRUPO, precisando cumprir as obrigações definidas em PIPEDA, e retidas pelo tempo PROPÓSITO DEFINIDO.

4/4

VOLTAR **FINALIZAR**

Fonte: Otávio de Paula Albuquerque, 2020.

Para o auxílio na criação da regra de privacidade, foram implementados botões de ajuda, representados pelo ponto de exclamação, apresentados nas figuras 36, 37 e 38, no qual foram inseridas caixas de diálogos com textos instrutivos, com o intuito de instruir, tirar dúvidas e esclarecer as informações referente as etapas e escolhas da funcionalidade. Todas às etapas da criação de regras de privacidade usaram esse mecanismo de apoio, explicando os passos e opções a serem definidas no processo de criação da regra.

Figura 36 – Caixa de diálogo de ajuda nas telas de controle de acesso principal

Criar nova regra

Nome da regra: _____

Descrição da regra: _____

Controle de acesso

Por exemplo, para uma regra em que "o sujeito A pode capturar o arquivo B", então, o "sujeito A" é o "serviço móvel", o "arquivo B" é o "objeto", e "Capturar" é a "operação".

FECHAR

1/4 **CANCELAR** **PRÓXIMO**

Criar nova regra

Nome da regra: _____

Serviço móvel do sistema de brinquedo

Serviço móvel é um serviço disponibilizado pelo brinquedo para proporcionar a execução de parte de suas funcionalidades.

Cada serviço móvel precisa acessar diferentes tipos de objetos de dados para seu funcionamento.

FECHAR

1/4 **CANCELAR** **PRÓXIMO**

Criar nova regra

Nome da regra: _____

Objetos

Os objetos representam os tipos os dados provenientes do uso do brinquedo, capturados ou gerados e armazenados por dispositivos do brinquedo.

Importante: negar a permissão de coleta ou uso de determinados objetos de dados pode interferir diretamente na experiência da criança com o uso do brinquedo.

Para mais informações, acesse: "Área dos pais > Restrições de uso"

FECHAR

1/4 **CANCELAR** **PRÓXIMO**

Criar nova regra

Nome da regra: _____

Operações

As operações são ações que os serviços móveis podem executar sobre objetos de dados, conforme abaixo:

Capturar: permite que o objeto seja lido, ou seja, que dados sejam capturados (por exemplo, que áudio seja capturado de um microfone, que uma foto seja capturada de uma câmera, que uma posição de geolocalização seja capturada de um GPS etc.).

Enviar: permite que dados sejam escritos no objeto, ou seja, que dados sejam enviados (por exemplo, que áudio seja enviado para um auto-falante, que vídeo seja enviado para uma tela etc.).

FECHAR

1/4 **CANCELAR** **PRÓXIMO**

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 37 – Caixa de diálogo de ajuda nas telas de controle de acesso estendido para propósito e destinatário

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 38 – Caixa de diálogo de ajuda nas telas de controle de acesso estendido para obrigação e retenção

Fonte: Otávio de Paula Albuquerque, 2020.

Caso seja escolhida para a criação da regra de privacidade, usar os modelos de regra predefinidos; é selecionada a opção *baseado em modelo* da figura 39. A funcionalidade dá a possibilidade de selecionar e usar uma regra de privacidade fornecida pela própria ferramenta, onde são apresentadas a sua descrição e utilidade para a proteção da privacidade. Os pais então podem selecionar, caso a regra esteja de acordo com o seu desejo, e habilitar

a regra no seu painel de regra de privacidade. A ferramenta também possibilita a procura por regras de privacidade externas à ferramenta, habilitando anexar arquivos com extensão XML que contenham regras de privacidade.

Figura 39 – Tela de modelos de regra de privacidade

Fonte: Otávio de Paula Albuquerque, 2020.

6.5 Considerações finais

Para a criação de uma navegabilidade que fizesse sentido e não atrapalhasse a experiência de quem fosse usar o protótipo, foram inseridos os botões/opções relacionados aos requisitos não implementados, os quais ao serem selecionados seguiam para uma interface que apresentava a descrição de sua funcionalidade, com o intuito de deixar o usuário ciente do que deveria ter lá, apesar de não implementado.

O objetivo da construção do protótipo, foi estabelecer uma visão computacional do modelo de ferramenta de controle parental criado neste trabalho, servindo como artefato para auxiliar a avaliação da importância dos requisitos funcionais, bem como avaliar a satisfação da implementação dos requisitos; confirmando a importância dos requisitos funcionais para um ferramenta de controle parental para brinquedos inteligentes.

7 Avaliação dos requisitos e do protótipo da ferramenta

Neste capítulo são apresentados os procedimentos realizados para coleta e análise dos dados das avaliações deste projeto. Inicialmente, apresentam-se as etapas da coleta de dados por meio das avaliações, tanto dos requisitos levantados como do artefato (protótipo); posteriormente, são revelados os resultados por meio da exposição das análises e discussões.

7.1 *Escopo da avaliação*

A abordagem qualitativa e quantitativa apresentada para a coleta e análise deste trabalho findou para o uso do Questionário como instrumento para a coleta de dados. Optou-se pelo questionário, por se tratar de um instrumento de fácil envio e acesso via internet, e que por isso abrange ampla distância territorial (PERKINS, 2004). Possibilitar o sujeito respondente escolher o local e a hora mais adequados para contribuir, tendo em vista que o questionário pode demandar tempo face à necessidade de instalar e usar o protótipo de ferramenta como uma de suas etapas pode ser relevante para a qualidade das respostas.

O questionário usado foi do tipo estruturado, com perguntas objetivas fechadas e apenas uma pergunta aberta subjetiva, a fim de realizar duas avaliações relacionadas aos requisitos levantados deste trabalho. Os objetivos das avaliações foram: verificar se os requisitos funcionais e não funcionais identificados são importantes para o desenvolvimento de uma ferramenta de controle parental para brinquedos inteligentes, visando apresentar o grau de relevância de cada um dos requisitos do conjunto levantado, sejam eles funcionais ou não-funcionais; e se os requisitos funcionais estão bem implementados nas funcionalidades do protótipo, analisando o grau de representatividade/satisfação da implementação. Usou-se a escala de likert para categorização das respostas, mensurando o grau de concordância com as perguntas, aplicando uma escala com 5 pontos.

Como sujeitos da avaliação, escolheram-se pesquisadores de universidades brasileiras especialistas na área de brinquedos inteligentes. Que foram compostos por graduandos, pós-graduandos e professores que produziram ou produzem trabalhos na área, e que convenientemente conhecem a fundo os temas mais discutidos da área, como privacidade e segurança.

7.2 Planejamento de avaliação

Este trabalho tem como objetivo principal, apresentar um conjunto de requisitos, funcionais e não-funcionais, importantes para uma ferramenta de controle parental, para brinquedos inteligentes, e para isso, precisou avaliar esses requisitos presentes nesse conjunto, além de avaliar também o protótipo computacional desenvolvido. Os requisitos levantados foram avaliados quanto à sua relevância para a construção da ferramenta, e assim determinar quão útil para os pais/responsáveis legais tais requisitos são; já o protótipo foi avaliado com relação à sua implementação e quão satisfatório os requisitos estão representados em suas funcionalidades.

Para a coleta de dados das avaliações, foi aplicado um questionário estruturado, no qual foram criadas duas perguntas objetivas; uma pergunta satisfazia a 1ª avaliação que se pretendeu realizar: *qual a importância desse requisito para uma ferramenta de controle parental?*; todos os requisitos, funcionais e não funcionais, foram avaliados nesse quesito. A 2ª avaliação corresponde apenas aos requisitos funcionais implementados no protótipo: *o quão satisfatório esse requisito está implementado no protótipo avaliado?*.

O questionário foi composto por 7 seções (apêndice A): na 1ª seção, introduz-se o trabalho e descrevem-se as avaliações que serão realizadas; a 2ª seção descreve alguns conceitos importantes para o direcionamento do tema do questionário, além de apresentar as etapas para instalação e uso do protótipo da ferramenta, que será necessário para responder as questões posteriormente; na 3ª estabeleceu-se um exemplo de regra de privacidade para criação no protótipo, com o intuito de certificar se houve o entendimento sobre a funcionalidade da criação de regras de privacidade; a 4ª seção definiu algumas variáveis independentes relacionadas ao grau de escolaridade e conhecimento sobre brinquedos inteligentes; na 5ª seção, são avaliados os requisitos funcionais. 19 perguntas relacionadas ao grau de importância dos requisitos para uma ferramenta de controle parental, e 13 perguntas relacionadas ao grau de satisfação da implementação dos requisitos no protótipo são realizadas; na 6ª etapa são avaliados os requisitos não-funcionais e o seu grau de importância para uma ferramenta de controle parental; como última etapa há uma caixa de diálogo livre para a descrição de sugestões.

As 50 perguntas feitas nesse questionário, seguiram a escala de likert de 5 pontos. Para a 1ª avaliação foram mensurados os graus de importância dos requisitos, no qual as

alternativas variavam de: 1-pouco importante à 5-muito importante; para a 2ª avaliação de: 1-pouco satisfatório para 5-muito satisfatório. Vale ressaltar que a definição da escala começa do “pouco importante” e não do “nada importante” foi estabelecida em vista de o levantamento dos requisitos ter ocorrido por meio de suas identificações em artigos de conferência, revistas ou leis de privacidade estabelecidas no meio jurídico, ou seja, os requisitos já eram considerados importantes desde o seu levantamento.

As características que se pretendeu observar nesse questionário são as variáveis dependentes e independentes. As questões das avaliações serviram pra medir as variáveis: dependentes, importância dos requisitos funcionais e não-funcionais para ferramenta de controle parental, e a satisfação da implementação dos requisitos funcionais no protótipo; e as independentes, dados iniciais que comprovam o conhecimento dos sujeitos avaliadores sobre a área de brinquedos inteligentes; nos quais eram: grau de escolaridade e o quanto o indivíduo considerava conhecer sobre brinquedos inteligentes.

7.3 Execução da avaliação

O questionário foi aplicado no mês de janeiro de 2020, por meio da criação de um formulário online enviado por e-mail para uma determinada lista de indivíduos (sujeitos especialistas na área de brinquedos inteligentes). Para a avaliação, junto ao questionário foi disponibilizado o link do protótipo da ferramenta para *download*, tendo em vista que o seu uso era obrigatório como sendo uma das etapas para o andamento da avaliação. Além do uso do protótipo, as questões referentes aos requisitos, tanto funcionais como não-funcionais, eram acompanhadas de suas descrições, para apoio na avaliação da importância.

No total, foram coletadas 10 avaliações de pesquisadores especialistas na área de brinquedos inteligentes no Brasil. Considerando a quantidade de pesquisadores brasileiros da área, o número de amostras foi julgado satisfatório, tendo em vista também a profundidade de tais avaliações face ao conhecimento dos avaliadores.

7.4 Resultados e discussões

Nesta seção são apresentados os resultados obtidos da coleta de dados das avaliações através do questionário. Afirmando a abordagem mista deste trabalho, análises descritivas e inferenciais dos resultados, além de análises qualitativas foram realizadas.

7.4.1 Análises quantitativa

Com os resultados das 10 aplicações do questionário coletadas, pode-se analisar as avaliações, tanto das variáveis independentes quanto das dependentes. Para os resultados principais, dividiram-se as análises das avaliações dos dados referentes às questões relacionadas à importância do requisito, e das questões relacionadas à satisfação da implementação.

Os primeiros resultados analisados estão relacionados às variáveis independentes do questionário: o nível de escolaridade, e o grau de conhecimento sobre brinquedos inteligentes. Estes dados foram importantes para apoiar e confirmar a escolha do sujeito avaliador, que foram pesquisadores especialistas na área de estudo, com trabalhos publicados.

Como pode ser observado na figura 40, a maioria dos respondentes são doutorandos ou doutores (professores), o que geralmente indica maior experiência sobre pesquisa científica, e conseqüentemente mais conhecimento sobre o determinado foco de pesquisa.

Figura 40 – Nível de escolaridade

Fonte: Otávio de Paula Albuquerque, 2020.

A figura 41 representa o grau de conhecimento dos avaliadores, relacionados à área de brinquedos inteligentes. Considerando que os avaliadores foram selecionados pessoalmente, ou seja, eram conhecidos por trabalhos realizados na área, se esperava que o resultado indicasse um elevado grau de conhecimento.

Figura 41 – Grau de conhecimento sobre brinquedos inteligentes

Fonte: Otávio de Paula Albuquerque, 2020.

A relação entre o nível de escolaridade e o grau de conhecimento sobre a área não é diretamente proporcional, por exemplo, o indivíduo avaliador que indicou ter graduação completa informou ter mais conhecimento na área que um dos indivíduos doutores.

Com relação a análise dos dados das variáveis dependentes, que era o objetivo principal do questionário, os resultados foram divididos em 3 partes para apresentação. A 1ª parte está relacionada ao grau de importância dos requisitos funcionais para uma ferramenta de brinquedo inteligente; a 2ª parte também está relacionada à importância dos requisitos para a ferramenta, no entanto, se refere aos requisitos não-funcionais de usabilidade, interoperabilidade, implementação, segurança e legais respectivamente; 3ª e última parte, estão os resultados relacionados ao uso do protótipo e da avaliação do quão satisfatório os requisitos funcionais estão implementados nele.

A figura 42 representa a 1ª parte dos resultados; a avaliação dos requisitos funcionais relativos a suas respectivas importâncias para a ferramenta. A importância dos requisitos funcionais para os avaliadores foi considerada alta, representadas pelas notas 4 e 5, as quais foram as notas mais frequentes nas avaliações. Dentre os requisitos, vale destacar positivamente, *apresentar a política de privacidade da empresa e monitorar e alertar sobre assuntos suspeitos mencionados pela criança* que obtiveram avaliação máxima unânime entre os pesquisadores.

Esperava-se que o requisito de *apresentar a política de privacidade da empresa* fosse considerado muito importante por causa do seu destaque na literatura, como mostrado na figura 13, representado pelos riscos de *abertura, transparência e notificação*. Esse requisito visa facilitar o acesso à política de privacidade do brinquedo, assim como tornar os textos da política claros e concisos, melhorando o entendimento dos pais sobre os assuntos contidos nela, o que torna o requisito imprescindível para uma ferramenta de controle parental.

Monitorar e alertar sobre assuntos suspeitos mencionados pela criança pode ser considerado um dos requisitos que se faz necessário na atualidade dos brinquedos conectados à internet. Justificando a importância dos requisitos complementares, não se atendo apenas à preservação da privacidade, mas considerando contribuir também na proteção física e psicológica da criança.

Entre as menores médias dos requisitos funcionais apresentadas na figura 43, ressalta-se as dos requisitos, *definir data de validade de regra de privacidade* (F08), *disponibilizar links úteis para os pais* (F012) e *disponibilizar acesso a "Dúvidas Comuns"(FAQ)* (F15), com as menores médias. Os requisitos F12 e F15 podem ter sido considerados menos importantes por causa de suas funcionalidades estáticas, comumente usados em *web sites*.

Figura 42 – Grau de importância dos requisitos funcionais

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 43 – Média das avaliações do grau de importância dos requisitos funcionais

Fonte: Otávio de Paula Albuquerque, 2020.

Para a 2ª parte dos resultados, as avaliações dos requisitos não-funcionais (figura 44 e 45) foram ainda mais positivas. As avaliações consideram os requisitos de usabilidade *fácil instalação e fácil uso* muito importantes para a ferramenta. Isso se deve ao fato de que os pais têm, geralmente, pouco entendimento sobre o uso de *smartphones*; portanto, há a necessidade de as ferramentas de controle parental disporem de um ambiente amigável, intuitivo, propício para o uso.

Os requisitos de segurança *autenticar e autorizar comunicações* e *criptografar comunicação* também foram considerados muito importantes, por se tratar de requisitos que visam proteger o transporte dos dados entre a ferramenta de controle parental e o ambiente de computação para brinquedos. Esses requisitos propõem mitigar riscos graves como violação e vazamento de dados, que podem ocorrer quando o dado está em transferência. Outro requisito de segurança com avaliação máxima foi *seguir boas práticas de segurança de software*, considerado um requisito padrão, mas que geralmente é negligenciado pelos desenvolvedores.

Como último requisito não-funcional avaliado como muito importante por todos os avaliadores, está o requisito de implementação: *implementar seguindo o "Privacy by Design"*, concluindo que uma ferramenta de preservação da privacidade necessita planejar técnicas que atendam aos requisitos de privacidade e regulamentos, desde sua implementação.

Figura 44 – Grau de importância dos requisitos não-funcionais

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 45 – Média das avaliações do grau de importância dos requisitos não-funcionais

Fonte: Otávio de Paula Albuquerque, 2020.

A 3ª parte, trata da avaliação do protótipo de ferramenta de controle parental, ou seja, do quão satisfatório os requisitos funcionais estão implementados na ferramenta (figuras 46 e 47). Dos 19 requisitos funcionais apresentados para compor a 1ª avaliação, 13 foram implementados e usados para a 2ª.

As avaliações que menos variaram e receberam maiores médias foram sobre os requisitos *consultar descrição de regra de privacidade*, *disponibilizar links úteis para os pais* (F012) e *disponibilizar acesso a "Dúvidas Comuns" (FAQ)* (F15). Pode-se afirmar que o motivo das altas médias de satisfação foi o mesmo pelos quais os requisitos F012 e F015 foram avaliados com as menores médias de importância (é necessário ter em mente que isso não quer dizer que tais requisitos são pouco importantes, mas sim menos importantes que os outros), por se tratar de funcionalidades estáticas simples, já estabelecidas no meio computacional, e consequentemente fáceis de implementar.

Quando se considera o oposto, o requisito que mais obteve avaliações notas 1, foi *definir data de validade de regra de privacidade* (F08). O requisito foi implementado como uma opção incorporada na etapa de seleção da retenção, na funcionalidade *criação de regras de privacidade*, na qual é a entidade que determina a quantidade de tempo que o dado será coletado. Essa escolha de implementação pode ter dificultado a identificação do requisito na funcionalidade, deixando-o pouco visível.

Figura 46 – Grau de satisfação da implementação dos requisitos funcionais no protótipo

Fonte: Otávio de Paula Albuquerque, 2020.

Figura 47 – Média das avaliações do grau de satisfação da implementação do protótipo

Fonte: Otávio de Paula Albuquerque, 2020.

Cruzando a análise dos dados entre os graus de importância e satisfação, observa-se que o requisito funcional que apresentou menor média de satisfação de implementação dentre todos os requisitos, *notificar mudanças na política de privacidade da empresa* (F03), foi uma das maiores médias de importância. Por se tratar de um requisito comumente utilizado em redes sociais como Facebook, LinkedIn, Twitter etc., estabeleceu-se uma estrutura predefinida, na qual as notificações têm sua interface isolada das demais, específica para receber aviso de atualizações na rede. Na implementação da funcionalidade de notificação do protótipo, os pais precisarão visitar frequentemente a aba do menu principal *área de suporte* para verificar se há novas notificações, além do que a notificação é apenas uma das

funcionalidades dessa aba do menu, o que pode explicar as proporções inversas nas médias das avaliações de importância e satisfação.

Outro requisito que obteve média alta no grau de importância e baixa no grau de satisfação da implementação foi *remover dados sensíveis e/ou PII*. As avaliações do requisito podem ser explicadas devido alguns avaliadores não concordarem com a maneira como seria executada a funcionalidade, o que será abordado, em seguida, na análise qualitativa dos dados.

7.4.2 Análise qualitativa

A análise qualitativa dos dados foi realizada por meio da análise de conteúdo das respostas provenientes da questão subjetiva do questionário (apêndice B), no qual visava coletar sugestões de ideias de novos requisitos e recomendações para melhoria do protótipo.

A maioria das sugestões foi de caráter recomendatório, relacionadas a melhorias do protótipo. Em grande parte as recomendações foram referentes a usabilidade da ferramenta, levando em consideração a importância da implementação de um ambiente amigável, intuitivo, que os usuários se sintam à vontade para usar.

Incluíram-se nas respostas, sugestões como a obrigatoriedade de confirmação e consentimento para a conclusão de uma operação, adequação textual para uma linguagem mais acessível, tratamento de exceções (por exemplo, "campos obrigatórios") para respostas a interações do usuário etc. Apesar de o protótipo não ter levado em consideração a usabilidade da ferramenta na sua implementação, as recomendações foram consideradas pertinentes para a realização de trabalhos futuros no protótipo, no qual serão considerados os requisitos não-funcionais, incluindo a usabilidade.

A recomendação que mais obteve menções está relacionada à conscientização sobre a manipulação de dados e o funcionamento do ambiente de computação para brinquedos. O aperfeiçoamento do texto da política de privacidade foi a sugestão mais difundida entre os avaliadores, por causa da importância da conscientização dos pais, principalmente sobre como ocorrerá a coleta, o uso e o compartilhamento de dados da criança usuária do brinquedo. É necessário que a ferramenta de controle parental tenha mecanismos para aperfeiçoar a leitura e compreensão do texto da política de privacidade, evitando informações em excesso, seccionando os pontos chave e garantindo que a leitura seja

realizada por completo, por exemplo, por meio da habilitação do consentimento (li e concordo) somente após o pai chegar no fim do texto.

Sugestões que reuniram mais de uma menção que valem ressaltar por sua importância, estão relacionadas ao aprendizado dos pais quanto ao uso correto da ferramenta para a criação de regras de privacidade, funcionalidade principal da ferramenta. Identificou-se a necessidade de criar um tutorial para a criação da primeira regra de privacidade, exibindo e explicando, controladamente, o passo a passo da funcionalidade, seguindo o fluxo de atividade definido no planejamento para a criação da regra, do seu início até sua conclusão.

Relacionando-se ainda com a criação de regras de privacidade, recomendou-se que a ferramenta use os modelos predefinidos de regras de privacidade como opção padrão de criação de regra, por se tratar da opção mais prática de uso para os pais. Para auxiliar na decisão de escolha entre os modelos de regra, além de apresentar na janela de seleção uma descrição de suas funcionalidades e finalidades, listá-los por relevância, tomando como parâmetro a quantidade de usuários que as ativaram nos seus dispositivos.

Outra modalidade de sugestões foram as novas ideias de requisitos funcionais, não levantados por este trabalho, para uma ferramenta de controle parental. Entre as ideias, foram sugeridas algumas consideradas genéricas, como o caso do cadastro de PIN para acesso à ferramenta, que equivaleria a um módulo de login comum, usado em praticamente todos os aplicativos. Apesar da relevância para a ferramenta, esse tipo de requisito genérico foi descartado da primeira versão do protótipo por não tratar detalhes específicos para o contexto do controle parental para brinquedos inteligentes. Ideias incrementais aos requisitos já existentes também foram sugeridas, como a autenticação de identidade do responsável por fotos e documentos, na qual é um exemplo de mecanismo de verificação abordado pelo requisito *garantir autenticidade de acesso* (F06).

As novas ideias sugeridas que foram específicas para brinquedos inteligentes se assemelharam aos requisitos relacionados ao monitoramento dos pais e funcionalidades de apoio à tomada de decisão. Por exemplo, o requisito de *alerta de tempo de uso do brinquedo pela criança*, que tem como intuito auxiliar os pais no controle do uso do brinquedo. Esse requisito pode ser facilmente vinculado ao requisito *manter histórico de atividades da criança* identificado por este trabalho, no qual já disponibiliza um histórico de atividades realizadas pela criança com o brinquedo, registrando a data e o tempo da atividade. O requisito sugerido *criar histórico de dispositivos negados pela regra* remete ao requisito

já levantado informar sobre consequências da criação de regras de privacidade, no qual seriam adicionados os serviços móveis que tiverem o seu acesso negado após a criação da regra, permitindo os pais de terem melhor noção de quais serviços são mais invasivos.

7.5 *Considerações finais*

Ao final da análise dos resultados, verificou-se que o conjunto de requisitos funcionais e não-funcionais foram considerados importantes para o desenvolvimento de uma ferramenta de controle parental para brinquedos inteligentes. A aprovação das avaliações sobre a relevância da escolha da técnica de criação de regras de privacidade como a funcionalidade principal, bem como das funcionalidades complementares, reitera a significativa contribuição deste trabalho para o estabelecimento de uma proposta de ferramenta de controle parental padrão para brinquedos inteligentes, que sirva de referência para o desenvolvimento de ferramentas de controle parental por empresas de brinquedo, além do apoio à pesquisa na área de brinquedos inteligentes relacionado à privacidade.

A avaliação do protótipo também mostrou-se positiva, tendo em vista as suas satisfatórias médias, considerando que apesar de ser um protótipo da ferramenta no qual não houve a necessidade de aprofundar a implementação, o seu propósito de avaliar os requisitos implementados foi alcançado, colaborando para a definição de uma visão geral da ferramenta, além da sugestão de um fluxo de atividades e navegabilidade.

8 Conclusão

O mercado de brinquedos inteligentes ainda é considerado um mercado novo, porém, sua perspectiva de crescimento é enorme. Juniper Research (2017) estipula que o mercado crescerá para US\$ 11,3 bilhões até final de 2020, levantando assim indagações de pesquisadores e pais a respeito dos riscos relacionados a essa área, tendo em vista a alta expectativa de crescimento, e o pouco que está sendo feito com relação a segurança e privacidade para a área, ainda sendo considerada um tópico de pesquisa emergente e que precisa ser urgentemente explorado (HUNG *et al.*, 2016).

Brinquedos inteligentes são brinquedos físicos que integram, em sua estrutura, dispositivos móveis que se conectam à internet e coletam dado a fim de disponibilizar funcionalidades. A tendência é que tais brinquedos incorporem mais funcionalidades e consequentemente mais dispositivos, piorando o cenário de riscos à privacidade e segurança envolvidos no ambiente. Com isso, mecanismos que auxiliem os pais na proteção dos seus filhos fazem-se necessários, como o caso de ferramentas de controle acesso, que permite aos pais decidirem de acordo com suas preferências como o acesso aos dados ocorrerá. No entanto, não existe uma ferramenta de controle de acesso parental específica para o ambiente de computação para brinquedos. As existentes são adaptadas de ferramentas tradicionais, o que não satisfaz mais a necessidade dos pais para o novo contexto tecnológico atual.

Considerando tais circunstâncias, este trabalho levantou um conjunto de requisitos funcionais e não-funcionais importantes para o ambiente de computação para brinquedos, pretendendo disponibilizar um modelo de ferramenta de controle parental padronizado para ser usado como base para o desenvolvimento de ferramentas por empresas de brinquedos.

Para alcançar o objetivo geral, os requisitos foram postos à avaliação, para confirmar sua importância para a ferramenta, além da avaliação realizada no protótipo para avaliar a satisfação da sua implementação. Para as avaliações, foi criado um questionário online, aplicado para pesquisadores brasileiros especialistas em brinquedos inteligentes, visando responder sobre a importância dos requisitos e a satisfação da implementação do protótipo.

Os resultados das avaliações foram analisados, e concluiu-se que os requisitos levantados, de fato, são importantes para o desenvolvimento de uma ferramenta de controle parental. Tal conjunto de requisitos pode ser usado para que empresas de brinquedo

possam se basear para a implementação de suas ferramentas. O protótipo da ferramenta desenvolvido neste trabalho auxilia indicando fluxos de atividades e navegabilidade.

Pretende-se com este projeto, disponibilizar um modelo de ferramenta de controle parental para que empresas de brinquedos inteligentes usem como base para desenvolver suas próprias ferramentas; além de contribuir para o avanço na pesquisa da área de brinquedos inteligentes, relacionados, principalmente, a temas de privacidade e segurança.

8.1 Limitações

Por se tratar de um protótipo da ferramenta de controle parental, não houve uma implementação profunda, não sendo implementados alguns requisitos funcionais, e nenhum dos requisitos não-funcionais, o que pode ter interferido nas avaliações realizadas neste trabalho.

A amostragem da avaliação de 10 pesquisadores especialistas é pequena para alcançar a generalização. O uso do questionário como instrumento de coleta de dados pode ter sido uma das respostas para o pouco número de avaliações. Usar outro tipo de instrumento como grupos focais, realizados com pais de crianças até 13 anos, para avaliação, poderia ter fornecido resultados adicionais para a análise.

8.2 Trabalhos futuros

Como trabalho futuro, pretende-se melhorar a implementação do protótipo, adicionando os requisitos funcionais faltantes e os requisitos não-funcionais. Submeter o protótipo por avaliações e testes de usabilidade e comunicabilidade.

O protótipo e o questionário serão aplicados para pesquisadores especialistas estrangeiros, buscando aumentar a amostragem das avaliações e verificar se há diferentes percepções de importância e satisfação entre pesquisadores de países diferentes. Usar outros instrumentos de coleta de dados, como grupos focais, usando pais como sujeitos avaliadores.

Validar o modelo conceitual Rafferty de regras de privacidade para brinquedos inteligentes no ambiente computacional real. Implementar o processo de comunicação referente à criação de regras de privacidade.

Referências¹

- ABOWD, G. D.; DEY, A. K.; BROWN, P. J.; DAVIES, N.; SMITH, M.; STEGGLES, P. Towards a better understanding of context and context-awareness. In: SPRINGER. *International symposium on handheld and ubiquitous computing*. [S.l.], 1999. p. 304–307. Citado na página 31.
- ALBUQUERQUE, O. de P.; FANTINATO, M.; KELNER, J.; ALBUQUERQUE, A. P. de. Privacy in smart toys: Risks and proposed solutions. *Electronic Commerce Research and Applications*, Elsevier, 2019. Citado 10 vezes nas páginas 25, 32, 45, 46, 54, 55, 57, 58, 60 e 61.
- AMANCIO, F. M. P. *Percepção sobre segurança e privacidade infantil em relação a brinquedos inteligentes: um estudo comparativo entre países de diferentes níveis de desenvolvimento*. Dissertação (Mestrado) — Universidade de São Paulo, 2018. Citado na página 28.
- AVIZIENIS, A.; LAPRIE, J.-C.; RANDELL, B.; LANDWEHR, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, IEEE, v. 1, n. 1, p. 11–33, 2004. Citado na página 32.
- BERTINO, E.; FERRARI, E.; PEREGO, A. A general framework for web content filtering. *World Wide Web*, v. 13, n. 3, p. 215–249, 2010. Citado 4 vezes nas páginas 74, 76, 77 e 78.
- BRYMAN, A. *Social Research Methods*. 4. ed. Oxford, UK: Oxford University Press, 2012. Citado na página 50.
- CAMARATA, K.; GROSS, M. D.; DO, E. Y.-L. A physical computing studio: Exploring computational artifacts and environments. *International Journal of Architectural Computing*, SAGE Publications Sage UK: London, England, v. 1, n. 2, p. 169–190, 2003. Citado na página 36.
- Canada. *PIPEDA – Personal Information Protection and Electronic Documents Act*. 2018. Minister of Justice, Canada, <https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf>. Citado 2 vezes nas páginas 74 e 78.
- CARVALHO, L. G.; ELER, M. M. Security requirements for smart toys. In: *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS)*. [S.l.]: SciTePress, 2017. p. 144–154. Citado 6 vezes nas páginas 18, 54, 65, 73, 77 e 78.
- CARVALHO, L. G.; ELER, M. M. Security requirements and tests for smart toys. In: *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS)*. [S.l.]: Springer Verlag, 2018. p. 291–312. Citado 5 vezes nas páginas 54, 65, 73, 77 e 78.
- CARVALHO, L. G.; ELER, M. M. Security tests for smart toys. In: *Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS)*. [S.l.]: SciTePress, 2018. p. 111–120. Citado 5 vezes nas páginas 54, 65, 73, 77 e 78.

¹ De acordo com a Associação Brasileira de Normas Técnicas. NBR 6023.

CHAKRABORTY, S.; RAGHAVAN, K. R.; JOHNSON, M. P.; SRIVASTAVA, M. B. A framework for context-aware privacy of sensor data on mobile systems. In: *ACM. Proceedings of the 14th Workshop on Mobile Computing Systems and Applications*. [S.l.], 2013. p. 11. Citado na página 31.

CHOWDHURY, W. Toys that talk to strangers: A look at the privacy policies of connected toys. In: *Proceedings of the Conference of Future Technologies Conference (FTC)*. [S.l.]: Springer Verlag, 2018. p. 152–158. Citado 2 vezes nas páginas 54 e 65.

CHU, G.; APTHORPE, N.; FEAMSTER, N. Security and privacy analyses of internet of things children's toys. *IEEE Internet of Things Journal*, v. 6, n. 1, p. 978–985, 2019. Citado 4 vezes nas páginas 22, 54, 63 e 66.

CogniToy Dino. *Meet the CogniToys Dino*. 2016. Acesso em: 23/05/2018. Disponível em: <https://www.cognitoys.com/>. Citado 2 vezes nas páginas 29 e 30.

DEMETZOU, K.; BÖCK, L.; HANTEER, O. Smart bears don't talk to strangers: Analysing privacy concerns and technical solutions in smart toys for children. In: *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*. [S.l.]: IET, 2018. p. 1–7. Citado 3 vezes nas páginas 54, 65 e 66.

DENNING, T.; MATUSZEK, C.; KOSCHER, K.; SMITH, J. R.; KOHNO, T. A spotlight on security and privacy risks with future household robots: attacks and lessons. In: *Proceedings of the 11th International Conference on Ubiquitous Computing (UbiComp)*. [S.l.]: ACM, 2009. p. 105–114. Citado 2 vezes nas páginas 54 e 65.

ELSEVIER. Scopus - content coverage guide. *Elsevier B.V. Amsterdam, The Netherlands*, 2017. Disponível em: https://www.elsevier.com/_data/assets/pdf_file/0007/69451/0597-Scopus-Content-Coverage-Guide-US-LETTER-v4-HI-singles-no-ticks.pdf. Citado na página 48.

ESPINOSA-ARANDA, J. L.; VALLEZ, N.; RICO-SAAVEDRA, J. M.; PARRA-PATINO, J.; BUENO, G.; SORCI, M.; MOLONEY, D.; PENA, D.; DENIZ, O. Smart doll: Emotion recognition using embedded deep learning. *Symmetry*, v. 10, n. 9, p. 1–18, 2018. Citado 2 vezes nas páginas 54 e 65.

Estatuto da Criança e do Adolescente do Brasil. *Lei nº8.069/90, Art.2º*. 1990. Acesso em: 27/08/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Citado na página 33.

EU. *GDPR – General Data Protection Regulation*. 2016. Eur. Parliament and Council of the Eur. Union, <https://eugdpr.org>. Citado 3 vezes nas páginas 76, 78 e 84.

European Commission. *Benchmarking of parental control tools for the online protection of children*. 2017. <https://sipbench.eu>. Citado 5 vezes nas páginas 22, 70, 74, 75 e 76.

European Union Safer Internet Program. *Benchmarking of Parental Control Tools for the Onlin Protection of Children*. 2012. Acesso em: 23/05/2018. Disponível em: <http://sipbench.eu/transfer/SIPBENCHII5thcycleExecutivesummary.pdf>. Citado na página 40.

FANTINATO, M.; HUNG, P. C.; JIANG, Y.; ROA, J.; VILLARREAL, P.; MELAIS, M.; AMANCIO, F. A preliminary study of hello barbie in brazil and argentina. *Sustainable cities and society*, Elsevier, v. 40, p. 83–90, 2018. Citado na página 17.

FANTINATO, M.; HUNG, P. C. K.; JIANG, Y.; ROA, J.; VILLARREAL, P.; MELAIS, M.; AMANCIO, F. A preliminary study of hello barbie in Brazil and Argentina. *Sustainable Cities and Society*, v. 40, p. 83–90, 2018. Citado 6 vezes nas páginas 19, 54, 65, 66, 74 e 75.

FELT, A. P.; HA, E.; EGELMAN, S.; HANEY, A.; CHIN, E.; WAGNER, D. Android permissions: User attention, comprehension, and behavior. In: ACM. *Proceedings of the eighth symposium on usable privacy and security*. [S.l.], 2012. p. 3. Citado na página 19.

FERRAILOLO, D.; CHANDRAMOULI, R.; KUHN, R.; HU, V. Extensible access control markup language (xacml) and next generation access control (ngac). In: ACM. *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control*. [S.l.], 2016. p. 13–24. Citado na página 22.

FROST, J. L. *A history of children's play and play environments: Toward a contemporary child-saving movement*. [S.l.]: Routledge, 2010. Citado na página 16.

FROST, J. L.; WORTHAM, S. C.; REIFEL, R. S. *Play and child development*. [S.l.]: Merrill, Prentice Hall, 2001. Citado na página 16.

FUERTE, W.; QUIMBIULCO, K.; GALARRAGA, F.; GARCIA-DORADO, J. L. On the development of advanced parental control tools. In: *1st Int. Conf. on Software Security and Assurance*. [S.l.: s.n.], 2015. p. 1–6. Citado 3 vezes nas páginas 20, 70 e 75.

GIL, A. C. Como elaborar projetos de pesquisa. *São Paulo*, v. 5, n. 61, p. 16–17, 2002. Citado na página 24.

HAYNES, J.; RAMIREZ, M.; HAYAJNEH, T.; BHUIYAN, M. Z. A. 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. Citado 4 vezes nas páginas 17, 54, 66 e 67.

HE, Q. Privacy enforcement with an extended role-based access control model. *North Carolina State University at Raleigh, Raleigh, NC*, 2003. Citado na página 41.

Hello Barbie Mattel. *Meet Hello Barbie*. 2016. Acesso em: 23/05/2018. Disponível em: <http://helloworldbarbiefaq.mattel.com>. Citado 2 vezes nas páginas 29 e 30.

HERTZEL, D. A. Don't talk to strangers: An analysis of government and industry efforts to protect a child's privacy online. *Fed. Comm. LJ*, HeinOnline, v. 52, p. 429, 1999. Citado na página 35.

HEURIX, J.; ZIMMERMANN, P.; NEUBAUER, T.; FENZ, S. A taxonomy for privacy enhancing technologies. *Computers & Security*, Elsevier, v. 53, p. 1–17, 2015. Citado 2 vezes nas páginas 31 e 33.

HEVNER, A. R.; MARCH, S. T.; PARK, J.; RAM, S. Design science in information systems research. *MIS Quarterly: Management Information Systems*, v. 28, n. 1, p. 75–105, 2004. Citado 2 vezes nas páginas 24 e 25.

HINSKE, S.; LANGHEINRICH, M.; LAMPE, M. Towards guidelines for designing augmented toy environments. In: ACM. *Proceedings of the 7th ACM conference on Designing interactive systems*. [S.l.], 2008. p. 78–87. Citado na página 37.

HOLLOWAY, D.; GREEN, L. The internet of toys. *Communication Research and Practice*, p. 1–14, 2016. Citado 5 vezes nas páginas 35, 54, 64, 66 e 78.

HUNG, P. C.; CHENG, V. S. Privacy. In: *Encyclopedia of Database Systems*. [S.l.]: Springer, 2009. p. 2136–2137. Citado na página 33.

HUNG, P. C.; IQBAL, F.; HUANG, S.-C.; MELAIS, M.; PANG, K. A glance of child's play privacy in smart toys. In: SPRINGER. *International Conference on Cloud Computing and Security*. [S.l.], 2016. p. 217–231. Citado na página 69.

HUNG, P. C. K.; FANTINATO, M.; RAFFERTY, L. A study of privacy requirements for smart toys. In: *Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS)*. [S.l.]: AIS, 2016. p. 1–7. Citado 9 vezes nas páginas 19, 40, 54, 65, 71, 73, 74, 76 e 78.

HUNG, P. C. K.; FANTINATO, M.; RAFFERTY, L. A study of privacy requirements for smart toys. In: *Pacific Asia Conference on Information Systems, PACIS 2016 - Proceedings*. [S.l.: s.n.], 2016. p. 71. Citado na página 70.

HUNG, P. C. K.; FANTINATO, M.; ROA, J. Children privacy protection. In: LEE, N. (Ed.). *Encyclopedia of Computer Graphics and Games*. [S.l.]: Springer, 2019. Citado na página 46.

HUNG, P. C. K.; IQBAL, F.; HUANG, S.-C.; MELAIS, M.; PANG, K. A glance of child's play privacy in smart toys. In: *Proceedings of the 2nd International Conference on Cloud Computing and Security (ICCCS)*. [S.l.]: Springer Verlag, 2016. p. 217–231. Citado 11 vezes nas páginas 16, 18, 29, 31, 32, 34, 46, 54, 73, 75 e 120.

ISO/IEC. *Information technology — Security techniques — Privacy framework*. [S.l.]: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2011. (ISO/IEC 29100:2011(E)). Citado na página 52.

ISO/IEC 25010:2011. *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System And Software Quality Models*. 2011. Acesso em: 23/08/2018. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en>. Citado na página 40.

ITU; UNICEF. *Guidelines for Industry on Child Online Protection*. Geneva, Switzerland: International Telecommunication Union. 2014. International Telecommunication Union (ITU), United Nations Children's Fund (UNICEF). Disponível em: http://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_E.PDF. Citado 3 vezes nas páginas 18, 20 e 40.

JAOKAR, A.; FISH, T. *OpenGardens: The Innovator's Guide to the Mobile Data Industry*. [S.l.]: Futuretext, 2004. Citado na página 39.

JONES, M. L. Your new best frenemy: Hello barbie and privacy without screens. *Engaging Science, Technology, and Society*, v. 2, p. 242–246, 2016. Citado na página 54.

JONES, M. L.; MEURER, K. Can (and should) Hello Barbie keep a secret? In: *Proceedings of the 2016 IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS)*. [S.l.]: IEEE, 2016. p. 1–7. Citado 2 vezes nas páginas 54 e 79.

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. Citado na página 90.

Juniper Research. *Smart toy revenues to hit \$2.8bn this year, driven by black friday & christmas holiday sales*. 2017. Acesso em: 12/06/2018. Disponível em: [https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-\\$2-8bn-this-year](https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2-8bn-this-year). Citado 2 vezes nas páginas 18 e 120.

KITCHENHAM, B.; CHARTERS, S. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. 2007. Citado 3 vezes nas páginas 45, 48 e 49.

KSHETRI, N.; VOAS, J. Cyberthreats under the bed. *Computer*, v. 51, n. 5, p. 92–95, 2018. Citado 2 vezes nas páginas 54 e 64.

LICCARDI, I.; BULGER, M.; ABELSON, H.; WEITZNER, D. J.; MACKAY, W. E. Can apps play by the COPPA rules? In: *12th Ann. Int. Conf. on Priv., Sec. and Trust*. [S.l.]: IEEE, 2014. p. 1–9. Citado 4 vezes nas páginas 73, 74, 77 e 78.

LOUKIL, F.; GHEDIRA-GUEGAN, C.; BENHARKAT, A. N.; BOUKADI, K.; MAAMAR, Z. Privacy-aware in the IoT applications: A systematic literature review. In: *Proceedings of the 25th International Conference on Cooperative Information Systems (CoopIS)*. [S.l.]: Springer Verlag, 2017. p. 552–569. Citado 4 vezes nas páginas 51, 52, 58 e 59.

MAHMOUD, M.; HOSSEN, M. Z.; BARAKAT, H.; MANNAN, M.; YOUSSEF, A. Towards a comprehensive analytical framework for smart toy privacy practices. In: *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. [S.l.]: ACM, 2017. p. 64–75. Citado 2 vezes nas páginas 54 e 66.

MAHMOUD, M.; HOSSEN, M. Z.; BARAKAT, H.; MANNAN, M.; YOUSSEF, A. Towards a comprehensive analytical framework for smart toy privacy practices. In: ACM. *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*. [S.l.], 2018. p. 64–75. Citado na página 17.

MARTÍN-RUIZ, M. L.; FERNÁNDEZ-ALLER, C.; PORTILLO, E.; MALAGÓN, J.; BARRIO, C. del. Developing a system for processing health data of children using digitalized toys: Ethical and privacy concerns for the internet of things paradigm. *Science and engineering ethics*, Springer, p. 1–20, 2017. Citado na página 36.

MCREYNOLDS, E.; HUBBARD, S.; LAU, T.; SARAF, A.; CAKMAK, M.; ROESNER, F. Toys that listen: A study of parents, children, and internet-connected toys. In: *Proceedings of the 2017 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. [S.l.]: ACM, 2017. p. 5197–5207. Citado 4 vezes nas páginas 30, 54, 66 e 74.

MCREYNOLDS, E.; HUBBARD, S.; LAU, T.; SARAF, A.; CAKMAK, M.; ROESNER, F. Toys that listen: A study of parents, children, and internet-connected toys. In: ACM. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. [S.l.], 2017. p. 5197–5207. Citado na página 70.

MOINI, C. Protecting privacy in the era of smart toys: Does hello barbie have a duty to report. *Cath. UJL & Tech*, HeinOnline, 2016. Citado na página 20.

MOINI, C. Protecting privacy in the era of smart toys: Does hello barbie have a duty to report. *Catholic University Journal of Law and Technology*, v. 25, n. 2, p. 281–318, 2017. Citado 3 vezes nas páginas 54, 66 e 75.

More, S. V.; Chatterjee, M. Improved multiparty access control mechanism for osn. In: *Int. Conf. on Comp., Comm., Cont. and Aut.* [S.l.]: IEEE, 2017. p. 1–6. Citado na página 73.

OLSSON, T.; SALO, M. Online user survey on current mobile augmented reality applications. In: IEEE. *Mixed and Augmented Reality (ISMAR), 2011 10th IEEE International Symposium on.* [S.l.], 2011. p. 75–84. Citado na página 30.

PERKINS, G. H. Will libraries' web-based survey methods replace existing non-electronic survey methods? *Information Technology and Libraries*, American Library Association, v. 23, n. 3, p. 123–127, 2004. Citado na página 108.

PIMENTEL, M.; FILIPPO, D.; SANTORO, F. M. Design science research: fazendo pesquisas científicas rigorosas atreladas ao desenvolvimento de artefatos computacionais projetados para a educação. *Metodologia de Pesquisa em Informática na Educação: Concepção da Pesquisa*. Porto Alegre: SBC, 2019. Citado na página 25.

PLEBAN, J.-S.; BAND, R.; CREUTZBURG, R. Hacking and securing the AR.Drone 2.0 quadcopter: Investigations for improving the security of a toy. In: *Proceedings of the Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications*. [S.l.]: SPIE, 2014. p. 1–12. Citado 2 vezes nas páginas 54 e 65.

PRESSMAN, R.; MAXIM, B. *Engenharia de Software: Uma prática profissional*. [S.l.]: McGraw Hill Brasil, 2016. v. 8. Citado na página 26.

RAFFERTY, L.; FANTINATO, M.; HUNG, P. C. Privacy requirements in toy computing. In: *Mobile Services for Toy Computing*. [S.l.]: Springer, 2015. p. 141–173. Citado 11 vezes nas páginas 19, 27, 28, 34, 35, 36, 37, 70, 73, 75 e 93.

RAFFERTY, L.; HUNG, P.; FANTINATO, M.; PERES, S. M.; IQBAL, F.; KUO, S.; HUANG, S. Towards a privacy rule conceptual model for smart toys. In: *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS)*. [S.l.]: AIS, 2017. p. 1–10. Citado 17 vezes nas páginas 9, 18, 19, 20, 21, 29, 41, 42, 43, 54, 65, 69, 70, 73, 74, 75 e 78.

RAFFERTY, L.; HUNG, P. C. Introduction to toy computing. In: *Mobile Services for Toy Computing*. [S.l.]: Springer, 2015. p. 1–7. Citado 8 vezes nas páginas 16, 17, 36, 37, 38, 39, 41 e 44.

RAFFERTY, L.; HUNG, P. C.; FANTINATO, M.; PERES, S. M.; IQBAL, F.; KUO, S.-Y.; HUANG, S.-C. Towards a privacy rule conceptual model for smart toys. In: *Computing in Smart Toys*. [S.l.: s.n.], 2017. p. 85–102. Citado na página 86.

RAFFERTY, L.; KROESE, B.; HUNG, P. C. Toy computing background. In: *Mobile Services for Toy Computing*. [S.l.]: Springer, 2015. p. 9–38. Citado 7 vezes nas páginas 31, 37, 38, 39, 40, 69 e 70.

REIGADA, A. T. *La protección de datos personales: en busca del equilibrio*. [S.l.]: Tirant lo Blanch, 2011. 1990 p. Citado na página 36.

REUVER, M. de. Governance of mobile service innovation after the walled gardens. *info*, Emerald Group Publishing Limited, v. 13, n. 1, p. 43–60, 2011. Citado na página 39.

SAHA, D.; MUKHERJEE, A. Pervasive computing: a paradigm for the 21st century. *Computer*, IEEE, n. 3, p. 25–31, 2003. Citado na página 39.

SANDHU, R. S.; SAMARATI, P. Access control: principle and practice. *IEEE communications magazine*, IEEE, v. 32, n. 9, p. 40–48, 1994. Citado na página 40.

SHASHA, S.; MAHMOUD, M.; MANNAN, M.; YOUSSEF, A. Playing with danger: A taxonomy and evaluation of threats to smart toys. *IEEE Internet of Things Journal*, TBD, n. TBD, p. TBD, 2018. Citado 5 vezes nas páginas 17, 54, 65, 66 e 69.

SILVA, L. V.; BARBOSA, P.; MARINHO, R.; BRITO, A. Security and privacy aware data aggregation on cloud computing. *Journal of Internet Services and Applications*, v. 9, n. 1, p. 6, 2018. Citado na página 33.

SMITH, K. L.; SHADE, L. R. Children’s digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture. *Big Data & Society*, TBD, n. TBD, p. TBD, 2018. Citado na página 54.

statcounter Globalstats. *Mobile Operating System Market Share Worldwide*. 2020. Acesso em: 02/04/2020. Disponível em: <https://gs.statcounter.com/os-market-share/mobile/worldwide>. Citado na página 92.

TANG, J. K.; HUNG, P. C. *Computing in Smart Toys*. [S.l.]: Springer, 2017. Citado 2 vezes nas páginas 16 e 28.

TENNAKOON, H.; SARIDAKIS, G.; MOHAMMED, A. Child online safety and parental intervention: a study of Sri Lankan internet users. *IT & People*, v. 31, n. 3, p. 770–790, 2018. Citado na página 75.

USA. *COPPA – Children’s Online Privacy Protection Act*. 2002. Federal Trade Commis., US Congress, USA, <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>. Citado 2 vezes nas páginas 75 e 78.

VALENTE, J.; CARDENAS, A. A. Security & privacy in smart toys. In: *Proceedings of the 1st Workshop on Internet of Things Security and Privacy (IoT S&P)*. [S.l.]: ACM, 2017. p. 19–24. Citado 2 vezes nas páginas 54 e 65.

WENNING, R. Platform for privacy preferences (p3p) project: enabling smarter privacy tools for the web. 2007. Citado na página 41.

World Economic Forum. Personal data: the emergence of a new asset class. In: *World Economic Forum*. [S.l.: s.n.], 2011. Citado na página 31.

WRIGHT, D. A framework for the ethical impact assessment of information technology. *Ethics and information technology*, Springer, v. 13, n. 3, p. 199–226, 2011. Citado na página 36.

YANKSON, B.; IQBAL, F.; LU, Z.; WANG, X.; HUNG, P. C. K. Modeling privacy preservation in smart connected toys by petri-nets. In: *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS)*. [S.l.]: AIS, 2019. p. 1696–1705. Citado 2 vezes nas páginas 54 e 63.

YONG, S.; LINDSKOG, D.; RUHL, R.; ZAVARSKY, P. Risk mitigation strategies for mobile Wi-Fi robot toys from online pedophiles. In: *Proceedings of the 2011 IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT)*. [S.l.]: IEEE, 2011. p. 1220–1223. Citado 2 vezes nas páginas 54 e 65.

ZIMMECK, S.; WANG, Z.; ZOU, L.; IYENGAR, R.; LIU, B.; SCHAUB, F.; WILSON, S.; SADEH, N. M.; BELLOVIN, S. M.; REIDENBERG, J. R. Automated analysis of privacy requirements for mobile apps. In: *24th Ann. Netw. and Dist. Sys. Sec. Symp.* [S.l.: s.n.], 2017. Citado na página 78.

Apêndice A – Questionário

Este documento apresenta a versão final do questionário aplicado para avaliação da importância dos requisitos e da satisfação da implementação do protótipo.

Avaliação: ferramenta de controle parental para brinquedos inteligentes

Olá,

Sou Otávio de Paula Albuquerque, mestrando do Programa de Pós-graduação em Sistemas de Informação da USP, sob a orientação do Prof. Dr. Marcelo Fantinato, com a colaboração do Prof. Dr. Patrick C. K. Hung, da Ontario Tech University, do Canadá.

Gostaríamos que você pudesse avaliar um protótipo de ferramenta de "controle parental" para brinquedos inteligentes desenvolvido como parte de meu projeto de mestrado.

Para você participar, é necessário ter acesso a um celular com sistema operacional Android.

A avaliação é composta de duas partes:

1ª parte) Você deve instalar o aplicativo em seu celular Android e usá-lo um pouco, navegar por ele.

2ª parte) Você deve responder algumas perguntas sobre as funcionalidades e outras características para um aplicativo desse tipo (ou seja, seus requisitos funcionais e não-funcionais).

Ficariamos muito gratos se você puder contribuir com nossa pesquisa.

Atenciosamente,
Otávio, Marcelo e Patrick.

*Obrigatório

Conhecendo a ferramenta...

Por favor, baixe o aplicativo (apk) a partir deste link

https://drive.google.com/file/d/1NnS3GuVt5ZVo_aURXtUh9QDOoyk1Rjug/view?usp=sharing. Em seguida, instale o aplicativo e o explore, navegando por ele.

Caso o celular solicite permissão para instalação de aplicativos desconhecidos, é seguro permitir, tendo em vista que a fonte do download é o Google Drive e o aplicativo não tem conexão com entidades externas. Para permitir a instalação, siga os passos informados por seu celular, seguindo nas "configurações".

Alguns conceitos que podem ser úteis:

- **BRINQUEDO INTELIGENTE**: um brinquedo moderno, normalmente no formato de uma boneca, um robô ou um animal (urso, coelho, dinossauro), que pode oferecer várias opções de interatividade com a criança, incluindo conversar, gravar e mostrar vídeos, e jogos e brincadeiras interativas. Para isso, o brinquedo precisa estar conectado em uma rede wi-fi e se comunicar com um computador central da empresa que comercializa o brinquedo, localizado na "nuvem". Para oferecer ainda mais opções de interatividade para a criança, outras empresas podem desenvolver aplicativos de terceiros que se comunicam com o brinquedo.

- **FERRAMENTA DE CONTROLE PARENTAL**: um aplicativo para ser instalado em um celular, também conectado na rede wi-fi, que permite que o pai ou responsável legal pela criança defina que tipo de informação da criança o brinquedo e a empresa pode ter acesso, pensando em preservar a privacidade da criança. Uma vez que o brinquedo pode ter acesso a muitas informações das crianças que vão para a internet, os pais podem querer restringir o acesso a determinados tipos de informação, pelo menos para determinados fins; embora, se os pais restringirem demais, o brinquedo pode acabar sem utilidade.

- **REGRA DE PRIVACIDADE**: criar regras de privacidade é a principal funcionalidade de uma ferramenta de controle parental. Os pais podem criar várias e diferentes regras de privacidade, para diferentes fins. Por exemplo, "eu permito que o tipo de informação X seja usado apenas para tal coisa", "eu permito que o brinquedo envie vídeos mais que ele não grave vídeos, a não ser que seja para tal motivo específico", entre outros.

Criando uma "regra de privacidade"...

Para ter certeza de que você entendeu bem a ideia da ferramenta de controle parental, tente criar na ferramenta instalada em seu celular uma regra de privacidade para o seguinte propósito:

"Permitir que qualquer tipo de dados de localização da criança sejam coletados apenas para serem usados em jogos por meio do brinquedo com função multi-jogadores, desde que se cumpra com todas as políticas existentes relacionadas à privacidade online de crianças. Os dados de localização coletados poderão ficar armazenados pelo brinquedo e pela empresa no máximo até dois meses."

Avaliação da ferramenta...

Agora, você deverá avaliar a ferramenta e seus requisitos.

Mas antes das avaliações, por favor, preencha os dados a seguir.

1. Nome completo *

---

2. E-mail *

---

3. Nível de escolaridade? *

Marcar apenas uma oval.

- ☐ Graduação em andamento
- ☐ Graduação completa
- ☐ Mestrado em andamento
- ☐ Mestrado completo
- ☐ Doutorado em andamento
- ☐ Doutorado completo

4. O quanto você considera que conhece sobre brinquedos inteligentes? *

Marcar apenas uma oval.

	0	1	2	3	4	5	6	7	8	9	10	
Nenhum conhecimento	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Conhecimento de especialista

Avaliação dos REQUISITOS FUNCIONAIS

Começando pelos requisitos funcionais, ou seja, as funcionalidades que a ferramenta de controle parental deveria apresentar.

Nós listamos e explicamos abaixo 19 requisitos funcionais.

Para cada requisito funcional, você deve:

1º) **IMPORTÂNCIA:** classificar (de 1 a 5) o quão importante/útil você acha que o requisito é para uma ferramenta de controle parental para brinquedos inteligentes, ou seja, o quanto você acha que uma ferramenta de controle parental deveria ter esse requisito.

2º) **SATISFAÇÃO:** classificar (de 1 a 5) o quão representado você acha que o requisito está no protótipo de ferramenta que você avaliou, ou seja, o quanto você acha que o requisito está implementado satisfatoriamente/adequadamente na ferramenta.

Alguns requisitos não foram implementados, então apenas o 1º item é solicitado para esses requisitos. Outros, estão implementados apenas parcialmente, por se tratar de uma ferramenta protótipo; mas, nesse caso, você deve avaliar normalmente.

Requisito 1. Criar perfil dos pais ou responsáveis legais

Cadastrar dados básicos de contato do usuário da ferramenta (ou seja, dos pais ou responsável legal) tais como nome e e-mail, para permitir a comunicação entre o usuário e a empresa do brinquedo inteligente.

5. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

6. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 2. Obter consentimento dos pais

Obter o consentimento dos pais, no qual eles assumem a propriedade dos dados em nome da criança e concordam com a política de privacidade da empresa de brinquedo, garantindo o direito à coleta de dados da criança por parte da empresa, desde que não fira as regras de privacidade a serem definidas pelos pais por meio dessa ferramenta.

7. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

8. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 3. Notificar mudanças na política de privacidade da empresa

Notificar os pais sobre alterações na política de privacidade da empresa de brinquedos em relação às regras gerais de coleta, uso, compartilhamento e divulgação de dados da criança com os quais os pais haviam concordado antes e solicitar uma nova concordância dos pais.

9. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

10. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 4. Apresentar a política de privacidade da empresa

Apresentar e facilitar o acesso à política de privacidade da empresa do brinquedo, que define as regras básicas sobre as quais a empresa se compromete a lidar com os dados que ela terá acesso.

11. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

12. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 5. Garantir autenticidade de acesso (não implementado)

Verificar se o usuário cadastrado na ferramenta é realmente os pais da criança por meio de algum mecanismo de verificação, como confirmação de acesso por e-mail, formulário assinado e enviado digitalmente, cartão de crédito com débito reembolsado etc.

13. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 6. Criar regras de privacidade

Permitir que os pais criem "regras de privacidade" para definir como os dados manipulados pelo brinquedo (incluindo informações de identificação pessoal da criança) deverão ser coletados, manipulados, compartilhados, divulgados e enviados, permitindo ou negando acesso aos dados de acordo com as preferências do usuário.

14. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

15. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 7. Disponibilizar modelos de regras de privacidade (não implementado)

Auxiliar os pais na criação de "regras de privacidade" por meio da disponibilização de modelos (ou seja, templates) de regras de privacidade, incluindo modelos externos. Esses modelos devem funcionar como regras de privacidade predefinidas que podem ser alteradas posteriormente para atender exatamente o desejo do usuário.

16. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 8. Definir data de validade de regra de privacidade

Permitir que os pais definam uma data de validade para as regras de privacidades criadas, incluindo períodos pré-determinados ou indeterminados.

17. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

18. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 9. Consultar descrição de regra de privacidade

Permitir que pais verifiquem, a qualquer momento, todos os detalhes de uma regra de privacidade já criada anteriormente por eles.

19. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

20. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 10. Desabilitar regra de privacidade

Permitir que os pais possam, a qualquer momento, desabilitar uma regra de privacidade criada anteriormente por eles. Uma regra de privacidade desabilitada deixa de funcionar, mas não é apagada, podendo ser habilitada novamente posteriormente.

21. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

22. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 11. Disponibilizar diretrizes para os pais

Fornecer aos pais materiais informativos contendo orientações sobre riscos de privacidade online para crianças que usam brinquedos inteligentes assim como conteúdos para facilitar o aprendizado de uso da ferramenta, destacando a importância dos pais usarem os recursos fornecidos pela ferramenta de controle parental.

23. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

24. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 12. Disponibilizar links úteis para os pais

Disponibilizar para os pais links para conteúdos importantes relacionados a privacidade online infantil, facilitando o acesso a, por exemplo, atos, leis, políticas de privacidade da empresa de brinquedos etc.

25. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

26. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 13. Informar sobre consequências da criação de regras de privacidade (não implementado)

Explicar aos pais sobre restrições que algumas funcionalidades do brinquedo poderão apresentar se determinados tipos de regras de privacidade muito restritivas forem criadas.

27. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 14. Classificar riscos de privacidade online infantil (não implementado)

Classificar riscos de privacidade infantil para ajudar os pais em suas tomadas de decisão na criação de regras de privacidade. Essa classificação pode ser realizada com base em técnicas estatísticas ou de aprendizado de máquina, como modelos probabilísticos generativos. Os riscos de privacidade podem, por exemplo, ser listados por frequência de ocorrência ou grau de ameaça.

28. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 15. Disponibilizar acesso a "Dúvidas Comuns" (FAQ)

Fornecer aos pais respostas para as perguntas mais frequentes e relevantes relacionadas ao uso do brinquedo inteligente e da ferramenta de controle parental.

29. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

30. O quão satisfatório esse requisito está implementado no protótipo avaliado? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 16. Disponibilizar canal de fácil comunicação (Chat)

Proporcionar um canal de comunicação rápido e fácil para que os pais possam resolver dúvidas, registrar reclamações e enviar sugestões perante à empresa de brinquedos.

31. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

32. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 17. Remover dados sensíveis e/ou PII

Permitir que os pais solicitem que a empresa do brinquedo exclua todas os dados sensíveis e/ou de "Informações Pessoais identificáveis" (Personally Identifiable Information - PII) coletadas da criança durante suas interações com o brinquedo até o momento.

33. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

34. O quão satisfatório esse requisito está implementado no protótipo avaliado? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco satisfatório	☐	☐	☐	☐	☐	Muito satisfatório

Requisito 18. Manter histórico de atividades da criança (não implementado)

Registrar o histórico de todas as atividades realizadas pela criança ao usar o brinquedo inteligente, incluindo a gravação de conversas com o brinquedo (se o brinquedo possuir microfone) e disponibilizar esse histórico de atividades para acesso pelos pais (incluindo das conversas gravadas).

35. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 19. Monitorar e alertar sobre assuntos suspeitos mencionados pela criança (não implementado)

Aplicar técnicas de processamento de língua natural e reconhecimento de padrões nos diálogos entre a criança e o brinquedo inteligente para alertar imediatamente os pais caso sejam identificados assuntos suspeitos falados pela criança, se desejado pelos pais. Por exemplo, palavras como drogas, arma, morte, assédio, sangue, sexo, etc.

36. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Avaliação dos REQUISITOS NÃO-FUNCIONAIS

Vamos agora para os requisitos não-funcionais, ou seja, características ou propriedades que apoiam as funcionalidades da ferramenta de controle parental, tais como usabilidade, segurança, desempenho etc.

Há 18 requisitos não-funcionais para sua avaliação.

Esses requisitos não foram considerados diretamente no desenvolvimento desse protótipo de ferramenta de controle parental, pois o objetivo principal deste projeto são apenas os requisitos funcionais. Assim, você deve avaliar apenas a "IMPORTÂNCIA" de cada requisito não-funcional para uma ferramenta de controle parental, sem considerar se ele foi ou não adequadamente implementado no protótipo avaliado.

Alguns dos requisitos não-funcionais listados até foram implementados, pelo menos parcialmente, no protótipo da ferramenta, mas de forma indireta por meio da implementação de requisitos funcionais. Porém, como esse não era o objetivo principal deste projeto, isso não está agora em avaliação.

>>>> USABILIDADE

Requisito 1. Multiplataforma

Os pais devem poder usar a ferramenta de controle parental em seu ambiente tecnológico conhecido, considerando, por exemplo, diferentes tipos de dispositivos móveis e sistemas operacionais.

37. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 2. Múltiplos usuários

A ferramenta de controle parental deve permitir diferentes pais ou responsáveis legais criarem regras de privacidade para diferentes crianças.

38. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 3. Fácil instalação

Os pais devem ser capazes de entender e gerenciar facilmente o processo de instalação da ferramenta de controle parental.

39. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 4. Fácil uso

A empresa desenvolvedora da ferramenta de controle parental deve seguir os princípios de usabilidade de software, para oferecer aos pais uma ferramenta fácil de entender e de usar, de forma rápida e intuitiva.

40. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

>>>> INTEROPERABILIDADE

Requisito 5. Interoperabilidade semântica

A ferramenta de controle parental deve poder trocar informações de forma clara e correta com serviços móveis.

41. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

>>>> SEGURANÇA

Requisito 6. Autenticar usuário

A ferramenta de controle parental deve autenticar todos os seus usuários para garantir que apenas os pais ou responsáveis legais estejam desempenhando o papel de guardião da criança.

42. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 7. Criptografar "Informações Pessoais Identificáveis" (PII)

A ferramenta de controle parental deve criptografar as "Informações Pessoais Identificáveis" (PII) a serem acessadas por outros aplicativos, mesmo que o acesso seja por outros aplicativos sendo executados no mesmo dispositivo móvel.

43. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 8. Autenticar e autorizar comunicações

A comunicação entre a ferramenta de controle parental e o ambiente de computação para brinquedos deve usar protocolos de comunicação que permitam mecanismos de autenticação e autorização.

44. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 9. Criptografar comunicação

A comunicação entre a ferramenta de controle parental e o ambiente de computação para brinquedos deve usar mecanismos criptográficos.

45. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 10. Garantir a integridade do arquivo de configuração

---

A integridade do arquivo de configuração deve ser verificada e mantida para cada sessão de uso da ferramenta de controle parental no dispositivo móvel.

46. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 11. Exigir certificado digital para serviços móveis

---

A ferramenta de controle parental deve garantir que as "Informações Pessoais Identificáveis" (PII) da criança sejam enviadas ou compartilhadas apenas com serviços móveis que possuem certificados digitais que permitem a verificação de identidade digital.

47. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 12. Notificar violações de segurança

A ferramenta de controle parental deve notificar os pais sobre qualquer violação de segurança detectada em relação a seu uso.

48. Qual a importância desse requisito para uma ferramenta de controle parental? **Marcar apenas uma oval.*

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 13. Seguir boas práticas de segurança de software

A empresa desenvolvedora da ferramenta de controle parental deve seguir princípios de segurança de software conhecidos.

49. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

>>>>> LEGAL

Requisito 14. Cumprir com o consentimento dos pais

A ferramenta de controle parental deve garantir que as "Informações Pessoais Identificáveis" (PII) da criança não sejam coletadas, usadas, compartilhadas ou divulgadas com terceiros sem o consentimento dos pais, considerando suas preferências manifestadas pelas regras de privacidade criadas.

50. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 15. Cumprir com as normas legais

As operações realizadas, apoiadas e permitidas pela ferramenta de controle parental devem estar em conformidade com as normas legais definidas por leis e regulamentos gerais aplicáveis.

51. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 16. Cumprir com o direito à privacidade das crianças

---

As operações realizadas, apoiadas e permitidas pela ferramenta de controle parental devem respeitar os direitos de privacidade das crianças cumprindo as normas e atos específicos para esse fim.

52. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Requisito 17. Informar com clareza sobre a coleta e divulgação de dados

---

Esclarecer aos pais quais "Informações Pessoais Identificáveis" (PII) da criança estão sendo coletadas, como são usadas e compartilhadas com terceiros e práticas adicionais de divulgação.

53. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

>>>> IMPLEMENTAÇÃO

Requisito 18. Implementar seguindo o "Privacy by Design"

A empresa desenvolvedora da ferramenta de controle parental deve implementar efetivamente ações técnicas e organizacionais apropriadas para atender aos requisitos de privacidade dos regulamentos legais e proteger os direitos dos proprietários dos dados.

54. Qual a importância desse requisito para uma ferramenta de controle parental? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	☐	☐	☐	☐	☐	Muito importante

Sugestões?

55. Há requisitos adicionais que você acha importante para uma ferramenta de controle parental e que não foram apresentados aqui? Se sim, cite-os abaixo. Podem ser requisitos funcionais ou não-funcionais.

Powered by

Apêndice B – Dados qualitativos

Este documento apresenta as sugestões compiladas dos dados qualitativos, coletados por meio da pergunta subjetiva do questionário.

Sugestões
Autenticação de identidade do responsável por fotos e documentos, para garantir a integridade do vínculo entre responsável e dependente.
Cadastro de PIN para acessar o app.
Histórico de dispositivos que foram impedidos por alguma regra(para que pais possam ter noção de quais fabricantes são mais ou menos invasivos na coleta de dados).
Não é explicado como ela funciona, talvez ter um step by step para a criação da primeira regra, como acontece em jogos.
Botão editar e apagar habilitados mas sem funcionamento, quando não se tem uma regra
Botão apagar não pede confirmação. É importante ajudar o usuário a prever esses erros.
Tip do header de controle de acesso poderia ser explicado com exemplos reais, terminologia usada pode acabar confundindo. É preciso trazer mais compatibilidade do sistema ao mundo real, isso pode ser feito usando no app a mesma linguagem dos pais
Seria legal ter um link direto entre a explicação de cada uma das leis e essa tela, para não perder o status atual da criação
A regra que estou criando é para permitir acesso ou para restringir? Só descubro isso no final, quando o app gera um texto dizendo: “A regra de privacidade X permitirá que o serviço móvel...”
Não parece natural que as notificações de atualização de políticas fiquem nessa aba. Seria legal se tivesse um ícone de notificações, estilo Facebook, no header principal do app visível em todos os estados do aplicativo (uma vez que a informação é sensível), apenas para notificar a alteração. A lista de alterações em si parece ter mais a ver com a área dos pais. Mesmo ocorre para a remoção de dados sensíveis, parece ser uma opção para a área dos pais.
Qual empresa estou solicitando? Seria interessante se tivesse possibilidade de selecionar as empresas as quais quero fazer a solicitação.
A ferramenta pode aperfeiçoar a leitura e compreensão das políticas de privacidade e termos de uso. Por exemplo, seccionar o formulário dos termos para garantir a leitura completa. É um texto muito extenso. A ferramenta deve garantir sua leitura, ou re-inteirar todos os seus pontos ao longo das funcionalidades. Além disso, a linguagem está muito técnica para um pai/responsável leigo no assunto.
Quais os mecanismos de feedback para criação de regras impeditivas (que comprometam as funcionalidades essenciais do brinquedo)? Como eu associo o brinquedo a ferramenta de controle? Seria uma ferramenta genérica para todos os brinquedos ou ela seria incorporada por cada empresa/produto?
A semântica da criação de regras só fica explícita após a criação. O exemplo de regra já pode ser direto. Na aplicação não fica claro a vantagem de usar um modelo ou criar do início.
Evitar informações em excesso; pais e responsáveis podem não desejar passar muito tempo, nem usar frequentemente tais aplicações, visto que requer que eles pensem em ocasiões indesejadas para seus filhos. Por isso, tais aplicações precisam ser eficiente a ponto de não requisitar uso frequente dos pais.;
Prover alternativas de visualização para políticas de privacidade.;
Evitar o uso de jargões.;
Funcionar offline (e.g., alternativas aos vídeos do youtube).;
função de emergência claramente indicada.
Visualização e alteração de perfil do responsável;
Exibição das informações já compartilhadas;

Escolha de níveis de privacidade.
Acredito que os requisitos funcionais e não-funcionais já são suficientes para o que a ferramenta propõe.
O aplicativo deve passar por um teste de usabilidade robusto para que os pais/guardiões se sintam à vontade para utilizar o app.
Requisito Funcional: Adicionar alerta de tempo de uso da criança com o brinquedo.
Seria interessante que os pais pudessem configurar horário/dias da semana para a ativação ou desativação das regras.
A introdução com os objetivos da ferramenta poderia estar disponível em algum lugar, ou aparecer para o usuário outras vezes, não apenas no primeiro acesso.
Há muito texto no protótipo, o que torna a criação de mais de uma regra cansativa.
Entendo que criar regras baseadas em modelos é mais interessante para o usuário por ser um processo mais rápido, logo, é importante que essa seja a opção default.
Seria interessante, ainda, que essas regras "prontas" apareçam ordenadas por relevância, tomando como parâmetro a quantidade de usuários que as ativaram em seus dispositivos.
(1) Na aba "Dados do pai ou responsável" tem uma pergunta sobre se o usuário costuma receber por email as notificações (algo assim), POREM, somente é requerido o email, então não há resposta relativa a essa pergunta ok?
(2) Nas abas, em geral, os termos pai/guardião legal são recorrentes. Acho que merece ser atendida a expectativa das "mães", principalmente nos dias atuais. Vale a pena uma NOTA sobre isso, pelo menos.
(3) Na aba "política de privacidade" tem uma caixa de texto com CONTEÚDO textual extenso - a política inteira!! Bem, exige o uso do scroll. Fica uma questão: será que todo usuário vai usar o scroll? Será que vai perceber isso? Porque, de fato, não é exigido que o usuário LEIA todo o conteúdo. Bom, sabemos que essa prática é usual, uma vez que usuários não gostam de ler textos extensos e que sejam muito prolixos... porém, já vi alguns apps que pedem que pelo menos seja habilitado o botão de "li e concordo" depois de rodar todo o scroll... Enfim, por se tratar de um hot topic desse app, acho que merece um certo destaque essa estratégia de interação.
(4) ao sair da aba de 'política de privacidade' me foi apresentada uma pop-up que perguntava se eu tinha certeza do que eu vi!!! No entanto, propositalmente, eu não tinha clicado no "concordo"... Vai funcionar desse jeito mesmo ???
(5) enquanto eu criei regras, vi que nas opções de alguns elementos (obrigações por ex) eu não tinha escolhido / selecionado nenhum, e portanto apareceu uma mensagem em pop-up pedindo que eu selecionasse . Ok, porém o usuário pode não 'perceber o contexto'.. Em outra regra, que eu estava criando não foi exigida seleção de alguma das opções de "destinatários", por ex. Assim, fiquei imaginando que dependendo da regra, alguns elementos são obrigatório e outros não... Será que é isso mesmo??? ENFIM, parabéns pela app desenvolvida, as escolhas de design estão excelentes, tamanhos, cores, e navegação etc etc. PS: desculpe-me a demora pra retornar essa avaliação.
Não tenho um requisito novo para sugerir. Apenas esclarecendo sobre a nota 1 na questão de solicitar remoção de dados sensíveis. Na minha opinião, eu teria que poder solicitar isso sem apresentar justificativas. Acho que seria um direito meu. A empresa sim, deveria apresentar justificativas caso precise manter algum dado sensível por algum propósito, e eu avaliaria se ela poderia mantê-lo.
Em termos técnicos, o requisito está bem implementado no seu protótipo, visto que existe a possibilidade de solicitação, eu apenas não concordei com a maneira como essa ação seria executada no modelo de operação da empresa.

Anexo A – Anexo

Publicação do artigo referente a revisão sistemática da literatura.

Privacy in smart toys: Risks and proposed solutions

Otávio de Paula Albuquerque^a, Marcelo Fantinato^{a,*}, Judith Kelner^b,
Anna Priscilla de Albuquerque^b

^a University of São Paulo, São Paulo, SP, Brazil

^b Federal University of Pernambuco, Recife, PE, Brazil

ARTICLE INFO

Keywords:

Internet of Toys
Connected toys
Data privacy
Children
Literature review
Scoping review

ABSTRACT

Smart toys have become popular as technological solutions offer a better experience for children. However, the technology employed greatly increases the risks to children's privacy, which does not seem to have become a real concern for toy makers. We investigated this issue through a study driven by two major research questions: which are the major smart toys-related children's privacy risks and which are the major mitigation so to such risks. To answer these questions, we conducted a scoping review. As a result, we selected 26 primary studies and elaborated two classifications of risks and proposed solutions – technical and domain-specific. The most mentioned technical risk is data disclosure, while from a domain-specific perspective there is much concern on the children's physical and psychological safety. From a mitigation standpoint, many recommendations and solutions have been proposed, but without a more common type of contribution. As a main conclusion, we observed that toy makers and privacy regulations are not yet ready regarding children's privacy for a more active smart toys market.

1. Introduction

Both toy and game companies have started to integrate hardware and software computing into *smart toys* (Tang and Hung, 2017; Hung et al., 2017). Smart toys became able to collect and process data in real time favored by miniaturization and lower costs of processing circuits (Hung, 2015; Rafferty and Hung, 2015; Rafferty et al., 2015). The industry also refers to them as *connected toys* given their connectivity to other toys or gadgets such as smartphones, tablets and game consoles (McReynolds et al., 2017; Chowdhury, 2018). They can often connect to mobile and cloud services consequently permeating the domains of the Internet of Things (IoT), which in this context is sometimes called the *Internet of Toys* (IoToys) (Wang et al., 2010).

IoToys uses short- or long-range wireless communications protocols such as Wi-Fi, Bluetooth or Near Field Communication (NFC) for the acquisition, computing and transfer of child user's personal and non-personal information (Rafferty and Hung, 2015; Rafferty et al., 2015; Hung et al., 2017). The National Institute of Science and Technology (NIST) defines Personally Identifiable Information (PII) as “any information about an individual maintained by an organization that can be used to distinguish or trace an individual's identity, including any information linkable to an identifiable individual” (NIST, 2010). The International Organization for Standardization (ISO) defines PII as “any information that (a) can be used

to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person” (ISO/IEC, 2011).

In addition to PII, there are other types of user-sensitive data that may reveal personal information about them, such as *context data*. Context data is data observed and collected through sensors that gather signals on the user and its environment (Rafferty et al., 2015). Context data can be used to characterize some situation, as location or time, for example. Interaction data can also be sensitive, i.e., data derived from children's interactions with the toy, such as video and voice recordings (Yankson et al., 2019).

Smart toys use user-sensitive data for a variety of reasons. For example, pervasive location-based applications, such as Niantic's Pokémon Go (The Pokémon Company, 2016), collect Global Positioning System (GPS) data to allow outdoor playing. Smart toys such as Mattel's Hello Barbie (Mattel, 2017) and Cognitoys' Dino (Cognitoys, 2017), including companion robots such as Asus' Zenbo (ASUSTeK Computer Inc, 2018), aim to promote social communication between the user and the social toy or robotic agent. Conversation functions use speech recognition and Artificial Intelligence (AI) to establish and maintain a reasoning-based dialogue with the child. Thus, collecting, sharing, and storing PII, context data or interaction data, such as geo-location and child voice recordings, are common practices for these social agents in order to offer an experience resembling human communication.

* Corresponding author.

E-mail addresses: otavioalbuquerque@usp.br (O.d.P. Albuquerque), m.fantinato@usp.br (M. Fantinato), jk@cin.ufpe.br (J. Kelner), apa@cin.ufpe.br (A.P. de Albuquerque).

<https://doi.org/10.1016/j.elerap.2019.100922>

Received 1 May 2019; Received in revised form 10 November 2019; Accepted 10 November 2019

Available online 13 December 2019

1567-4223/ © 2019 Elsevier B.V. All rights reserved.

Similar to other IoT products, ensuring the privacy of the information collected is a critical challenge to smart toys (Hung et al., 2016b). In this case, the concern is even greater because PII is collected from underage users. Smart toy solutions can be opportunities for many risks to children's privacy, with PII becoming a target for unauthorized data collection, storage or disclosure (Shasha et al., 2018). Smart toy makers should consider threats and vulnerabilities to mitigate privacy risks before marketing new products that could compromise children's privacy. Smart toy solutions should at least ensure compliance with the information privacy and security regulations related to child users' PII.

Considering that authors from different knowledge areas do not always follow a common and well-defined nomenclature for terms related to privacy and security risks, threats and vulnerabilities, we use *risk* here as a general term to refer to all these related terms, disregarding the specificities that may exist in different fields. This is especially important in this multidisciplinary area that presents different perspectives on a same basic problem. Our study is concerned with both technical risks and domain-specific risks related to the use of smart toys by child users as well in with the different types of corresponding solutions.

As a recent technology and research field, we found no reference work in the literature on the key issues and solutions for smart toys-related privacy and security. As a result, it is still unclear, for example, whether the general IoT models apply. Thus, this study seeks to contribute to the following research questions:

1. Which risks to children's privacy when using smart toys have been addressed?
2. Which mitigation solutions to children's privacy risks have been proposed?

To gather information to answer our research questions, we conducted a scoping review (Paré et al., 2015), selecting 26 primary studies published from 2009 to 2019, combined with content analysis. Through content analysis, we analyzed indications found in primary studies and synthesized the evidences by relating them to different categorizations of privacy and security risks as well as of solutions to address those risks.

The study outcomes expose technical risks associated with children's privacy, mainly related to data breach, such as illegal or improper data disclosure, data leakage and theft, and data misuse. These issues can lead to domain-specific risks that threaten the physical and psychological safety of the child, including harassment, stalking, kidnapping, blackmail, bullying etc. Emerging risks were also detected such as dataveillance and online vandalism. As for solutions, most studies propose recommendations based on case studies, experiments and documentary studies. Such recommendations are targeted at toy makers, toy companies, lawmakers and parents. As a more concrete solution, frameworks were proposed to evaluate smart toys in relation to privacy regulations. Parental control tools are the most context-specific solution presented.

The remainder of this paper is organized as follows: Section 2 introduce children's privacy and smart toys. Section 3 summarizes literature reviews on correlated areas. Section 4 details the research method followed. Section 5 shows our results and findings. Section 6 presents a discussion of the results obtained, gathering all the analyzed information. Finally, Section 7 highlights the conclusions of our study.

2. Background

2.1. Privacy and children's privacy

Privacy can be considered a very vague concept and can be defined in different forms depending on the purpose (Solove, 2006). A generic way of defining privacy aligned to the purpose of this paper is *the right that someone has to keep their personal life or personal information secret or known only to a small group of people* (Cambridge Dictionary, 2019). We refer to *children's privacy* when the data for which privacy is desired is that of a child.

IoT-related products, including IoToys, offer clear risks to the user's privacy since they can collect, store and manage PII, including sharing users' PII with third parties. Governmental entities are worldwide taking efforts to regulate data privacy protection rules to be employed in companies and organizations. For example, the General Data Protection Regulation (GDPR) (EU, 2016) is a generic regulation on data protection and privacy for all individuals within the European Union and the European Economic Area, which also addresses the export of personal data outside this region. GDPR defines *Personal Data* (PD) as anything containing directly or indirectly compromising information that can expose user privacy and allow the singling out of individual behavior. PD includes the individual's name, his/her identification number, geolocation data and an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. Despite small differences between the concepts of NIST's PII and GDPR's PD, both refer to similar contexts that are distinguished only by the regulations they govern. PII is the most widely used term in North America and is more limited, while PD encompasses a wider range of information that may include publications on social media, photographs, personal preferences, transaction histories and IP addresses. Thus, the content of PII can be incorporated into PD. In this study, we use the term PII generically because it is the oldest and most used term.

A Brazilian law is based on PD while a Canadian is based on PII. The Brazilian General Law of Protection of Personal Data (GLPPD) (Brazil, 2018) was inspired by GDPR and incorporated the PD definition. GLPPD categorizes some types of PD as sensitive, which are any ethnic or racial information, political or religious affiliations or opinions, health status, sexual orientation, genetic data and biometrics. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada, 2018) refers to the PII definitions. PIPEDA applies to the collection, use or disclosure of PII in the course of commercial activities. It ensures that organizations must obtain the individual's consent to process their PII, and that individual has the right to access their PII maintained by the organization and contest its accuracy if necessary.

Further, the American Federal Trade Commission (FTC) offers specific PII regulations to the children's privacy, governed by the Children's Online Privacy Protection Act (COPPA) (USA, 2002). COPPA protects the online privacy of children under the age of 13 and states that a child's PII cannot be collected without parental consent. In 2010, an amendment to COPPA further elaborated that PII includes geolocation information, photographs and videos (Hung et al., 2016). In 2017, the FTC released an updated guidance document for COPPA that identifies smart toys as being covered under the act.

The children's privacy protection aims to enable parents to be in control of their children's privacy by specifying their privacy preferences for a toy, under the assumption that the toy has published an accurate privacy policy and complies with it in a privacy protection engine attached to the toy (Hung et al., 2019a).

COPPA, PIPEDA, GDPR and GLPPD has become quality references for smart toys, especially when it comes to protecting the children's privacy. Consumers, particularly parents, should be aware of these privacy risks considering that PII can only be used for the purposes for which it was collected. Thus, if a product plan to use them for another purpose, consent must be appropriately gotten. For instance, Mattel faced a lawsuit in 2016 due to a lack of information on Hello Barbie's privacy policies. This social toy was collecting children's PII (i.e., their voice recordings) before clearly notifying or receiving the consent of their parents since its behavior was not explicitly detailed in their privacy policies (McReynolds et al., 2017).

In 2017, the Mozilla Foundation launched the *privacy not included* website that aims to advise consumers on IoT products. The website includes a specific section focused on smart toys and other IoT gaming products, such as game consoles that can connect to online services. The site provides detailed information on some products, such as Hello Barbie and ToyMail Talkie (ToyMail, 2019). They include a discussion on whether these smart toys have secure access to sensitive peripherals

such as a built-in digital camera and microphone, and whether they can track user geolocation, among other types of PII.

2.2. Smart toys and smart toy-related privacy issues

Toys are products intended for leisure, learning, socialization and physical play that can address various benefits to child development (Rafferty and Hung, 2015). Smart toys appeared as a response to the sales decrease of traditional toys, which happened because of the increasing popularity of the internet- and console-based video gaming products (Dhar and Wu, 2015). The term *smart toy* covers a range of play products that can present different levels of network, processing and reasoning capabilities. Smart toys appear in various shapes, including anthropomorphic and humanoid, such as a plush toy, a doll, a companion robot or a wearable gadget. Technological solutions used by these smart toys vary since Augmented Reality (AR) resources to advanced functions such as wireless connectivity features and AI-based conversation functions.

There is still no consensus for smart toy terminology. Different terms appear such as connected toys, interactive toys, toy computing (Hung et al., 2019b), Internet of Toys (Wang et al., 2010) etc. For example, Denning et al. (2009) classified robot toys such as WowWee toys (WowWee, 2019) as smart toys as they present characteristics such as mobility, dexterity, sensing and output capability, and wireless communication. In another study, authors classified 23 interface setups for smart toys and referred to them as part of the Toy User Interfaces (ToyUI) concept (de Albuquerque and Kelner, 2018). ToyUI was defined as physical computing components, devices or peripherals, which promote physical and social play experiences to the users enabled by interactivity and connectivity features. Thus, a ToyUI includes different smart toy components and all other physical components connected to them (e.g., smartphones, game consoles and companion robots).

The term smart toys has long been used in the industry and may even refer to disconnected game products or sometimes non-electronic products (Tang and Hung, 2017; Hung et al., 2017). For instance, consumers use the term *smart toys* for challenging traditional children's toys, such as physical dexterity toys, puzzles, and board games (Ben-Joseph, 2018). Early electronic toys are also considered smart toys (Tang and Hung, 2017; Hung et al., 2017). They are mostly limited to remote-controlled cars and talking dolls, which although they can play a sequence of audio recordings, they differ from Mattel's Hello Barbie and Cognitoys Dino, which are speech recognition-enabled and offer reasoning capabilities. Successful examples of so-called unconnected smart toys are Bandai's first virtual pets, Tamagotchi (Bandai America Inc., 2019), 1996, and Tiger Electronics's plush toy, Furby (Hasbro, 2019), 1998.

Smart toys as other electronic products have evolved according to the popularization, miniaturization and lower costs of processing circuits. Ng et al. (2015) compared versions of the Bandai's Kamen Rider toy belts: the 2008 version emitted basic sounds and lights while the 2013 one had embedded digital sensors, which allowed it to process primary inputs from the player and output custom information. Due to the technological advances, smart toys became to collect user information, offering new risks to children's privacy.

The first smart toys introduced interactive toys with mobile applications (Hung, 2015; Rafferty and Hung, 2015; Rafferty et al., 2015). They can interact with related applications as an input by using AR-resources, computer vision, image processing, conductive materials or covering the smart devices with a physical toy shape (Tung, 2015; Kanev et al., 2015; Tang and Tewell, 2015; Kapralos et al., 2015). The risks to children's privacy with these interactive smart toys are similar to those offered by other mobile applications for social media and games. The risks include granting access to the smartphone's built-in cameras, microphones and using the related applications to collect PII such as GPS or profile information (e.g., children's full name, e-mail address etc.) (Ng et al., 2015; Rafferty et al., 2015a; Rafferty et al., 2017).

Concomitantly, other smart toys lines became to support wireless communication using protocols such as Bluetooth, Wi-Fi and NFC.

These network features amplified the smart toys capabilities for data collection and processing. Consequently, the network capabilities add new risks to children's privacy since collected information can become a target for retrieval during data traffic from the smart toy terminal to the connected device. In 2012, Hasbro released the connected smart toy Furby Boom able to connect via Bluetooth with corresponding iOS or Android mobile applications. Other examples of connected smart toys are Genesis' My Friend Cayla (Genesis Toys, 2019b) and IQue-robot (Genesis Toys, 2019a). Nintendo and Activision Blizzard also launched connected smart toy lines that use NFC to transfer data from the toy figurines to the connected game consoles.

A new wave of smart toys appeared more recently with the *toys that listen* (McReynolds et al., 2017). AI-based smart toys such as Hello Barbie, Dino, Anki's Cozmo (Anki, 2019), including companion robots such as Asus' Zenbo, offer more advanced conversation functions by collecting voice and presenting logical-reasoning capabilities. However, such capabilities evoke greater concerns to children's privacy and increase access to the toy to retrieve confidential and sensitive information. For instance, Hello Barbie doll plays pre-defined phrases that might encourage children to reveal confidential information on themselves and their family, which can be of great value to advertisers, among other risks to the children's privacy (Hung et al., 2016b).

Despite the several risks to children's privacy, smart toys are still a promising trend in the industry, expected to continuously grow. According to the United Kingdom-based Juniper Research group report from May 2018, they estimate a 7.878 billion (USD) revenue for smart toy vendors in America by 2023, and 17.7 worldwide. They consider both toy hardware purchase and in-app contents as most smart toys offer digital contents for purchase in their connected applications. However, this growth of industry depends on overcoming or at least mitigating the risks to children's privacy. Privacy risks associated with smart toys can compromise its future in the consumer's market, such as by affecting purchase intent and the distribution of these products to a worldwide audience (Fantinato et al., 2017; Fantinato et al., 2018). Thus, it is essential to address concrete solutions to mitigate those privacy risks aiming to support the promising future of smart toy markers.

3. Related work

We found a significant number of works addressing privacy and security concerns regarding smart toys. However, there is not yet a systematic study of the literature that analyzes the papers published in this context. We found some literature reviews that only partially cover our topic of interest. That means we could find some secondary studies on privacy and security in contexts other than smart toys as well as some secondary studies on smart toys with concerns other than privacy and security. Table 1 presents a comparative summary of the found reviews related to our study.

The *context* column shows that the found related reviews address broader research areas such as IoT (Loukil et al., 2017), Bring Your Own Device (BYOD) (Oktavia et al., 2017) and big data (Nelson and Olovsson, 2016). Although smart toys are considered a sub-area of IoT or BYOD, these more general reviews fail to address smart toys as this is a very specific subject within IoT and BYOD and they refer to more general aspects. Loukil et al. (2017) addresses six specific application domains: smart cities, smart homes, smart grids, health care, location sharing and smart spaces; none directly related to smart toys. Big data is high relevant to smart toys as one of the primary sources of risk of privacy violation when using smart toys is the large amount of data collected by the toy companies from their child-users. However, also in this case, as it is a very specific subject within the big data area, smart toys is not one of the topics covered in this review.

The other three reviews address smart toys without covering privacy concerns. Two of them address smart toys applied for clinical treatment. Nunes et al. (2015, 2017) present two complementary reviews on applying smart toys in the medical field, which include works to explain

Table 1

Comparison of related literature reviews.

Authors (and year)	Context	Period	Data source ²	Papers
Nunes et al. (2015)	Toys for clinical treatment	2010–2015	X,DL,WoS,SL,GS	13
Nelson and Olovsson (2016)	Privacy and security in big data	2012–2015	GS,SC	82
Oktavia et al. (2017)	Privacy and security in BYOD	2000–2017	S,GS,X	5
Nunes et al. (2017)	Toys for clinical treatment	N/D ¹	X,DL,GS	16
Loukil et al. (2017)	Privacy in IoT	2010–2017	DL,X,SD,WoS	90
de Albuquerque and Kelner (2018)	Smart toy interfaces	2008–2017	DL,X,SD,SL,S,SC	118
Our SLR, 2019	Privacy and security in smart toy	2009–2019	S,WoS	26

¹N/D: Not Defined./ ²Electronic Data Sources: S: Scopus; WoS: ISI Web of Science; X: IEEE Xplore; DL: ACM Digital Library; PM: PubMed; SL: SpringerLink; GS: Google Scholar; SD: Science Direct; SC: Specific Conferences.

medical procedures for hospitalized children or to assist in rehabilitation therapies for children with disabilities such as children with autism. The other review identifies the different types of interactions between users and smart toys, classifying them into different categories, such as gameplay, applications, among others (de Albuquerque and Kelner, 2018).

The six reviews found are recent as they refer to current subjects, with the oldest published in 2015. The length of time each review covered varies greatly (3–19 years), which depends on the specific context and purpose of each case. One may desire to increase or decrease the number of studies to be analyzed; or a specific topic may be so recent that it would not make sense to look for papers in a distant past.

Another factor potentially influencing the number of studies to be selected and analyzed in the review refers to which data sources were chosen to search for papers. Most reviews used multiple databases. Two reviews also looked for papers in specific conference proceedings. In the end, the number of papers (primary studies) ranged from 5 to 118, which resulted from both the search protocol decisions and mainly the review topic and context themselves. The search string used also influences the number of studies found and selected, but the string is not shown in this summary presented here.

Comparing these reviews with our review, several differences and some similarities can be pointed out. For example, we did not limit our review to any period of time. Despite this, the oldest document found by us dates back to 2009. As a result, the time period covered in our review is ten years. With regard to databases, we used only two, since Scopus is the largest base of peer-reviewed papers and indexes papers from other major databases, such as IEEE, ACM and Springer. We also used Web of Science as it has shown to be the only one to deliver additional papers. Scopus was used by only two of the six related reviews. On the other hand, four related reviews used Google Scholar, which was not used by us because it indexes many non-peer-review papers. As a result, we were able to select 26 primary studies for the context of privacy and safety in smart toys, a topic that had not yet been addressed through a literature review study.

4. Research method

To answer the research questions on what are the main risks to smart toy-related children's privacy and whether these risks can be mitigated, we conducted a scoping review (Paré et al., 2015). We analyzed the existing indications found through the literature review and synthesized the evidences relating them to the different categories of children's privacy risks and solutions to address them.

4.1. Scoping review

We conducted a scoping review based on the guidelines proposed by Kitchenham and Charters (2007) and Brocke et al. (2009), whose main steps are summarized as follows.

4.1.1. Search string

To identify suitable keywords, we conducted exploratory pilot searches. We refined our search string to get a comprehensive set of relevant

Table 2

Final search string.

String
<i>String without stems</i>   (privacy OR private OR security OR secret OR safety OR vulnerable OR protect OR preserve OR confidential OR sensitive OR reliability) AND ((smart OR connected OR clever OR intelligent OR anthropomorphic OR humanoid OR humanlike OR interactive OR cognitive OR social OR educational OR internet OR IoT OR online) W/5 (toys OR playthings OR dolls OR barbie))   <i>String with stems*</i>   (*privac* OR *private* OR *secur* OR *secre* OR *safe* OR *vulnerab* OR *protect* OR *preserv* OR *confiden* OR *sensitive* OR *reliab* AND ((smart* OR connected OR clever* OR intelligent* OR anthropomorph* OR humanoid* OR humanlike OR interactive OR cognitive OR social OR educati* OR internet OR IoT OR online) W/5 (toy OR toys OR plaything* OR doll OR dolls OR barbie))

* Stems were used to increase the chances of finding relevant papers.

papers. The final string (cf. Table 2) combines terms related to “privacy” with terms related to “smart” and “toys”. For both cases, we have included only those synonyms that have proven potentially useful in bringing relevant papers, through our exploratory searches. Keywords related to potential mitigation solutions were not included in the search string to ensure that papers addressing untreated risks could also be returned. Thus, only the research question 1 is directly represented in the search string, while the research question 2 is indirectly represented.

4.1.2. Databases

As a multidisciplinary topic, we expected to find relevant papers published in many fields. Thus, we did not limit ourselves to a specific number of journals or conferences. Instead, we searched for papers in two comprehensive databases: (1) Scopus (www.scopus.com) and (2) Web of Science (www.webofknowledge.com). Scopus is reported as the largest database of peer-reviewed literature, including scientific journals, books and conference proceedings, with titles from more than 5000 international publishers, including major publishers such as Elsevier, IEEE, Springer, Wiley, Taylor & Francis, World Scientific, SAGE, Emerald and InderScience (Elsevier, 2017). Web of Science was also used since, in previous reviews conducted by our research group, it was helpful to find additional papers not found by Scopus, even in very rare cases.

4.1.3. Inclusion and exclusion criteria

To guide our selection of primary studies, we defined inclusion and exclusion criteria. As inclusion criterion, we used: (i) the paper discusses children's privacy issues associated with the use of smart toys; and (ii) the paper possibly proposes solutions to children's privacy issues associated with

¹ For the ‘and’ relationship between these two terms, we used the ‘within’ (W/n) operator, where query terms must be within a specified number of terms n, with n = 5. Using the ‘and’ operator, meaning that the two terms could be found any distance between them, would return an excessively large number of irrelevant results.

the use of smart toys. As exclusion criteria, we defined: (i) the paper is not fully published in English; (ii) the work is published only as an abstract or extended abstract, not as a full paper or at least a short paper; and (iii) the paper is not a peer-reviewed scientific research work².

The survey was conducted on January 20, 2019 and again on March 15, 2019 to look for additional results. Altogether, our search resulted in 194 records, applying the search string to title, abstract and keywords in both databases (as summarized in Fig. 1). Duplicates were removed (39 records), resulting in 155 papers. Then, we analyzed the relevance of each paper by its title, keywords and abstract, applying the inclusion and exclusion criteria to eliminate those clearly irrelevant papers. This first analysis resulted in a set of 65 papers, which were then read in more detail, reapplying the inclusion and exclusion criteria based on the full text. As a result, we got a set of 22 relevant papers. When analyzing the references of these 22 papers, in a snowball strategy, we identified four additional papers. We used this final set of 26 papers as our primary studies to support subsequent content analysis.

4.2. Content analysis

To answer our research questions based on the primary studies identified as a result of our systematic search procedure, we combined qualitative and quantitative content analysis. Content analysis refers to the analysis of texts and the existence of specific categories of terms (Bryman, 2012). Quantitative content analysis is a positively-oriented approach, based on predefined categories. Qualitative content analysis, on the other hand, requires the inference of categories interpretively.

4.2.1. Quantitative content analysis

For the quantitative analysis, we used as a reference the taxonomy proposed by Loukil et al. (2017) in their systematic review on *privacy-aware in IoT applications*. This is the taxonomy with purpose more related to our study, considering the smart toys as a type of IoT. We used only four facets from the seven in the original classification as our study has a more specific aim. While they were interested in multiple analyzes (including also: *application domain*, *architecture types* and *life-cycle phases*), we are specifically concerned with the types of privacy and security-related risks and solutions. Fig. 2 presents the adapted taxonomy used herein. Besides not using some facets, we grouped *security properties* and *security requirements* as a single sub-facet of *Information security* to make the taxonomy more suitable for our purposes.

As a result, the classification used in the quantitative analysis has only two facets. The former (*ISO privacy principles*) is related to our first research question – the privacy risks involved in using smart toys, including threats and vulnerabilities. The latter (*Privacy preserving techniques*) is related to our second research question – solutions to mitigate privacy risks involved in using smart toys. Loukil et al. (2017) relied on a wide ISO standard ISO/IEC (2011) to define the privacy principles used in their classification.

We assumed that smart toy makers should adhere to this set of privacy principles so as not to pose risks to child users. Thus, we evaluated the primary studies to identify which were presenting concerns on which of these principles. There are 11 privacy principles, one of which – information security – is divided into six other principles specifically related to security, referenced as security properties and requirements. This second level of classification is important as information security is usually one of the most important aspects to ensure the privacy of information. As for privacy preservation, Loukil et al. (2017) considered five main techniques: two of the ‘data perturbation’ type (*noise addition* and *anonymization* protection) and three of the ‘data restriction’ type (*access control*, *cryptographic* protection and *blockchain*-based).

For the quantitative data analysis, all 26 primary studies were

analyzed using keywords that could show the concern of the authors regarding each subject in Fig. 2. As a quantitative analysis, each term was accounted for in the data extraction for a given paper only when a direct (i.e., clear and explicit) concern manifestation was found in the paper on the corresponding term.

4.2.2. Qualitative content analysis

The classification raised through the quantitative content analysis is driven to technical risks and solutions, an effect delivered by the taxonomy adopted. Although important for our study, this partial contribution is focused on aspects aimed at the public specialized in information security and privacy. The taxonomy used, while applicable to the context of the smart toy, relies on technical concepts of security and privacy, which are used to both identify risks and address possible mitigation solutions.

We carried out a qualitative content analysis to produce also a classification of risks and solutions more aligned to the application area. Our interest here was to identify privacy risks and possible solutions more representative for the context of smart toys. We sought to find risks more tangible to child users as well as solutions more directly targeted to this type of user. For this case, a qualitative content analysis was necessary because no suitable taxonomy was previously identified specifically for this purpose. Thus, this classification had to emerge from the analysis of the 26 primary studies. For this, a careful reading of all the studies was done so that such risks and solutions could be identified. First, a broad set was identified, including a series of synonyms and similar expressions. Then, we worked on this initial set, through several iterations, until we reduced it to a smaller set that generically reflected all the primary studies.

5. Results and findings

Table 3 summarizes the 26 primary studies identified. We believe that these papers represent the vast majority of studies published until the beginning of 2019 that address the risks involved in children’s privacy associated with the use of smart toys as well as possible solutions discussed so far for these risks. Considering the systematization followed in our search for papers, there is only a small chance of missing relevant papers.

Fig. 3 shows graphically the time evolution of the primary studies found. Although the first paper to mention this problem was published in 2009, the vast majority of papers were published as of 2016 (about 88% of them), with a highlight to 2018 (with 35% of the papers). In fact, it is notorious that the concept of smart toys started to become better known around 2015, especially after Hello Barbie was launched, followed by various media reports on both its characteristics and risks involving children’s privacy. The numbers are still low for 2019 probably because the search was conducted in the first months of the year.

Regarding vehicle type, most of the papers were published in conference proceedings, which is common in technology and computing fields. However, an increase occurred in the number of papers published in journals in 2018, which may show a maturity gain for research in this area. There is no focus on any conference or journal, except for a conference that has published three papers and a conference and a journal with two papers each. In fact, Table 4 shows a broad distribution of vehicles in different areas of knowledge, which is quite reasonable because of the highly multidisciplinary nature of the problem in question. There are quite technical vehicles (involving, for example, *dependability in sensor*, *cloud and big data*; *ubiquitous computing* and *IoT*) whereas others address the interface between social and technical aspects (e.g., *ethics in engineering*, *science and technology*; *big data and society* and *law and technology*).

Another aspect that shows the multidisciplinary of the topic addressed in this scoping review is the origin of the authors of the primary studies. An analysis of the authors affiliations shows a great diversity of areas of activity, as summarized in Table 5. Only the areas of activity of

² This exclusion criterion was applied to avoid poor quality primary studies.

Fig. 1. Summary of the search for primary studies.

Fig. 2. Taxonomy for data extraction and classification (quantitative content analysis), adapted from Loukil et al. (2017).

Table 3

Primary studies (VT: Vehicle Type; J – Journal; C – Conference).

ID	Title	Authors-Year	VT
1	Security and privacy analyses of internet of things children's toys	Chu et al. (2019)	J
2	Modeling Privacy Preservation in Smart Connected Toys by Petri-Nets	Yankson et al. (2019)	C
3	Playing with danger: A taxonomy and evaluation of threats to smart toys	Shasha et al. (2018)	J
4	Children's digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture	Smith and Shade (2018)	J
5	Toys that talk to strangers: A look at the privacy policies of connected toys	Chowdhury (2018)	C
6	Smart doll: Emotion recognition using embedded deep learning	Espinosa-Aranda et al. (2018)	J
7	Cyberthreats under the bed	Kshetri and Voas (2018)	J
8	A preliminary study of Hello Barbie in Brazil and Argentina	Fantinato et al. (2018)	J
9	Smart bears don't talk to strangers: Analysing privacy concerns and technical solutions in smart toys for children	Demetrou et al. (2018)	C
10	Security tests for smart toys	Carvalho and Eler (2018)	C
11	Security requirements and tests for smart toys	Carvalho and Eler (2018a)	C
12	A framework for preventing the exploitation of IoT smart toys for reconnaissance and exfiltration	Haynes et al. (2017)	C
13	Towards a comprehensive analytical framework for smart toy privacy practices	Mahmoud et al. (2017)	C
14	Security & privacy in smart toys	Valente and Cardenas (2017)	C
15	Protecting privacy in the era of smart toys: Does Hello Barbie have a duty to report	Moini (2017)	J
16	Security requirements for smart toys	Carvalho and Eler (2017)	C
17	Toys that listen: A study of parents, children, and internet-connected toys	McReynolds et al. (2017)	C
18	Towards a privacy rule conceptual model for smart toys	Rafferty et al. (2017)	C
19	A study of privacy requirements for smart toys	Hung et al. (2016)	C
20	A glance of child's play privacy in smart toys	Hung et al. (2016b)	C
21	The Internet of toys	Holloway and Green (2016)	J
22	Your New Best Frenemy: Hello Barbie and Privacy Without Screens	Jones (2016)	J
23	Can (and should) Hello Barbie keep a secret?	Jones and Meurer (2016)	C
24	Hacking and securing the AR.Drone 2.0 quadcopter: Investigations for improving the security of a toy	Pleban et al. (2014)	C
25	Risk mitigation strategies for mobile Wi-Fi robot toys from online pedophiles	Yong et al. (2011)	C
26	A spotlight on security and privacy risks with future household robots: Attacks and lessons	Denning et al. (2009)	C

Fig. 3. Distribution of primary studies per vehicle type and per year.

Table 4

Themes of the vehicles (conferences and periodicals) in which the primary studies were published.

Big Data and Society	Communication Research and Practice
Cloud Computing and Security	Dependability in Sensor, Cloud, and Big Data Systems and Applications
Computer	Engaging Science, Technology, and Society
Future Technologies	Enterprise Information Systems
Information Systems	Ethics in Engineering, Science and Technology
Internet of Things	Human Factors in Computing Systems
Law and Technology	Internet of Things – Security and Privacy
Social Computing	Living in the Internet of Things: Cybersecurity of the IoT
Sustainable Cities and Society	Mobile Devices and Multimedia: Enabling Technologies Alg. and App.
Symmetry	Privacy, Security, Risk and Trust
System Sciences	Socio-Technical Aspects in Security and Trust
Ubiquitous Computing	

each institute (or school, department etc.) informed in the authors affiliations are presented in the table, without the type of institute, to facilitate the analysis. In addition, each institute was considered only once in this analysis, regardless of the number of authors and papers coming from it. In total, there are 28 institutes. Much of them are institutes related to general aspects of technology, computing, engineering, systems, and information systems. However, we can highlight those related to human subjects, such as law, social sciences, arts and humanities, and business and economics. In addition, there are still those naturally multidisciplinary involving mixed subjects such as business and IT, data science and society, informatics and media, culture and technology. Finally, one area is cybersecurity, directly linked to the topic covered in this scoping review.

Still as a general characterization of the primary studies, Table 6 presents a summary of the research methods adopted by the authors of each paper. We identified different types of research methods applied. In the vast majority of papers, authors apply two or more methods together. The classification presented here is probably not accurate as several authors did not present the characterization of the research method adopted. Thus, we had to infer this information from the description of their work for analysis and comparison purposes. As a result, the content of Table 6 represents our view of the research methods applied. Many works were classified as *design science* because they propose some type of artifact (i.e., methods, techniques, guidelines, conceptual models, taxonomies, policies etc.).

Some of these artifacts were used in *experiments* while the others were only discussed from a theoretical point of view or with illustrative examples. In addition, some of these artifacts were proposed based on *documentary* research, using regulations, privacy policies and media

news. As an alternative to artifact proposition, many researchers conducted *case studies*, which would be highly expected considering the nature of the problem we are studying. There were case studies with *experimental* purposes, aiming, for example, to find privacy and security breaches in some smart toys. There were also case studies with a *documentary* nature, in which the researchers investigated, for example, news content, privacy policies and regulations of different types to carry out analyses on this context. Only one study conducted a *survey* to hear the opinion of potential consumers and only one work conducted *interviews* with parents after a session of use of toys with pairs of parents and children, which seems very little considering the context of our problem here. Finally, there were two papers that used also *expert opinion* as part of their research method.

In the following, we present the content extracted from the 26 primary studies.

5.1. Technical risks and proposed solutions

5.1.1. Identified technical risks – privacy principles and information security

Fig. 4 shows the classification of the 26 primary studies according to the concerns expressed by the authors on the 11 privacy principles. The data presented in this chart reflects the researchers' main concerns on children's privacy risks in using smart toys. Some of these risks are only briefly mentioned in some papers, with shallow coverage, while others have a deep coverage. Thus, for a better characterization, data extraction considered whether the paper treats a particular risk in a deep or shallow way.

Fig. 4 shows different levels of interest and concern in primary

Table 5

Areas of the authors activity, according to their affiliations in their papers.

Business and IT	Arts and Humanities	Arts, Sciences and Humanities
Cybersecurity	Business and Economics	Communication, Culture & Technology
Information	Business and Law	Computer Science and Engineering
Information	Computer Science	Computer Science and Software Engineering
Law	Computer Science	Engineering & Computer Science
Social Sciences	Data Science and Society	Information Systems Engineering
Social Sciences	Electronic Engineering	Information Systems Security Management
Tech Policy	Informatics and Media	Science, Technology & International Affairs
Technology	Technological Innovation	Vision and Intelligent Systems
Telecooperation		

Table 6

Research methods adopted in the primary studies.

ID	Authors-Year	Design Science	Case Study	Experimental/Simulation	Documentary	Survey	Interviews	Expert Opinion
1	Chu et al. (2019)		x	x	x			
2	Yankson et al. (2019)			x				
3	Shasha et al. (2018)	x		x				
4	Smith and Shade (2018)				x			x
5	Chowdhury (2018)		x		x			
6	Espinosa-Aranda et al. (2018)	x		x				
7	Kshetri and Voas (2018)				x			x
8	Fantinato et al. (2018)					x		
9	Demetzou et al. (2018)	x			x			
10	Carvalho and Eler (2018)	x			x			
11	Carvalho and Eler (2018a)	x			x			
12	Haynes et al. (2017)	x		x	x			
13	Mahmoud et al. (2017)	x		x	x			
14	Valente and Cardenas (2017)			x				
15	Moini (2017)	x						
16	Carvalho and Eler (2017)	x			x			
17	McReynolds et al. (2017)			x			x	
18	Rafferty et al. (2017)	x						
19	Hung et al. (2016)	x			x			
20	Hung et al. (2016b)				x			
21	Holloway and Green (2016)		x		x			
22	Jones (2016)		x					
23	Jones and Meurer (2016)			x				
24	Pleban et al. (2014)		x					
25	Yong et al. (2011)	x						
26	Denning et al. (2009)			x				

studies. The three most frequently found risks refer to: (1) the way in which the data is used (including its retention and mainly its disclosure); (2) the need for consent for any type of data operation to be performed (including offering different options); and (3) the need for broad transparency by smart toy makers so that the child guardian has an extensive knowledge of what is involved in the operations with the child's data. These risks refer to the first three principles in Fig. 4: *Use, retention and disclosure limitation*; *Consent and choice*; and *Openness, transparency and notice*. These three principles were at least shallowly addressed by at least 20 of the 26 primary studies and deeply covered by at least 11 papers. Analyzing these studies, we can easily see a pattern of concern from the authors, who express a clear interest in these basic risks to smart toy privacy, showing that even these basic risks are not being properly addressed by smart toy makers. Some of these authors' recurring concerns relate to the following issues: whether parents know exactly what child's data is collected; whether parents are properly notified; whether there is transparency in the privacy policies of smart toy makers; whether consent actions work as expected; what exactly is done with the child's PII; whether data is kept stored after use or discarded; and whether there is a risk of improper disclosure of child users' PII.

The fourth principle in number of concerns' occurrences in Fig. 4 is *information security*, which is, in fact, an average of the six sub-principles presented in Fig. 5. The six sub-principles in Fig. 5 had different levels of occurrence each one in the 26 primary studies; what appears in Fig. 4 is an average value considering all of them for each primary study. In fact, one of the six sub-principles – *Confidentiality* – is the most

present concern in the 26 primary studies, deeply covered in 16 of them. On the other hand, *integrity*-related concerns appear in only seven papers, mostly shallowly covered only.

These six data security-related principles are addressed in the 26 primary studies also as a reflex of how authors have positioned themselves on the risks related to smart toy-related children's privacy. The majority expressed concerns on the most latent risk, namely the *confidentiality* of the child's data. This shows that even the most basic principles have not been adequately addressed by smart toy makers. The following most mentioned concerns are on those easily and directly related to maintaining confidentiality, i.e., *authorization* and *authentication*. On the other hand, risks related to *integrity*, *availability* and *accountability* are not yet part of the main concerns of researchers, perhaps because data confidentiality and data privacy are not easily and directly connected to these three principles. However, all principles of information security are interconnected with similar importance to ensure privacy. For example, a lack of integrity in data stored by a toy company can indirectly facilitate data leakage. Even accountability that appears with a larger number of occurrences by the authors still refers to shallow manifestations in each paper in which they appear.

After the first four privacy principles (cf. Fig. 4), the remaining seven did not have many occurrences in the primary studies. The principle *collection limitation* stands out with eight deep manifestations. A reasonable number of authors have expressed concerns on the amount of data collected by toy companies larger than necessary. On the other hand, *data minimization*, the extreme of the principle of collection limitation, was the least mentioned. Minimizing data means that

Fig. 4. Classification of papers by ISO privacy principles.

Fig. 5. Classification of papers by security properties and requirements (Information security sub-principles).

there should be a limitation on data processing, not just data collection. In general, more specific privacy concerns, which are usually not obvious, have not yet been addressed. For example, while many authors have dealt with *disclosure limitation*, *consent* and *transparency*, few have addressed *individual participation and access*, which refers to giving users the right to review, change, amend and remove their data in a simple manner whenever desired.

5.1.2. Proposed technical solutions – privacy preserving techniques

Although there are many privacy risks (cf. Fig. 2), only five privacy preservation techniques are clearly defined in the basic taxonomy used by our study. Per Fig. 6, only two techniques of the *data restriction* type received a reasonable number of mentions – *Cryptographic* and *Access control*. The high number of cryptographic-related solutions reflects one of the researchers' biggest concerns – the risk of confidentiality breach. Several researchers addressed in their papers the need to encrypt children's PII, and possibly related data, when using smart toys. Researchers are also very interested in proposing ways to control the access to toys only to those authorized. Access control can be treated with specific levels and objectives. One form of access control specific to the context of smart toys is through parental control tools, which are addressed in some of these papers as a proposed solution to reduce the risks to children's privacy.

Techniques related to *Anonymization* and *Noise addition* were merely mentioned as solutions only in some primary studies. It remains to be seen whether these techniques of the *data perturbation* type are not appropriate for smart toys or whether they have not yet been considered by researchers in this context. At least for the general IoT context, according to the systematic review conducted by Loukil et al. (2017), the number of solutions found related to anonymization was about 60% greater than to access control. This scenario is very different from the one found for smart toys. Finally, solutions related to blockchain were not mentioned in any paper. However, this could be an expected result as blockchain is a very recent technique. Even for the more general IoT context, very few papers mentioned blockchain as a possible solution to privacy risks in the systematic review conducted by Loukil et al. (2017).

Fig. 6. Classification of papers by privacy preserving techniques.

5.1.3. Cross-analysis between the risks and proposed solutions

Fig. 7 shows a cross-analysis between the data presented in Figs. 4 and 5 and the data presented in Fig. 6, i.e., a cross-analysis between the risks identified and the types of solutions proposed in the primary studies. The data in Fig. 7 show more clearly what could have been inferred from previous data: what are the main concerns addressed by researchers in terms of risks to children's privacy and what types of solutions could be used to mitigate such risks. The graph shows the number of papers for which a particular pair of principles occurs. For example, the principles *data minimization* and *anonymization* are present in the same paper for only three of the 26 primary studies. Still, some important analysis can be conducted. For example, at least 14 papers mention the risks associated with *Consent and choice*, *Use, retention and disclosure limitation*, *Openness, transparency and notice*, *Information security – Confidentiality* and *Information security – Authorization* as well as possible solutions associated with *Access control* and *Cryptographic*. This does not mean that these topics are necessarily connected in these papers. However, some strong signals gotten are, for example, that consent risks are viewed as possibly addressed by access control techniques or that authorization risks should be addressed through cryptographic techniques.

5.2. Domain-specific risks and proposed solutions

Table 7 shows the results of the qualitative content analysis of the primary studies. Through our qualitative analysis, a new classification of risks and proposed solutions was raised in addition to the one presented in Fig. 2. While that one was driven by technical risks of the IoT environment in general, this one is geared towards risks closer to the specific domain being addressed, i.e., smart toys and child users.

Not all primary studies address some domain-specific risk. Rather, some naturally emphasize technical risks as explored in Figs. 4 and 5. Others mention domain-specific risks but rather superficially, only as a basic motivation for their technical work. On the other hand, some works seek a social impact strand and explore the risks that can directly affect children using smart toys. Table 7 present our resulting categorization of these domain-specific risks. The most common risk

Fig. 7. Cross-analysis between risks identified (Privacy principles) and proposed solutions (Privacy preserving techniques).

pointed out by the authors is *data breach*, found in almost all papers. Different types and levels of data breach are grouped into this category, including: illegal or inappropriate data disclosure, data leakage, data spill, data theft, stolen data and data misuse. In fact, this type of risk is not fully domain-specific, as the others presented in Table 7; however,

most authors highlight the specificities of child data and hence of the child data breach. Considering more tangible risks, many authors raised concerns on the *physical safety* of child users. Children may experience problems related to harassment, stalking, grooming, sexual abuse, exploitation, kidnapping, pedophilia and other types of violence. Similar

Table 7

Domain-specific risks and proposed solutions.

ID	Domain-specific risks	Domain-specific proposed solutions
1	Data breach; physical safety	Sharing lessons learned; evaluation framework
2	Data breach; physical safety	Recommendations for toy makers
3	Data breach; physical safety; psychological safety	Evaluation framework
4	Data breach; breach of children's privacy ethical rights; children's advertisement	Sharing lessons learned
5	Data breach	Recommendations to improve privacy policies
6	Data breach	Recommendations for toy makers
7	Data breach	Sharing lessons learned
8	Data breach; physical safety	Parental control
9	Data breach; physical safety; breach of children's privacy ethical rights	Recommendations for toy makers
10	Data breach	Recommendations for toy makers; parental control
11	Data breach	Recommendations for toy makers; parental control
12	Physical safety; psychological safety	Evaluation framework
13	Data breach	Evaluation framework
14	Physical safety; psychological safety	Recommendations for toy makers
15	Breach of children's privacy ethical rights	Recommendations for lawmakers
16	Data breach	Recommendations for toy makers; parental control
17	Data breach; breach of children's privacy ethical rights	Recommendations for toy makers; recommendations for lawmakers; parental control
18	Data breach; physical safety	Recommendations for toy makers; parental control
19	Data breach; physical safety	Recommendations for toy makers; recommendations for lawmakers; parental control
20	Data breach; physical safety	Recommendations for toy makers; parental control
21	Data breach; data breach; unauthorized remote control	Recommendations for lawmakers
22	Data breach; breach of children's privacy ethical rights; psychological safety	Recommendations for toy makers; recommendations to improve privacy policies
23	Data breach; psychological safety	Recommendations for toy makers
24	Data breach; unauthorized remote control	Recommendations for toy makers
25	Physical safety	Recommendations for toy makers; recommendations for parents
26	Spying; unauthorized remote control; psychological safety	Recommendations for toy makers

to this, there are concerns on *psychological safety*, since children may experience problems related to blackmail, insults, confidence loss, trust loss and bullying. A less prominent risk is the *dataveillance*, i.e., data surveillance, which can be carried out by the toy company itself, by the government or by unauthorized third parties. Also not very prominent, there is the risk of *remotely controlling the toy* without authorization, which can be done, for example, by vandalism or to steal the toy. There is also the risk of *inappropriate child-targeted advertising campaigns* mentioned only once. Finally, there is the risk of *spying* (surveillance), which can be done even by the parents themselves. However, in the latter case, there is controversy over whether this should be considered a risk or a solution; in any case, this is indicated in Table 7 as *breach of children's privacy ethical rights*.

The domain-specific risk categories in Table 7 are not mutually exclusive. There are interrelated risks. For example, many data breach risks are motivating for physical safety risks. Unauthorized remote controlling of a toy can lead physical or psychological safety risks. The complexity of the risks involved is such that we could not produce a mutually exclusive taxonomy or a model of relationships among the categories.

From the solutions perspective (cf. Table 7), not all primary studies aim to present domain-specific solutions. Some papers intend to present only analytical contributions and not concrete solutions (as presented in Table 6, on the research methods adopted). In these cases, only a few possible general recommendations are to be expected, which are pointed out in Table 7 as *Sharing lessons learned*. Other works naturally focus on more technical solutions, related to the principles summarized in Figs. 4 and 5. However, Table 7 seeks to classify all works from the point of view of proposed solutions specific to the domain of smart toys and child users. The proposed solutions differ greatly from each other. We aimed to aggregate the proposed solutions into major categories, most of them related to recommendations: *recommendations for toy makers*, including techniques, methods, models, frameworks, best practices, guidelines etc. useful for developers to produce smart toys under security and privacy regulations; *recommendations for lawmakers*, including suggestions and recommendations for improvements related to laws, legislation and regulations associated with this context; *recommendations to improve privacy policies*, including suggestions for toy companies to improve communication on their privacy policies, such as increasing their transparency; and *recommendations for parents*, which was mentioned only once and aims to list the actions that parents can take to avoid problems. Another important type of solution are the *evaluation frameworks* proposed to support the analysis of smart toys and possibly their classification based on their compliance with safety and privacy regulations. Finally, a very specific solution for this domain, and mentioned by many authors, is the need and the importance of adequate *parental control* tools.

Fig. 8 presents grouped and hierarchical views of the risks and proposed solutions shown in Table 7. This figure provides clear visual information on which types of risks and proposed solutions are most commonly addressed in primary studies. The primary studies associated with each category of the graph are presented in brackets, with some studies present in more than one category.

6. Discussion

6.1. Smart toy-related children's privacy risks

The results show that there are many risks and many concerns of researchers regarding smart toys-related children's privacy. The IoT environment is itself susceptible to such risks. However, with IoT toys, the user being a child is a relevant aggravating factor, as pointed out by researchers analyzed. According to Hung et al. (2016), children do not understand the concept of privacy, which makes it easier for criminals and makes it difficult for their guardians, smart toy makers, lawmakers, researchers etc. Child users exhibit a varying level of awareness

regarding their online activities and understanding of privacy risks (Hung et al., 2016). Children may disclose as much information to people they can trust (Hung et al., 2016), which will be exploited by online predators. According to Moini (2017), children seem to be open to trading their privacy in return for gaining access to social media and other online services, which can be easily transferred to the smart toys world. And the risk can be greater the lower the age of the child. According to a study conducted by Shasha et al. (2018), with 11 smart toys analyzed, the toys for younger children collected more PII than those toys for older children. Children's data is widely considered sensitive and should be treated with extreme care by law and legislation (Hung et al., 2016).

The current scenario is that toy companies are not taking responsibility for privacy and security flaws (Holloway and Green, 2016). According to Kshetri and Voas (2018), for now, parents are solely responsible for monitoring the use of smart toys and protecting children's data. Parents are tasked to act as data proxies and supervisors for children (Smith and Shade, 2018). Instead, toy companies are using complicated terms and conditions to shift responsibility to consumers (Holloway and Green, 2016). For example, Chowdhury (2018) shows that privacy policy documents of 15 toy companies analyzed claimed to have privacy measures in place, what might make parents feel relieved to trust the companies to be responsible caretakers of their children. However, they also show that the privacy policies of almost all the companies accepted that their databases might not be secure enough to prevent data breaches (Chowdhury, 2018). Besides deciding whether or not to allow the collection of certain data, there is still data that can be indirectly inferred by smart toys and toy companies, such as consumption habits. Smart toys are capable to gather significant amount volunteered and non-volunteered data, which lacks privacy considerations (Yankson et al., 2019).

The priority has been neither security nor privacy in smart toys. According to Kshetri and Voas (2018), experience suggests many smart toy makers ignore or only pay lip service to security and privacy concerns. In part because of limited technology budgets, many smart toy makers have weak security and privacy policies (Kshetri and Voas, 2018). Toy makers sometimes fail to make serious efforts to strengthen security and privacy even after experiencing significant attacks (Kshetri and Voas, 2018). However, smart toys-related privacy and security scandals could compromise the future of this design trend in the industry, such as by affecting sales and the distribution of these products to a worldwide audience (Fantinato et al., 2018).

Our strategy of addressing two levels of risk allowed us to raise a comprehensive socio-technical view of the types of smart toys-related privacy and security risks. In technical terms, the adopted IoT risk classification taxonomy shows researchers are more concerned with certain types of risks than others. Many authors mention risks related mainly to data collection, disclosure and leakage. The largest number of occurrences of this type of risk is likely to be caused by the novelty of a toy connecting to the internet to exchange sensitive data with a private company in a non-necessarily controlled manner. In a systematic study, Mahmoud et al. (2017) found three most issues that make smart toys vulnerable: a potentially excessive collection of children's private information, incomplete/lack of information on data storage location and legal compliance and over-privilege with the potential to leak child's private information in most apps.

To provide the most relevant services to the user, it is natural that personal and context information should be collected. While allowing context data to be collected for services can prove to be of great benefit to users, there is a tradeoff between utility and privacy (Rafferty et al., 2017). However, personalization is proposed as the benefit of disclosing data (Smith and Shade, 2018). Companies posit that users are responsible for their own security; however, users are often threatened of losing services if they exercised control of their privacy, for example, if users did not share data with third parties (Chowdhury, 2018).

While most risks were highlighted here because of the connectivity

Fig. 8. Hierarchical view on domain-specific risks and proposed solutions.

of toys to the cloud, there are also risks associated with big data. According to [Smith and Shade \(2018\)](#), big data has had a prominent role in reducing children's privacy rights, as responsible for targeted marketing and advertisement actions. Advertising and promotional culture are present in children's digital playgrounds ([Smith and Shade, 2018](#)). This is supported by machine learning techniques, although the algorithms that power digital playgrounds remain opaque for parents ([Smith and Shade, 2018](#)). With the extensive use of databases, the security of user information thus relies on the security of the databases of a connected toy company or of the third parties that the company shares information with ([Chowdhury, 2018](#)). Of all 11 ISO privacy principles, one of them is specifically dedicated to information security, which has been addressed here split into six sub-principles: three with more concerns from the researchers – confidentiality, authorization, authentication; and the other three less mentioned by them in their papers – accountability, availability and integrity. Even simple and well-known security practices, such as transport-layer encryption, are neglected by developers ([Chu et al., 2019](#)).

From the social point of view, we addressed domain-specific risks, i.e., risks more related to smart toys instead of general IoT risks. The largest number of authors pointed out concern about the data breach. While this may be considered a general IoT risk, the specificities of child data make child data breaches a much more severe social issue. The type of user in conjunction with the type of product can make the combination explosive: [Hung et al. \(2016b\)](#) found examples of unintended phrases in Hello Barbie's repertoire that might encourage children to reveal private information indirectly. This is especially dangerous as children are often unaware that others might hear what was said to the toy ([McReynolds et al., 2017](#)). On the other hand, parents are not sure about what data would be retained by companies ([McReynolds et al., 2017](#)).

Many examples of physical and psychological safety risks have been listed by researchers in a list that appears to be far from extensive. The creativity of criminals is certainly greater. Concerns with harassment, stalking, grooming, sexual abuse, exploitation, kidnapping, pedophilia and other types of violence were raised. [Valente and Cardenas \(2017\)](#) cite the risk of criminals taking the remote control of a toy and using it to perform tasks inside a house or else asking a child to do so such as opening the house door. Examples of concerns with psychological safety risks include blackmail, insults, confidence loss, trust loss and bullying. As an example of psychological impact, usually unrelated to privacy risk, [Jones and](#)

[Meurer \(2016\)](#) argue that over-sharing data among so many parties may negatively impact children's ability to trust while undermining parental authority in managing their child's data. [Pleban et al. \(2014\)](#) cite the risk of theft of the toy itself after criminals can take remote control of the toy which would be more likely with a drone, for example.

[Holloway and Green \(2016\)](#) mention the risk of corporate and government surveillance of children's activities and encroachments upon their data privacy and security, a risk not widely cited by other researchers. More mentioned by researchers is the risk of a breach of trust between parents and children because the parents themselves are spying their children. While the industry, some experts and some parents may understand some functionalities as a benefit, because they can care for their children even more; other experts and parents understand it as anti-ethical and as teaching children that no one is entitled to fully unique and inviolable privacy. The problem may lie in how private data is currently used. For example, the Hello Barbie records every single interaction, stores them on a ToyTalk system, and posts them to a parent's portal where they are stacked chronologically as pink audio files ([Jones, 2016](#)). Instead of parents having direct access to all recorded conversations, machine learning techniques should scan them to identify suspicious subjects and only then notify their parents, which would have access to the conversations only in those situations ([Moini, 2017](#)). Such a strategy would not eliminate all the aforementioned risks of possible data breaches.

Although it may seem that Hello Barbie is one of the most vulnerable products, because it is probably the most cited in the works, this should occur because it has become a reference for its category. In fact, according to the systematic comparison conducted by [Mahmoud et al. \(2017\)](#), it has proved less vulnerable, considering an average of the criteria considered by them. On the other hand, in the studies of [Haynes et al. \(2017, 2018\)](#), Hello Barbie was not the best rated, but neither was the worst.

Not only do toys have issues, but also the privacy policies that come with them. For example, the lack of easily accessible privacy policies and complexity of the policies hinder parents' ability to fathom potential risks of smart toys and the companion apps for their children ([Mahmoud et al., 2017](#)). [Chowdhury \(2018\)](#) show that most toy makers do not mention or clarify in their privacy policy documents how their toys protect user's security and privacy. Issues with privacy policies as well as the other types of issues highlighted above are largely due to the lack of appropriate government actions. Government initiatives have not yet been effective in addressing these issues. After examining

regulatory initiatives to protect children (Kshetri and Voas, 2018), regulatory efforts to address this issue are incipient, a gap that various government agencies and consumer watchdog groups are trying to fill. Holloway and Green (2016) also raised concerns on the lack of regulatory direction relating to children's data privacy and security within this market niche.

6.2. Solutions to mitigate smart toy-related children's privacy risks

There is a menacing scenario according to the researchers in terms of smart toys-related privacy and security risks. Nevertheless, despite their potentially serious impact, most existing vulnerabilities are easily correctable (Chu et al., 2019). They are most likely caused because of substantial developer error, apathy, or ignorance of privacy and security best practices. Maybe toy makers are not very concerned about security and privacy issues as they are just toys when it should be exactly the opposite as *they* are just kids. To properly address these problems, toy makers need to include this concern at the very earliest stages of the smart toy development lifecycle. For example, Yankson et al. (2019) show the importance of addressing privacy descriptor elements when modeling the data flow during requirements analysis and system modeling.

However, the current scenario shows that when considering children's privacy solutions to develop new smart toys, developers need to understand that safety and security of children's data require going beyond the basic *opt-in-opt-out* paradigm of data privacy (Holloway and Green, 2016). Smart toys products can be even more vulnerable to cyber attacks than other IoT devices, providing an often-overlooked entry point for hackers (Kshetri and Voas, 2018), showing that extra cares must be taken.

Aiming to provide privacy guarantees, first, a good technical solution related to information security should be met. This common scenario for the IoT environment is naturally applied for IoToys. However, as stated by several authors, specificities must be addressed. Although smart toys are considered a sub-area of IoT (Hung et al., 2016b), security should be addressed in a deeper way for this domain, because end users are children who often have little concern and awareness about privacy, not deciding about privacy policies. In addition, smart toys must be under the child's privacy rights, which may change according to the region and country (Carvalho and Eler, 2017). As generic security requirements are not fully appropriate since smart toys have an enlarged attack surface, Carvalho and Eler (2017, 2018a) proposed a set of security requirements specifically elicited for smart toys based in also specific security issues and threats.

Many technical solutions have been presented by the researchers, some incredibly punctual for very specific issues. These cases are usually the result of experimental studies in which concrete flaws and vulnerabilities have been demonstrated, while their corrections have also been presented as possible. As warned by some researchers, many of the necessary technical tools already exist as they are generic to the IoT domain. The technical solutions related to encryption and access control have been more mentioned so far, both of the data restriction type. Techniques of data perturbation type have not been much mentioned by researchers (i.e., anonymization and noise addition), which differs from IoT in general.

Considering domain-specific solutions, at a social level, several recommendations have been presented. These recommendations are derived from different research methods; some are merely lessons learned or collections of insights, others result from more systematic studies such as case studies and experiments, while others are derived from detailed analyses of the legislation and privacy policies of certain smart toys. Moreover, there are recommendations specifically aimed at smart toy developers, others at lawmakers, while others at toy companies as responsible for developing privacy policies. In addition, some authors proposed evaluation frameworks to support the analysis of smart toys and possibly their classification based on their compliance with safety and privacy regulations which can be useful for developers, companies

and lawmakers. Finally, some authors show the need for parental control tools as the most domain-specific solution.

Most recommendations for developers, that is, toy makers, are comprised of technical recommendations, in the format of best practices, requirements, frameworks etc., such as those presented by Denning et al. (2009), Pleban et al. (2014), Hung et al. (2016), Valente and Cardenas (2017), Carvalho and Eler (2017), Carvalho and Eler (2018a), Carvalho and Eler (2018), Shasha et al. (2018), Demetzou et al. (2018). (Fantinato et al., 2018) are examples of authors who recommend no strictly technical solution as they suggest for toy makers to reduce privacy issues by improving parental control tools using data mining, a part of a more strategical solution.

Carvalho and Eler (2018a) argue that smart toys makers should provide parents with information on which actions they should take to ensure the security and safety of their children. The most complete solution proposed so far for this purpose is from Rafferty et al. (2017), which proposed a conceptual model to enable parents (or legal guardians) to provide consent through access rules that define that their child's data to be shared according to their privacy preferences. The model allows parents to systematically create privacy rules and receive acknowledgments regarding their children's privacy-sensitive data. This conceptual model is, in fact, a powerful basis for creating much more appropriate parental control tools than the simple setting tools currently offered (Fantinato et al., 2018). Many researchers lament how mediocre are the current parental control tools at the same time they highlight the potential that this type of solution presents to solve many of the risks presented in the form of an umbrella solution.

Considering that the risks exist because of the high connectivity of smart toys, Espinosa-Aranda et al. (2018) argue that avoiding sending so much processing to the cloud would be possible. They show that it is possible to perform emotion recognition through local processing in the toy using deep learning. While it is unreasonable to treat all processing as local, which would even go in the opposite direction of the modern world ubiquity, this corroborates directly with the ISO privacy principle of data processing minimizing.

Chowdhury (2018) recommended toy makers to explicit their privacy policies so parents can have more transparency to decide whether to buy smart toys for their children. For example, a Frequently Asked Questions (FAQ) with privacy items should accompany privacy policy documents to make it easier to see what and how information is collected, used and disclosed (Chowdhury, 2018).

According to Fantinato et al. (2018), toy safety guidelines, such as Health Canada's Safety Requirements for Children's Toys and Related Products, are out of date with the current innovations in smart toy technology. These guidelines concentrate on physical safety-related to traditional toys and do not consider recent developments in toy technologies, which now have a wide range of sensory and networking capabilities creating new privacy risks. It is expected that the contributions presented by the researchers are used by the public interest. Moini (2017), for example, proposed an amendment to COPPA to include the obligation of the smart toy (in fact, the company responsible for it, including computer technicians and service providers) to monitor and track suspicious recordings on critical matters such as sexual abuse to alert the parents. The IoToys is likely to become an increasingly important topic for public concern and discussion over the coming years (Holloway and Green, 2016). Policy development is already underway in the broader domain of the IoT in Australia, Europe and the USA, however, and it is to be hoped that further policy statements and initiatives occur (Holloway and Green, 2016). Lawmakers should help children, parents and toy makers become more aware of privacy issues, strengthen the existing children's privacy protections such as COPPA, and addressing the same issues with other internet-connected devices that are not toys but also used by children such as Siri, Amazon Echo and Alexa (McReynolds et al., 2017). Despite the incompleteness of these regulations, much is already covered by them. For example, data minimization, an important step for reducing privacy risks, is a data processing principle mentioned in Article 5(1c) of the GDPR that

obliges the data controller to process only personal data that are *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* (Demetrou et al., 2018).

Some authors contributed importantly by proposing evaluation frameworks (Mahmoud et al., 2017; Haynes et al., 2017; Shasha et al., 2018; Chu et al., 2019). Each one with their specific details, they have common aims: allowing stakeholders to evaluate and compare smart toys from a given set of criteria. These frameworks are very important because they allow the stakeholders to get a comprehensive view of both sets of existing risks and the quality of given smart toys. Haynes et al. (2017) suggested that the toy can be accompanied by a badge, classified as A+, A, B+, B or C, depending on the number of criteria satisfied.

6.3. Final considerations

If smart toys become more attractive to children and their sales increase considerably soon, both toy makers and privacy regulations are not yet ready to deal with the risks posed to children's privacy. While smart toys are not yet widely used by children around the world, children will still find smart toys as an important entertainment opportunity because they are excluded from many social media platforms due to age, by regulations adopted (e.g., Facebook, Twitter, Snapchat etc.). Smart toys should become increasingly popular as they acquire more technological capabilities with the power to attract the children of today's world. These same technological resources should increase their vulnerabilities relative to privacy risks. Children are by far more receptive to the adoption and use of new technologies than previous generations and express little or no concern about the privacy implications associated with the use of these technologies and devices. If today the problem is not so large because there are few children who use smart toys, it can become much bigger soon. That will depend on how smart toys will evolve to really attract kids and permeate their lives and how their manufacturers will be prepared to offer secure solutions.

7. Conclusion

This study aimed to review the scope of published work related to privacy issues in smart toys, focusing on the risks and proposed solutions. Two research questions were addressed. For the first research question - *which risks to children's privacy when using smart toys have been addressed?*, the most commonly mentioned technical risk is *data disclosure*, while from a domain-specific perspective, there is much concern on the *children's physical and psychological safety*. As for the second research question - *which mitigation solutions to children's privacy risks have been proposed?*, while several recommendations and solutions have been proposed, we did not identify a more frequent contribution type. We observed that many issues could certainly be mitigated most of the time with *existing, and even simple, solutions from the broader IoT context*, although many authors show that toy companies appear not to be concerned about this problem.

We proposed a two-level classification of risks and proposed solutions: a technical level (based on general IoT issues) and a domain-specific level (target at the domain of smart toys). As future work, a new smart toy privacy assessment framework may be proposed, with a purpose similar to those proposed by Haynes et al. (2017), Mahmoud et al. (2017), Shasha et al. (2018), Chu et al. (2019). However, this new framework could be much more systematic and comprehensive, involving the full classification taxonomy adopted in the study presented in this paper; consequently allowing more thorough evaluation studies.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRedit authorship contribution statement

Otávio de Paula Albuquerque: Investigation, Resources, Data curation, Writing - original draft. **Marcelo Fantinato:** Conceptualization, Validation, Methodology, Writing - original draft, Writing - review & editing, Visualization, Supervision, Project administration. **Judith Kelner:** Writing - review & editing. **Anna Priscilla de Albuquerque:** Writing - original draft, Writing - review & editing.

References

- Anki, 2019. Cozmo – Meet Cozmo. San Francisco, CA, USA. <https://anki.com/en-us/cozmo.html>.
- ASUSTeK Computer Inc, 2018. ASUS Zenbo – Your Little Smart Companion. ASUS, Taipei, Taiwan. URL: <https://zenbo.asus.com>.
- Bandai America Inc., 2019. Tamagorchi On – By Bandai America Inc. BANDAI Wiz, Tokyo, Japan <https://tamagotchi.com>.
- Ben-Joseph, E.P., 2018. Smart Toys for Every Age. Nemours' KidsHealth. <https://kidshealth.org/en/parents/smart-toys.html>.
- Brazil, 2018. GLPPD – General Law of Protection of Personal Data. URL: http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709compilado.htm. Brazil's National Congress and Presidency of the Republic.
- Bryman, A., 2012. *Social Research Methods*, forth ed. Oxford University Press, Oxford, UK.
- Cambridge Dictionary, 2019. PRIVACY – Definition in the Cambridge English Dictionary. Cambridge University Press, Cambridge, UK. URL: <https://dictionary.cambridge.org/us/dictionary/english/privacy>.
- Canada, 2018. PIPEDA – Personal Information Protection and Electronic Documents Act. URL: <https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf>. Minister of Justice, Canada.
- Carvalho, L.G., Eler, M.M., 2017. Security requirements for smart toys. In: Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS). SciTePress, Setúbal, Portugal. pp. 144–154. <https://doi.org/10.5220/0006337001440154>.
- Carvalho, L.G., Eler, M.M., 2018b. Security tests for smart toys. In: Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS). SciTePress, Setúbal, Portugal. pp. 111–120. <https://doi.org/10.5220/0006776101110120>.
- Carvalho, L.G., Eler, M.M., 2018a. Security requirements and tests for smart toys. In: Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS). Springer Verlag, Berling, Germany, pp. 291–312. https://doi.org/10.1007/978-3-319-93375-7_14.
- Chowdhury, W., 2018. Toys that talk to strangers: a look at the privacy policies of connected toys. In: Proceedings of the Conference of Future Technologies Conference (FTC). Springer Verlag, Berling, Germany, pp. 152–158. https://doi.org/10.1007/978-3-030-02686-8_12.
- Chu, G., Aphorpe, N., Feamster, N., 2019. Security and privacy analyses of internet of things children's toys. *IEEE Internet Things J.* 6, 978–985. <https://doi.org/10.1109/JIOT.2018.2866423>.
- Cognitoys, 2017. Cognitoys Dino Internet-Connected Smart Toy. New York, NY, USA. URL: <https://cognitoys.com/collections/all/products/cognitoys-dino>.
- de Albuquerque, A.P., Kelner, J., 2018. Toy user interfaces: systematic and industrial mapping. *J. Syst. Architect.* 97, 77–106. <https://doi.org/10.1016/j.sysarc.2018.12.001>.
- Demetrou, K., Böck, L., Hanteer, O., 2018. Smart bears don't talk to strangers: analysing privacy concerns and technical solutions in smart toys for children. In: Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT. IET, Stevenage, UK, pp. 1–7. <https://doi.org/10.1049/cp.2018.0005>.
- Denning, T., Matuszek, C., Koscher, K., Smith, J.R., Kohno, T., 2009. A spotlight on security and privacy risks with future household robots: attacks and lessons. In: Proceedings of the 11th International Conference on Ubiquitous Computing (UbiComp). ACM, New York, NY, USA, pp. 105–114. <https://doi.org/10.1145/1620545.1620564>.
- Dhar, T., Wu, T., 2015. Mobile computing toys: marketing challenges and implications. In: Hung, P.C.K. (Ed.), *Mobile Services for Toy Computing*. Springer Verlag, Berling, Germany, pp. 39–49. https://doi.org/10.1007/978-3-319-21323-1_3.
- Elsevier, 2017. Scopus – Content Coverage Guide. Elsevier B.V. Amsterdam, The Netherlands. URL: https://www.elsevier.com/_data/assets/pdf_file/0007/69451/0597-Scopus-Content-Coverage-Guide-US-LETTER-v4-HI-singles-no-ticks.pdf.
- Espinosa-Aranda, J.L., Vallez, N., Rico-Saavedra, J.M., Parra-Patino, J., Bueno, G., Sorci, M., Moloney, D., Pena, D., Deniz, O., 2018. Smart doll: emotion recognition using embedded deep learning. *Symmetry* 10, 1–18. <https://doi.org/10.3390/sym10090387>.
- EU, 2016. GDPR – General Data Protection Regulation. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. European Parliament and Council of the European Union.
- Fantinato, M., Hung, P.C.K., Jiang, Y., Roa, J., Villarreal, P., Melaisi, M., Amancio, F., 2017. A survey on purchase intention of hello barbie in brazil and argentina. In: Tang, J.K., Hung, P.C.K. (Eds.), *Computing in Smart Toys*. Springer Verlag, Berling, Germany, pp. 21–34. https://doi.org/10.1007/978-3-319-62072-5_3.
- Fantinato, M., Hung, P.C.K., Jiang, Y., Roa, J., Villarreal, P., Melaisi, M., Amancio, F., 2018. A preliminary study of hello barbie in Brazil and Argentina. *Sustain. Cities Soc.* 40, 83–90. <https://doi.org/10.1016/j.scs.2018.03.006>.
- Genesis Toys, 2019. i-Que Intelligent Robot. USA. URL: <https://www.genesis-toys.com/>

- ique-intelligent-robot.
- Genesis Toys, 2019. My Friend Cayla. USA. URL:<https://www.genesis-toys.com/my-friend-cayla>.
- Hasbro, 2019. Furby Official Website – Furby Boom. Pawtucket, Rhode Island, USA. URL:<https://furbys.hasbro.com/en-us>.
- Haynes, J., Ramirez, M., Hayajneh, T., Bhuiyan, M.Z.A., 2017. A framework for preventing the exploitation of IoT smart toys for reconnaissance and exfiltration. In: Proceedings of the 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS). Springer Verlag, Berlin, Germany, pp. 581–592. https://doi.org/10.1007/978-3-319-72395-2_53.
- Holloway, D., Green, L., 2016. The internet of toys. Commun. Res. Practice 1–14. <https://doi.org/10.1080/22041451.2016.1266124>.
- Hung, P.C.K., 2015. Mobile Services for Toy Computing, first ed. Springer Verlag, Berlin, Germany. <https://doi.org/10.1007/978-3-319-21323-1>.
- Hung, P.C.K., Fantinato, M., Rafferty, L., 2016. A study of privacy requirements for smart toys. In: Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS). AIS Atlanta, GA, USA, pp. 1–7.
- Hung, P.C.K., Iqbal, F., Huang, S.C., Melaisi, M., Pang, K., 2016b. A glance of child's play privacy in smart toys. In: Proceedings of the 2nd International Conference on Cloud Computing and Security (ICCCS). Springer Verlag, Berlin, Germany, pp. 217–231. https://doi.org/10.1007/978-3-319-48674-1_20.
- Hung, P.C.K., Tang, J.K.T., Kanev, K., 2017. Introduction. In: Tang, J.K., Hung, P.C.K. (Eds.), Computing in Smart Toys. Springer Verlag, Berlin, Germany, pp. 1–5. https://doi.org/10.1007/978-3-319-62072-5_1.
- Hung, P.C.K., Fantinato, M., Roa, J., 2019a. Children privacy protection. In: Lee, N. (Ed.), Encyclopedia of Computer Graphics and Games. Springer Verlag, Berlin, Germany. https://doi.org/10.1007/978-3-319-08234-9_198-1.
- Hung, P.C.K., Rafferty, L., Fantinato, M., 2019b. Toy computing. In: Lee, N. (Ed.), Encyclopedia of Computer Graphics and Games. Springer Verlag, Berlin, Germany 10.1007/978-3-319-08234-9_197-1.
- ISO/IEC, 2011. Information Technology—Security Techniques—Privacy Framework. ISO/IEC 29100:2011(E). first ed. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Geneva, Switzerland.
- Jones, M.L., 2016. Your new best frenemy: hello barbie and privacy without screens. Engag. Sci. Technol. Soc. 2, 242–246. <https://doi.org/10.17351/ests2016.84>.
- Jones, M.L., Meurer, K., 2016. Can (and should) Hello Barbie keep a secret? In: Proceedings of the 2016 IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS). IEEE, Washington, DC, USA, pp. 1–7. <https://doi.org/10.1109/ETHICS.2016.7560047>.
- Kanev, K., Oido, I., Hung, P.C.K., Kapralos, B., Jenkin, M., 2015. Case study: approaching the learning of kanji through augmented toys in japan. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 175–192. https://doi.org/10.1007/978-3-319-21323-1_9.
- Kapralos, B., Kanev, K., Jenkin, M., 2015. Advanced sound integration for toy-based computing. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 107–127. https://doi.org/10.1007/978-3-319-21323-1_6.
- Kitchenham, B., Charters, S., 2007. Guidelines for performing Systematic Literature Reviews in Software Engineering. Technical Report EBSE-2007-01. Software Engineering Group, School of Computer Science and Mathematics, Keele University and Department of Computer Science, University of Durham. UK. Version 2.3.
- Kshetri, N., Voas, J., 2018. Cyberthreats under the bed. Computer 51, 92–95. <https://doi.org/10.1109/MC.2018.2381121>.
- Loukil, F., Ghedira-Guegan, C., Benharkat, A.N., Boukadi, K., Maamar, Z., 2017. Privacy-aware in the IoT applications: a systematic literature review. In: Proceedings of the 25th International Conference on Cooperative Information Systems (CoopIS). Springer Verlag, Berlin, Germany, pp. 552–569. https://doi.org/10.1007/978-3-319-69462-7_35.
- Mahmoud, M., Hossen, M.Z., Barakat, H., Mannan, M., Youssef, A., 2017. Towards a comprehensive analytical framework for smart toy privacy practices. In: Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST). ACM, New York, NY, USA, pp. 64–75. <https://doi.org/10.1145/3167996.3168002>.
- Mattel, 2017. Hello Barbie. El Segundo, CA, USA. URL:<http://hellobarbiefaq.mattel.com>.
- McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., Roesner, F., 2017. Toys that listen: a study of parents, children, and internet-connected toys. In: Proceedings of the 2017 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI). ACM, New York, NY, USA, pp. 5197–5207. <https://doi.org/10.1145/3025453.3025735>.
- Moini, C., 2017. Protecting privacy in the era of smart toys: does hello barbie have a duty to report. Catholic Univ. J. Law Technol. 25, 281–318.
- Nelson, B., Olovsson, T., 2016. Security and privacy for big data: a systematic literature review. In: Proceedings of 2016 IEEE International Conference on Big Data (Big Data). IEEE, Washington, DC, USA, pp. 3693–3702. <https://doi.org/10.1109/BigData.2016.7841037>.
- Ng, G., Chow, M., Salgado, A.D.L., 2015. Toys and mobile applications: current trends and related privacy issues. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 51–76. https://doi.org/10.1007/978-3-319-21323-1_4.
- NIST, 2010. Guide to protecting the confidentiality of personally identifiable information (PII). URL:https://tsapps.nist.gov/publication/get.pdf.cfm?pub_id=904990. National Institute of Standards and Technology, U.S. Department of Commerce.
- Nunes, E.P.D.S., Lemos, E.M., Maciel, C., Nunes, C., 2015. Human factors and interaction strategies in three-dimensional virtual environments to support the development of digital interactive therapeutic toy: a systematic review. In: Proceedings of 7th International Conference on Virtual, Augmented and Mixed Reality (VAMR). Springer Verlag, Berlin, Germany, pp. 368–378. https://doi.org/10.1007/978-3-319-21067-4_38.
- Nunes, E.P.D.S., Conceição Jr., V.A.d., Santos, L.V.G., Pereira, M.F.L., de Faria Borges, L.C.L., 2017. Inclusive toys for rehabilitation of children with disability: a systematic review. In: Proceedings of 11th International Conference on Universal Access in Human-Computer Interaction (UAHCI). Springer Verlag, Berlin, Germany, pp. 503–514.
- Oktavia, T., Tjong, Y., Prabowo, H., 2017. Meyliana Security and privacy challenge in bring your own device environment: a systematic literature review. In: Proceedings of 2016 International Conference on Information Management and Technology (ICIMTech). IEEE, Washington, DC, USA, pp. 194–199. <https://doi.org/10.1109/ICIMTech.2016.7930328>.
- Paré, G., Trudel, M.C., Jaana, M., Kitsiou, S., 2015. Synthesizing information systems knowledge: a typology of literature reviews. Inf. Manage. 52, 183–199. <https://doi.org/10.1016/j.im.2014.08.008>.
- Pleban, J.S., Band, R., Creutzburg, R., 2014. Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy. In: Proceedings of the Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications. SPIE, Bellingham, WA, USA, pp. 1–12. <https://doi.org/10.1117/12.2044868>.
- Rafferty, L., Hung, P.C.K., 2015. Introduction to toy computing. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 1–7. https://doi.org/10.1007/978-3-319-21323-1_1.
- Rafferty, L., Kroese, B., Hung, P.C.K., 2015. Toy computing background. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 9–38. https://doi.org/10.1007/978-3-319-21323-1_2.
- Rafferty, L., Fantinato, M., Hung, P.C.K., 2015a. Privacy requirements in toy computing. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 141–173. https://doi.org/10.1007/978-3-319-21323-1_8.
- Rafferty, L., Hung, P., Fantinato, M., Peres, S.M., Iqbal, F., Kuo, S., Huang, S., 2017. Towards a privacy rule conceptual model for smart toys. In: Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS) AIS, Atlanta, GA, USA, pp. 1–10.
- Shasha, S., Mahmoud, M., Mannan, M., Youssef, A., 2018. Playing with danger: a taxonomy and evaluation of threats to smart toys. IEEE Internet Things J. 6, 2986–3002. <https://doi.org/10.1109/JIOT.2018.2877749>.
- Smith, K.L., Shade, L.R., 2018. Children's digital playgrounds as data assemblages: problematics of privacy, personalization, and promotional culture. Big Data Soc. 5, 1–12. <https://doi.org/10.1177/2053951718805214>.
- Solove, D.J., 2006. A taxonomy of privacy. Univ. Pennsylvania Law Rev. 154, 477–564.
- Tang, J.K., Hung, P.C.K., 2017. Computing in Smart Toys. first ed. Springer Verlag, Berlin, Germany. <https://doi.org/10.1007/978-3-319-62072-5>.
- Tang, J.K.T., Tewell, J., 2015. Emerging human-toy interaction techniques with augmented and mixed reality. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 77–105. https://doi.org/10.1007/978-3-319-21323-1_5.
- The Pokémon Company, 2016. Homepage – Pokémon Go. Niantic. San Francisco, CA, USA. URL:<https://www.pokemongo.com/en-us>.
- Toymail, 2019. Toymail – Toys that Bring you Closer to Your Kids. Toymail Inc., New York, NY, USA. URL:<https://toymail.co>.
- Tung, W.F., 2015. Augmented reality for mobile service of film-induced tourism app. In: Hung, P.C.K. (Ed.), Mobile Services for Toy Computing. Springer Verlag, Berlin, Germany, pp. 129–140. https://doi.org/10.1007/978-3-319-21323-1_7.
- USA, 2002. COPPA – Children's Online Privacy Protection Act. URL:<https://www.ftc.gov/sites/default/files/documents/rules/children%2080%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf>. Federal Trade Commission, US Congress, USA.
- Valente, J., Cardenas, A.A., 2017. Security & privacy in smart toys. In: Proceedings of the 1st Workshop on Internet of Things Security and Privacy (IoT S&P). ACM, New York, NY, USA, pp. 19–24. <https://doi.org/10.1145/3139937.3139947>.
- von Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A., 2009. Reconstructing the giant: on the importance of rigour in documenting the literature search process. In: Proceedings of the 17th European Conference on Information Systems (ECIS) AIS, Atlanta, GA, USA, pp. 2206–2217.
- Wang, W., Kuo, V., King, C., Chang, C., 2010. Internet of toys: An e-pet overview and proposed innovative social toy service platform. In: Proceedings of the 2010 International Computer Symposium (ICS). IEEE, Washington, DC, USA, pp. 264–269. <https://doi.org/10.1109/COMPSYM.2010.5685507>.
- WowWee, 2019. WowWee – Astonishing Imagination. WowWee Group Limited, Hong Kong. URL:<https://wowwee.com>.
- Yankson, B., Iqbal, F., Lu, Z., Wang, X., Hung, P.C.K., 2019. Modeling privacy preservation in smart connected toys by petri-nets. In: Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), AIS Atlanta, GA, USA, pp. 1696–1705.
- Yong, S., Lindsog, D., Ruhl, R., Zavarsky, P., 2011. Risk mitigation strategies for mobile Wi-Fi robot toys from online pedophiles. In: Proceedings of the 2011 IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT). IEEE, Washington, DC, USA, pp. 1220–1223. <https://doi.org/10.1109/PASSAT/SocialCom.2011.194>.