Brinquedos conectados e os riscos à infância

Marina Pita, formada em comunicação social pela Pontifícia Universidade Católica de São Paulo, pesquisadora de mídias digitais e direitos das crianças do programa Prioridade Absoluta do Instituto Alana, do qual é também assessora para advocacy.

Data da publicação:

Junho e 2019

Considerando a necessidade de acompanhar o desenvolvimento tecnológico com vistas a maximizar oportunidades e reduzir riscos no uso de Tecnologias da Informação e Comunicações (TICs) por crianças e adolescentes, é fundamental que nos debrucemos o quanto antes sobre a tendência de conexão de objetos, um processo que vem sendo chamado de Internet das Coisas (IoT, na sigla em inglês).

Na esteira da ampliação da oferta de novos dispositivos domésticos conectados, cabe atenção especial para o mercado de brinquedos conectados e inteligentes. De acordo com pesquisa da Juniper Research, em 2017, a receita com brinquedos inteligentes nas Américas estava estimada em 2,14 bilhões de dólares e a remessa, nas Américas, em 118,2 milhões de unidades.

Em junho de 2017, a consultoria avaliou que o baixo custo de componentes digitais, o avanço de tecnologias de conexão-sem-fio de baixo consumo energético e as melhorias em capacidade de processamento criaram um ambiente tecnológico em que a barreira de preço já não seria mais um fator restritivo à expansão do mercado de brinquedos inteligentes e conectados.

O mercado de brinquedos conectados pode ser suportado por *smartphones* e *tablets*, cuja penetração na população já alcança patamares altos, inclusive no Brasil. Ainda, o desenvolvimento e a popularização da computação em nuvem são fatores auxiliares ao desenvolvimento desse tipo de produtos, já que, segundo a Juniper Research:

“*O brinquedo pode apenas funcionar como um dispositivo de gravação, cuja função é a retransmissão de informações à nuvem, onde podem ser processadas. Este fator permite que dispositivos locais excedam suas limitações em termos de capacidade de processamento”.*

Outro importante motor para a ampliação das vendas de brinquedos conectados é a preocupação crescente de mães, pais, educadores e responsáveis com o uso crescente de telas por crianças e os efeitos deste hábito – ao qual o uso de brinquedos inteligentes poderia, teoricamente, se contrapor. A mesma pesquisa avalia que “os brinquedos conectados educacionais são uma reação a isso [crítica ao uso exagerado de telas por crianças], já que são percebidos como uma atividade mais produtiva”.

Por essa lista de fatores, a consultoria enquadrou a indústria de brinquedos conectados como uma das principais tendências tecnológicas. Em apresentação sobre suas apostas para o mercado de tecnologia, escreveu:

“acreditamos que este será o ano para os brinquedos focados em educação, com ênfase em ensino de programação, se tornarem uma tendência dominante”.

Os brinquedos conectados permitem que a indústria estabeleça um contato – e também contrato – prolongado com as crianças e utilize o modelo de "desbloqueio" de funcionalidades (pagas) ao longo do tempo, a cada atualização com novos desenvolvimentos. Assim, o retorno financeiro com o brinquedo conectado não é apenas o preço pago pelo dispositivo em sua aquisição. Este modelo provê à indústria de brinquedos uma forma de se reinventar, compensando a queda nas vendas de fornecedores tradicionais[1].

Os elementos apresentados demonstram a necessidade de atenção dos agentes públicos e da sociedade como um todo para o mercado de brinquedos conectados, em franca expansão, para assim garantir que a inovação tecnológica esteja calcada no melhor interesse das crianças, na responsabilidade empresarial e não unicamente na rentabilidade das empresas.

Os itens a seguir procuram sistematizar alguns dos riscos aos direitos de crianças relacionados aos brinquedos conectados, a partir de uma análise das implicações pós-digitalização da Convenção dos Direitos das Crianças, das Nações Unidas, observando, prioritariamente, o direito da criança à participação e à proteção, conforme abordagem proposta por Livingstone e O'Neill[2].

Acesso não autorizado

Entre 2016 e 2017, a organização britânica de defesa do consumidor Which? realizou, em parceria com diversas entidades de defesa dos consumidores e especialistas em segurança, uma série de testes com brinquedos inteligentes[3]. Os resultados apontam a facilidade para qualquer pessoa se conectar aos brinquedos a partir de um *smartphone*, inclusive sem a necessidade de violar o funcionamento normal dos dispositivos, tão pouco seguros eram seus sistemas. Sobre tais descobertas, a Which? escreveu:

"*Algumas das funcionalidades dos brinquedos tornam possível que qualquer um possa enviar seu próprio áudio para ser reproduzido para quem estiver ao alcance do alto-falante do brinquedo. Ou, qualquer um poderia capturar um áudio, remotamente, através do brinquedo, e ouvi-lo por um telefone ou laptop. Vulnerabilidades significativas tornam esses brinquedos alvos de hackeamento ou algo mais sinistro. Alguém com intenções maliciosas poderia usar esses brinquedos para falar com seus filhos diretamente, de fora de sua casa."*

O brinquedo falante e conectável *Furby*, fabricado pela empresa Hasbro e vendido no Brasil por cerca de 260 reais[4], foi um dos testados. A empresa de segurança da informação parceira da Which?, a Context IS – a partir de uma sugestão de hacking disponível na Web –, conseguiu fazer o objeto tocar uma música e foi capaz de manipular os gráficos que aparecem em seu olho/tela.

O fato de a forma de acesso não autorizado ao brinquedo ter sido encontrada na Web é relevante. A cultura hacker considera a invasão de dispositivos como um desafio[5] que, após superado, deve ser divulgado, como troféu, à comunidade e, claro, para possibilitar a correção dos erros pelos responsáveis. Ou seja, é comum que as formas encontradas para acessar dispositivos sejam divulgadas em comunidades online. Sendo este fato notório e diante da inércia da fabricante, que pode ser entendida como negligência, é possível concluir que a preocupação com as vulnerabilidades dos dispositivos lançados está longe de ser uma prioridade da companhia.

Ainda, de acordo com o levantamento, não foi possível acessar os áudios coletados pelo *Furby*,

no tempo em que a pesquisa foi realizada, mas a Context IS afirmou que provavelmente este objetivo seria alcançado com um pouco mais de dedicação, por meio da modificação do *firmware* (*software* que controla *hardware*) do brinquedo.

Assim como o *Furby*, a quase totalidade dos brinquedos testados não dispunha de qualquer processo de autenticação, o que significa que estranhos poderiam, por exemplo, enviar mensagens pelos brinquedos e, inclusive, como no cachorro-robô *Toy-Fi Teddy*, da fabricante *Spiral Toys*, receber a resposta da criança[6].

No caso do *i-Que Intelligent Robot*, fabricado pela Genesis Toys, a investigação descobriu que qualquer pessoa poderia baixar o aplicativo, encontrar um *i-Que* por meio da busca do *Bluetooth* e passar a usar a voz do robô, simplesmente digitando em uma caixa de texto no aplicativo. A mesma empresa manufatura a boneca *My Friend Cayla*, cuja conexão por *bluetooth* não pode ser desligada ou protegida por senhas, motivo que levou à proibição de sua comercialização na Alemanha[7].

Após analisar os brinquedos conectados, a pesquisadora independente de segurança cibernética, Sarah Jamie Lewis, afirmou que muitos dos produtos não adotaram medidas básicas para garantir que suas comunicações sejam seguras e que as informações de uma criança sejam protegidas. Segundo ela, os brinquedos agiam como "dispositivos espiões descontrolados"[8] porque os fabricantes não incluíam um processo que permitisse que os *gadgets* se conectassem apenas por certos dispositivos selecionados.

Até mesmo o mais icônico dos brinquedos americanos, a Barbie, teve sua versão conectada e inteligente hackeada. O pesquisador americano em segurança digital, Matt Jakubowski[9], descobriu que, quando conectada ao *Wi-Fi*, a boneca se tornava vulnerável. Ele conseguiu acessar o sistema de informação, os dados da conta, os áudios gravados e o microfone, inclusive burlando o sistema de criptografia para o envio de dados[10].

A ausência de sistemas seguros em brinquedos conectados também deixa vulneráveis dados extremamente sensíveis como de localização das crianças usuárias. A análise do Q50[11], um relógio inteligente para crianças, comercializado como uma forma de ajudar os pais a se comunicarem facilmente com seus filhos e acompanharem sua localização em tempo real, mostrou que as falhas no dispositivo permitiriam que *hackers* interceptassem todas as comunicações, ouvissem remotamente a vizinhança e falsificassem a localização da criança.

A pesquisa do órgão governamental Conselho de Consumidores da Noruega (NCC, na sigla em inglês) acerca dos relógios conectados[12] demonstra que este não é um caso isolado. A pesquisa identificou outros dois modelos dos chamados *smartwatches* em que um estranho poderia assumir o controle do relógio, seguindo alguns passos simples. E poderia também realizar escutas não autorizadas das conversas da criança, rastrear sua localização e até contatá-la e conversar com ela. Em outros modelos, os dados, inclusive de localização, são transmitidos e armazenados sem criptografia, vulneráveis à interceptação.

O amplo e preocupante espectro de vulnerabilidades no acesso aos dados apresentado em brinquedos conectados já disponíveis no mercado é tamanho que o Federal Bureau de Investigation (FBI) americano decidiu manifestar-se. O órgão do sistema de segurança daquele país publicou um alerta intitulado “*Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*”[13]. Na abertura do documento, o FBI é bastante explícito:

"*O FBI incentiva os consumidores a considerarem a segurança cibernética antes de introduzir brinquedos inteligentes, interativos e conectados à Internet em suas casas ou ambientes confiáveis. Brinquedos inteligentes e dispositivos de entretenimento para crianças estão incorporando cada vez mais tecnologias que aprendem e adaptam seus comportamentos com base nas interações com o usuário. Esses brinquedos normalmente contêm sensores, microfones, câmeras, componentes de armazenamento de dados e outros recursos multimídia – incluindo reconhecimento de fala e opções de georreferenciamento. Esses recursos podem colocar em risco a privacidade e a segurança das crianças devido à grande quantidade de informações pessoais que podem ser reveladas involuntariamente".*

Informações pessoais (como nome, data de nascimento, fotos, endereço) geralmente são fornecidas ao criar contas de usuário nesses sistemas. Além disso, as empresas coletam grandes quantidades de dados adicionais, como mensagens de voz, conversas, geolocalização, histórico de uso da Internet e endereços IPs. A exposição dessas informações a pessoas mal-intencionadas cria condições favoráveis a fraudes de identidade infantil. Além disso, o potencial uso indevido de dados confidenciais, como informações de localização, identificadores visuais como fotos ou vídeos, combinados com listagem de interesses, podem ser determinantes para angariar a confiança de uma criança, aumentando os riscos de exploração por criminosos.

A vulnerabilidade por padrão dos dispositivos produzidos para crianças fere o princípio de que, para garantir o direito da criança à privacidade e a proteção de seus dados, as empresas devem tomar medidas que impeçam o acesso e intrusão não autorizada, conforme indicado em documento orientador de melhores práticas para a indústria, formulado pelo Fundo da Nações Unidas para a Infância (UNICEF)[14]. Dmonstra ainda o quão longe a indústria de brinquedos conectados está de considerar a privacidade ao longo no processo de desenvolvimento do produto, contrariando outra orientação do órgão.

Vulnerabilidades no armazenamento de dados

O total descaso com a segurança das crianças demonstrado pela indústria dos brinquedos conectados vai além dos dispositivos em si. Também nos centros de armazenamento e processamento de dados das empresas constata-se a ausência de rígido controle e de padrão elevado de qualidade na operação, esperado de entidades que gerenciam dados pessoais, especialmente de hipervulneráveis como são as de 12 anos.

A VTech, fabricante de relógios inteligentes e outros dispositivos conectados voltados para o público infantojuvenil, teve seus sistemas hackeados em 2015, o que resultou na exposição de dados de aproximadamente 6,4 milhões de pessoas – o maior vazamento de dados envolvendo crianças até hoje.

Em janeiro de 2018, a VTech chegou a um acordo com a Federal Trade Comission (FTC), dos Estados Unidos, para encerrar o processo de investigação contra ela, iniciado a pedido do Departamento de Justiça do país[15], pelo qual pagará 650 mil dólares ao órgão norte-americano.

A empresa violou a lei de privacidade de crianças dos EUA ao coletar informações pessoais de crianças sem fornecer notificação direta nem obter o consentimento de seus pais. Adicionalmente, infringiu a legislação local ao deixar de tomar medidas razoáveis para proteger os dados coletados, tais como salvaguardas e medidas de segurança adequadas para proteger

informações transmitidas e armazenadas, e implementar um sistema de prevenção ou detecção de intrusões que pudessem alertar a empresa de invasão não autorizada a sua rede.

Ainda, de acordo com a FTC, a VTech mentia em sua política de privacidade ao declarar que boa parte dos dados dos usuários, fornecidos por meio de sua plataforma, seriam criptografados. Além da multa, a empresa deverá implementar um amplo programa de proteção de dados, sujeito a auditorias independentes, por 20 anos.

Mais recentemente, a empresa CloudPets foi acusada de expor as informações pessoais de meio milhão de pessoas, incluindo endereços de e-mail, senhas, fotos de perfil e mais de dois milhões de gravações de voz de crianças e adultos, que usaram os brinquedos de pelúcia da marca[16], segundo o reconhecido serviço de informação de vazamentos de dados, "*have I been pwned*?"[17].

Os dados pessoais de crianças expostos ou vazados a partir dos centros de processamento de dados das empresas podem ser usados, da mesma forma que aqueles obtidos diretamente por intrusão nos brinquedos, para fraudes e por criminosos.

Vale lembrar que, uma vez expostos, estes dados jamais poderão ser completamente eliminados. A Internet tem um caráter distribuído e aberto, em que todos os pontos conectados estão habilitados a salvar conteúdo e a redisponibilizá-los a qualquer momento. Isso significa que o impacto na vida das crianças e a violação de seus direitos pode perdurar indefinidamente, exigindo esforço constante de proteção dos dados pessoais.

Ainda, ausência de padrões rígidos de segurança no armazenamento de dados fere os princípios da responsabilidade e da prevenção, além dos já apontados princípios do desenvolvimento de produtos observando as garantias da segurança e da privacidade. Também é notório que as empresas não tenham mecanismos para identificar intrusões e procedimentos para alertar os usuários em caso de exposição ou vazamento de dados, ou que não estejam obrigadas a fazê-lo, o que pode significar a manutenção da condição de risco e violação de direitos.

O estabelecimento de práticas de apagamento para que os dados pessoais sejam conservados apenas durante o período considerado necessário para a prestação do serviço é fundamental para reduzir o risco de vazamentos no médio e longo prazos.

A redução do volume de dados coletados também é uma medida adequada, especialmente em se tratando de informações de crianças. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário e apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. O UNICEF recomenda, inclusive, que empresas considerem a possibilidade de oferta de uma versão de seus produtos que não coletem dados de crianças[18].

Exploração comercial de dados.

Em uma economia cada vez mais orientada por dados[19], seja pela venda simples ou pela análise de grandes e complexas bases de dados, é fundamental compreender como os dados de crianças estão sendo usados. Ou, uma vez armazenados, como podem ser utilizados no futuro.

O modelo mais reconhecido de uso de dados é para direcionamento de conteúdo e

publicidade, para grupos ou indivíduos específicos[20]. Este processo ocorre por minucioso processo de micro-segmentação dos consumidores[21]. As grandes empresas utilizam o conhecimento acerca das preferências de cada pessoa para personalizar ofertas comerciais e influenciar comportamento e opinião.

Por meio de tecnologias sofisticadas e aplicação de métodos psicológicos e comportamentais[22], os dados pessoais são, muitas vezes, utilizados para seduzir consumidores-alvos, tornando-os ainda mais fragilizados nesta relação já tão desigual, marcada pela assimetria informacional.

Se o alvo do anúncio é uma criança, a desigualdade informacional é ainda maior. Não à toa, a doutrina consumerista já considera crianças hipervulneráveis e hipossuficientes[23]. Em um contexto de massiva coleta e tratamento de dados pessoais e de avanço nas tecnologias de análise e direcionamento de publicidade, este grupo está ainda mais suscetível às pressões advindas desta complexa relação entre empresas e consumidores, já que crianças não detêm as ferramentas biopsíquicas adequadas para responder com igualdade a essas pressões.

Quando uma boneca ou outro brinquedo conectado pergunta a brincadeira, cor, animal, vídeo ou música preferida de uma criança, está construindo um banco de dados sobre suas preferências. Este conhecimento sobre o imaginário infantil pode facilmente ser traduzido em ofertas comerciais, que podem se dar por meio do próprio brinquedo, mediante a citação do produto, por exemplo.

O uso de dados também pode ocorrer em contextos diferentes daquele em que houve a coleta. Isso pode ocorrer pelo uso de telas em que o cruzamento de endereços IPs e perfil identifique o usuário, ou a partir da identificação da criança por mecanismos de reconhecimento facial.

À medida que as lojas, centros comerciais e mesmo sistemas de transporte de massa[24] adotam ferramentas de coleta de dados,[25] utilizando identificação de dispositivos móveis ou por reconhecimento facial, o direcionamento de ofertas nestes ambientes se tornará mais comum. E a tecnologia não é nova. Em janeiro de 2016, artigo[26] no blog do Information Commissioner's Office (ICO), regulador do uso de dados do Reino Unido, já apontava que lojas poderiam modificar preços ou oferecer determinados produtos por perfil do transeunte, a partir da identificação por sistema de conexão wi-fi, Bluetooth e reconhecimento facial.

O uso de informações coletadas em um dispositivo para oferta comercial em outros contextos e ambientes é dificilmente rastreável, até mesmo para especialistas, de forma que a capacidade de resposta a usos indevidos, por meio de atuação *ex-post*, é prejudicada. Considerando o modelo de análise de risco versus oportunidade, comum na definição das práticas comerciais das empresas, agentes privados poderiam estar inclinados a ver aqui uma oportunidade de rentabilização dos dados sem que possam ser responsabilizados pela abusividade.

Mas os dados de crianças não necessariamente precisam ser usados imediatamente para que tenham valor comercial e possam ser vendidos. Há toda uma indústria de compra e venda de dados no atacado, que opera sem conhecimento do público e cujas práticas são desconhecidas[27]. A necessidade de regulação da operação destas empresas, chamadas de Data Brokers, vem sendo uma tônica em diversas partes do mundo. A Federal Trade Comission fez um alerta ao Congresso norte-americano neste sentido[28] e a lei europeia de proteção de dados[29], vigente desde maio de 2018, tratou desta preocupação.

Termos de uso genéricos

As empresas fabricantes de brinquedos conectados não estão assumindo a devida responsabilidade por garantir a privacidade de crianças e ainda estão usando os termos de uso para se blindarem. A VTech, por exemplo, alterou os termos e condições de uso para incluir que não é responsável por nenhum vazamento de dados[30].

O modelo binário de aceitar ou negar os termos dos brinquedos conectados, em desrespeito ao princípio da necessidade, pelo qual a coleta de dados deve ser justificada para determinada finalidade, tem limitado a escolha dos pais e impõe que tenham de aceitar a totalidade do contrato para que seus filhos possam usar plenamente os jogos e aplicativos.

"*Isso posiciona pais e cuidadores como os únicos responsáveis pela privacidade de dados e segurança das crianças, transferindo a responsabilidade legal pela coleta, armazenamento, análise e compartilhamento de dados das empresas para eles. Essas estratégias dão às entidades sinal verde para que continuem, e até expandam as práticas de coleta de dados, mesmo de crianças com menos de 13 anos*"[31].

Os termos e condições dos brinquedos conectados, em muitos casos, não exige o consentimento livre, expresso e informado de mães, pais ou responsáveis, mesmo quando a oferta desses produtos se dá em países cuja legislação exige consentimento parental, como no Brasil, Estados Unidos[32] e União Europeia[33]. Ao assumir que o uso dos dispositivos significa o consentimento e aceite dos termos de uso e de privacidade, empresas violam o direito à privacidade das crianças, bem como ignoram sua condição de hipervulnerável e, portanto, incapaz de celebrar contrato.

Mesmo os brinquedos que exigem que o responsável autorize a coleta de dados da criança, por registro de e-mail, por exemplo, apresentam termos de uso e política de privacidade em longos textos[34], escritos em letra diminuta, que exigem longo tempo para leitura e, frequentemente, encontram-se escondidos em página alternativa. Este modelo de termos de uso e política de privacidade é uma forma de perpetuação dos modelos de negócios das empresas, sem controle social ou governamental.

Vale destacar que quarenta por cento dos brasileiros não se atentam ao contrato de licença durante a instalação de um aplicativo no celular, e outros 15% não leem as mensagens de instalação dos programas, apenas clicam em 'avançar' e 'aceito', sem saber o que estão autorizando[35]. Este dado, bem como a análise do modelo de oferta de informação por empresas, demonstra o potencial risco de uso inescrupuloso dos dados de crianças , sem conhecimento real dos responsáveis.

Mesmo quando os pais leem os termos de uso e privacidade para consentir, o fato de estes serem continuamente alterados, sem obrigação de notificação e novo consentimento, torna o modelo uma carta branca às empresas, especialmente porque o adulto responsável pode não manter vigília constante quando se trata de um dispositivo ou sistema usado pela criança.

Ou seja, o atual modelo de oferta de informações a pais e responsáveis e mesmo a exigência de consentimento parental, sem o estabelecimento de padrões éticos de coleta e tratamento de dados de crianças, é insuficiente diante da opção social pela proteção integral das crianças. O atual modelo de funcionamento da indústria coloca sobre a família todo o peso da responsabilidade pela garantia da segurança, bem-estar e melhor interesse da criança, sem oferecer-lhe os instrumentos adequados.

O consentimento para o tratamento dos dados de crianças deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca do responsável legal. Nos casos em que o tratamento sirva a fins múltiplos, deverá ser dado um consentimento para todos esses fins.

O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples, inclusive para crianças, em respeito a seu estágio de desenvolvimento constante e o direito a acessar informações que tenham impacto em seus direitos.

Violação da privacidade e datatificação da infância

À medida que brinquedos conectados, assistentes digitais e outros dispositivos habilitados com sensores e conectados à Internet passam a fazer parte do cotidiano das crianças, um grande volume de dados detalhados sobre elas passa a ser gerado, armazenado, analisado e distribuído.

O primeiro risco atrelado a este crescente tratamento de dados de crianças diz respeito a seu direito à privacidade. Isso é um fator fundamental para o desenvolvimento natural de crianças. A privacidade está diretamente atrelada à formação da identidade, desenvolvimento da personalidade e à habilidade de construir relacionamentos sadios com outros[36].

No momento do brincar, a criança exterioriza certos aspectos de si mesma em um movimento de elaboração de suas primeiras experiências. Para elas, não é simples a compreensão de que estes objetos, de uso íntimo, podem ser portas de acesso ao momento de intimidade, especialmente porque os sensores – microfones e câmeras, por exemplo – não chegam a ser visíveis. Violar o momento do brincar significa interferir em um processo necessário de desenvolvimento e cujos impactos ainda são desconhecidos. Sabe-se, no entanto, que tal prática pode reduzir a confiança na capacidade de discernimento acerca do ambiente e em seus pais e responsáveis.

Adicionalmente, os brinquedos e demais dispositivos conectados estimulam a vigilância parental invasiva, sem necessariamente o conhecimento do sujeito vigiado, com implicações na privacidade da criança, em sua liberdade e desenvolvimento. A Hello Barbie, da Mattel, por exemplo, envia trechos das conversas da criança com a boneca aos pais por e-mail e disponibiliza botões para compartilhamento nas redes sociais em evidente estímulo à exposição da intimidade deste grupo.

De acordo com o relatório *Guidelines for Industry on Child Online Protection*, produzido pela UNICEF em parceria com a UIT, quando algum programa permite que pais e responsáveis monitorem a comunicação da criança no universo online, é importante que isso seja discutido abertamente com ela. “Do contrário, tal conduta pode ser percebida como vigilância e pode minar a confiança entre os membros da família”[37].

Mas as práticas de vigilância e controle parental podem ter outros efeitos nefastos. Segundo Charlotte Faircloth, professora sênior do Departamento de Ciências Sociais da Universidade de Roehampton e membra fundadora do Centro para Estudos da Parentalidade[38],“até o momento, pesquisas sociológicas acerca da crescente tecnologização da vida familiar apontam para o

aumento da ansiedade dos pais, mais do que sua diminuição".

Adicionalmente, a inserção da IoT nos lares pode amplificar a tendência em direção ao que chama de "parentalidade performativa", em que os pais, em vez de apenas brincarem com as crianças porque é divertido ou desejado, se engajarão em fazê-lo como uma forma de "otimizar o desenvolvimento cerebral" ou de "modelar o bom comportamento", na avaliação de Charlotte Faircloth.

Ainda, à medida que a privacidade é substituída pela vigilância e que a criança toma consciência de que está acompanhada a todo momento, é provável que passe a agir de forma diferente[39], com impacto em sua liberdade e no desenvolvimento de sua identidade e personalidade. Considerando que as oportunidades de uma pessoa são, de forma crescente[40], definidas pelos tipos de ordenação social proporcionados pela análise de dados, a criança exposta a sistemas de coletas de dados está suscetível a formas de perfilamento que podem afetar seu futuro, sem que ela tenha consciência ou conhecimento.

Julgamentos ou inferências com base em dados abrem a possibilidade de que o resultado dessas práticas seja a circunscrição das complexidades e potencialidades da criança. Por ser a criança uma pessoa em desenvolvimento, o perfilamento tem potencial de dano e violação de direitos maior do que o uso desta tecnologia em adultos.

A estas questões se somam a expansão e complexificação dos sistemas de classificação e perfilamento, já em andamento, que tende a reduzir cada vez mais as oportunidades para as pessoas desafiarem as inferências e previsões feitas por algoritmos. Nesse sentido:

"*As pessoas geralmente têm pouco conhecimento sobre como as corporações estão explorando os dados pessoais e os utilizando para construir perfis detalhados usados para decisões sobre acesso a empregos, impostos, benefícios sociais, ofertas especiais e crédito*"[41]

A "perfilização" acaba por gerar novas identidades virtuais sobre os indivíduos, baseadas em estereótipos e que podem ser determinantes para acesso a serviços, produtos e oportunidades de educação e trabalho[42] no presente e no futuro.

O impacto da perfilização por sistemas baseados em dados e inteligência artificial para o acesso a oportunidades vem sendo estudado simultaneamente à aplicação dessas técnicas, com grande risco de discriminação. O fato de anúncio de emprego com salário alto ser direcionado, por mecanismos automáticos de seleção de perfis com base em dados, mais frequentemente a homens, conforme indica pesquisa da Carnegie Mellon University[43], poderia afetar o acesso de mulheres a cargos executivos e de liderança. A busca de nomes em mecanismos de pesquisa apresentar, com mais frequência, referências relacionadas a registros criminais quando tais nomes são mais usados pela comunidade negra, como aponta levantamento da Harvard University[44], pode afetar o sucesso pessoal e profissional de negros e negras. A perfilização utilizada por agentes de segurança pública tem levado à discriminação racial contra grupos historicamente oprimidos[45], uma vez que as bases de dados já estavam contaminadas por preconceitos.

Atenta a estas questões, a Casa Branca norte-americana encomendou em 2015 um levantamento sobre os riscos de discriminação a partir de processos automatizados de análise de grande volume de dados[46], que concluiu:

"*ao lado de seu potencial benéfico, de ser usado para ampliar o acesso a crédito ou melhorar os resultados da educação, reside o potencial de as tecnologias de big data serem usadas para a discriminação contra indivíduos, tanto intencionalmente quanto inadvertidamente, permitindo resultados discriminatórios, com redução de oportunidade e das opções disponíveis a estes".*

O relatório tem como principais recomendações a limitação do uso de dados educacionais de crianças, para protegê-las deste potencial discriminatório e o fortalecimento das agências de defesa do consumidor e de direitos civis, com vistas a expandir o conhecimento técnico, de forma a capacitá-las a identificar práticas discriminatórias resultantes do uso de ferramentas de análise de dados, bem como desenvolvimento de planos de investigação e solução para potenciais violações.

Reconhecer o potencial de exploração comercial e de resultados discriminatórios pelo uso de dados é um primeiro passo, mas o tempo de ajuste das políticas públicas e da legislação para resolver tais questões pode não dar conta de proteger as crianças, de forma que medidas rápidas devem ser tomadas para disciplinar a coleta e tratamento de dados de crianças, bem como sua perfilização.

Os riscos de discriminação e de violação ao desenvolvimento livre da criança a partir de tratamento de dados ainda são desconhecidos por boa parte da população e as reflexões acerca do tema seguem limitadas a rodas de especialistas. Certamente os perigos mais facilmente compreendidos são aqueles que têm a ver com a segurança física e psicológica imediata da criança, os riscos de que pessoas não autorizadas tenham acesso à criança, ganhem a confiança da mesma por meio das informações obtidas na web e por acesso não autorizado a dados.

Mas, à medida que os sistemas de análise de dados avançam, outros riscos surgem e não são tão conhecidos das famílias, dos reguladores e muito menos das crianças. O potencial para que o perfil de dados de uma pessoa afete sua experiência cotidiana no presente ou no futuro aumenta, conforme aponta relatório da *Children's Commission* inglesa, publicado em novembro de 2018[47].

E, ainda que pesquisas apontem que as crianças têm mostrado conhecimento e preocupação acerca dos dados que compartilham nas relações interpessoais, resultados preliminares de levantamento realizado pela professora Sonia Livingstone, da London School of Economics and Political Science, mostra que as crianças têm pouca ciência das dimensões institucionais da privacidade, como as que envolvem os dados que as escolas têm, por exemplo, e como podem ser usados, assim como os dados que empresas comerciais coletam.

Agenda camuflada

Os brinquedos conectados interagem com as crianças e propõem ações. Mas o algoritmo responsável pelas escolhas de repertório dos brinquedos, bem como os seus princípios, parâmetros e fundamentos, são inacessíveis. Ou seja, existe uma agenda algorítmica que, cada vez mais, passa a tomar decisões que afetam a vida das crianças, sem que pais, mães, sociedade e Estado possam acessá-la. São uma caixa-preta.

Considerando que estes brinquedos estão associados a modelos de negócio complexos, suas interações com a criança podem partir de acordos preestabelecidos, não necessariamente informados aos pais e responsáveis. A empresa Genesis Toy, por exemplo, foi acusada de imiscuir comunicação mercadológica no repertório da boneca conectada *My Friend Cayla.* O

brinquedo, conforme pesquisa, foi pré-programado a fazer referência à *Disneyworld* e aos filmes da *Disney*. “A Cayla diz às crianças que seu filme favorito é *Pequena Sereia* e sua música preferida é *Let It Go*, trilha da animação *Frozen*, ambos da Disney. A boneca também afirma que adora ir à Disneylândia e ao parque Epcot, na Disneyworld”[48]. A Genesis Toy, por sua vez, veiculou publicidade no Disney Channel, em que informava ser “uma orgulhosa patrocinadora” do canal.

A agenda algorítmica destes dispositivos pode facilmente incluir referências a partir de acordos comerciais com terceiros, induzir ao consumo constante de jogos e adereços relacionados ao próprio brinquedo e/ou incentivar padrões de comportamento como competição, consumismo e vaidade excessivos. Ademais, se já há consenso sobre a dificuldade de a criança reconhecer e compreender a comunicação mercadológica[49], este formato de disseminação de conteúdo torna esta tarefa praticamente impossível, inclusive muito difícil até para adultos.

Porém, essa estratégia comercial, baseada em uma relação personalizada de confiança e identificação da criança com os brinquedos, pode ser extremamente eficiente. Ao fazer com que as crianças se identifiquem com um produto, a empresa é mais capaz de envolver a criança e prepará-la para ser uma consumidora fiel desde a mais tenra idade.

A preocupação acerca dos princípios e fundamentos da mediação algorítmica deve ser maior à medida que assistentes digitais – como o Echo, da Amazon – passam a organizar a vida das crianças e a selecionar produtos e conteúdos a serem consumidos por elas, não apenas no mundo virtual, mas possivelmente no mundo concreto, já que a expectativa para este segmento é que automatize as tarefas domésticas como, por exemplo, compras. Há que se questionar desde já se a escolha de itens que estarão à disposição das crianças vai ser baseada no melhor interesse da criança ou em acordos comerciais.

--

1 https://oglobo.globo.com/economia/negocios/receita-da-mattel-cai-com-bar...

2 Livingstone, S., & O’Neill, B. (2014). “Children’s rights online: Challenges, dilemmas and emerging directions”. In S. van der Hof, B. van den Berg, & B. Schermer (Eds.), *Minding minors wandering the web: Regulating online child safety* (pp. 19– 38). Berlin: Springer.

3 https://www.which.co.uk/reviews/smart-toys/article/smart-toys-should-you...

4 https://www.americanas.com.br/busca/furby

5 https://makezine.com/2017/02/06/toy-hacking-simone-giertz

6 Conforme pesquisa realizada pela organização de defesa do consumidor alemã Stiftung Warentest em parceria com a Which?

7 https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/1...

8 https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html

9 https://about.me/jaku

10 https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi...

11 https://www.top10vpn.com/privacy-central/privacy/smart-toys-safety-review

12 https://snl.no/smartklokke

13 *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*. Disponível em https://www.ic3.gov/media/2017/170717.aspx

14 UNICEF (2018). *Industry Toolkit: Children's online and freedom of expression*. Disponível em: https://issuu.com/unicefusa/docs/unicef_toolkit_privacy_expression?e=296...

15 https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_comp...

16 https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach...

17 Disponível em https://haveibeenpwned.com

18 UNICEF (2018). *Industry Toolkit: Children's online and freedom of expression*. Disponível em https://issuu.com/unicefusa/docs/unicef_toolkit_privacy_expression?e=296...

19 *The Economist*. "Data is giving rise to a new economy" (Maio 2017). Disponível em https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-.... Acesso em: 14 de maio de 2018.

20 Pesquisa da americana Data & Marketing Association aponta que anunciantes gastaram US$15,5 bilhões em dados e serviços atrelados a dados em 2018, para personalizar publicidade. Disponível em: https://thedma.org/news/seeking-customer-personalization-marketers-spend.... Acesso em 14 de maio de 2018.

21 Pesquisa da empresa SalesForce com anunciantes indica que 90% usam ou planejam usar dados coletados online, em 2018. Cinquenta por cento usam ou pretendem usar dados adquiridos de terceiros, intenção que cresce em 30% quando questionados sobre o uso de dados adquiridos de terceiros, em dois anos. Os terceiros são agregadores de dados cujo negócio é comercialização. Disponível em https://c1.sfdcstatic.com/content/dam/web/en_us/www/assets/pdf/datasheet.... Acesso em: 14 de maio de 2018.

22 Recentemente, um modelo de análise de dados pessoais para inferir personalidade e comportamento e influenciá-los, desenvolvido por pesquisadores da Stanford University e do Psychometrics Center da University of Cambridge, ficou mundialmente conhecido. Disponível em https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavio.... Acesso em: 14 de maio de 2018.

23 *Código Brasileiro de Defesa do Consumidor comentado pelos Autores do Anteprojeto*. São Paulo: Editora Forense. p. 299-300.

24 https://veja.abril.com.br/tecnologia/portas-da-linha-4-do-metro-vao-faze...

25 https://www.theguardian.com/technology/2016/jan/21/shops-track-smartphon...

26 https://iconewsblog.org.uk/2016/01/21/how-shops-can-use-your-phone-to-tr...

27 Yael Grauer. "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?". Disponível em https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-

brokers-.... Acesso em 12 de junho de 2018.

28 Federal Trade Comission. *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information*. Disponível em https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-co.... Acesso em 12 de junho de 2018.

29 Regulamento (ue) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a diretiva 95/46/ce (Regulamento Geral sobre a Proteção de Dados). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 12 de junho de 2018.

30 Global News. "Hacked toy maker VTech changes terms to say it's not liable for data breaches". Ver http://globalnews.ca/news/2508781/hacked-toy-maker-vtech-changes-terms-t...

31 Donell Holloway & Lelia Green (2016). 'The Internet of toys", *Communication Research and Practice*, DOI: 10.1080/22041451.2016.1266124. Ver http://dx.doi.org/10.1080/22041451.2016.1266124

32 Nos Estados Unidos, a Lei de Proteção da Privacidade de Crianças (COPPA, na sigla em inglês) institui regras para responsáveis por websites e serviços online visando a promoção da privacidade de crianças e adolescentes de até 13 anos na internet. Entre as obrigações estabelecidas pela norma está a de disponibilizar de forma clara sua política de privacidade para este público. A coleta de informações de meninos e meninas, salvo exceções, fica condicionada à obtenção de consentimento dos pais que também podem corrigir ou solicitar a exclusão dos registros. Pela regra, websites e serviços online ficam proibidos de repassar informações coletadas de crianças a terceiros, devendo mantê-las somente enquanto forem necessárias no processo de tratamento.

33 O Regulamento Geral de Proteção de Dados na União Europeia (GDPR) estabelece proteção específica aos dados pessoais de crianças e adolescentes, que se aplica para efeitos de comercialização, de criação de perfis e na coleta de dados pessoais em serviços disponibilizados diretamente a eles. Para serviços da sociedade da informação, há a obrigação de consentimento parental ou de responsável legal para coleta e tratamento de dados de pessoas com até 16 anos de idade, ainda que os Estados-membros possam definir a idade de maioridade para consentimento, desde que não inferior a 13 anos.

34 Leitura de 'termos e condições' de serviços na internet exige 4,5 horas. Ver http://www1.folha.uol.com.br/tec/2017/12/1945132-leitura-de-termos-e-con.... Acesso em 8 de maio de 2018.

35 40% dos usuários brasileiros não leem termos de uso ao instalar aplicativos. Ver http://tecnologia.ig.com.br/2016-03-29/40-dos-usuarios-brasileiros-nao-l.... Acesso em 8 de maio de 2018.

36 http://www.cyanb.ca/images/ChildrensOnlinePrivacy-e.pdf

37 UNICEF e UIT. *Guidelines for Industry on Child Online Protection*. Ver https://www.unicef.org/csr/files/COP_Guidelines_English.pdf

38 https://www.designcouncil.org.uk/news-opinion/will-internet-things-set-f...

39 Elmer, 2003.

40 Lyon e Bauman, 2013; Robinson et al.,2014; Rosenblat et al., 2014. The datafied child: The dataveillance of children and implications for their rights". Ver http://journals.sagepub.com/doi/pdf/10.1177/1461444816686328. Acesso em 8 de maio de 2018.

41 Crawford e Schultz, 2014. "The datafied child: The dataveillance of children and implications for their rights". Disponível em http://journals.sagepub.com/doi/pdf/10.1177/1461444816686328

42 https://www.wired.com/2012/04/ff_klout/all/1

43 Amit Datta, Michael Carl Tschantz, and Anupam Datta. "Automated Experiments on Ad Privacy Settings". Ver http://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf

44 Latanya Sweeney. "Discrimination in Online Ad Delivery". Ver https://dataprivacylab.org/projects/onlineads/1071-1.pdf

45 https://www.hrw.org/news/2012/04/17/us-end-discriminatory-profiling-police

46 White House. *About Big Data: Seizing Opportunities, Preserving Values*.Ver https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_B.... Acesso em 11 de junho de 2018.

47 Children's Comission. "Who Knows What About Me? A Children's Comissioner Report into the collection and sharing of children's data".
Ver https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/who-.... Acesso em 17 dez. 2018.

48 https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf

49 Angela J. Campbell, Georgetown University Law Center. "Rethinking Children's Advertising Policies for the Digital Age". Disponível em: https://scholarship.law.georgetown.edu/facpub/1945. Acesso em 12 de junho de 2018.

Categoria:

- poliTICs 29