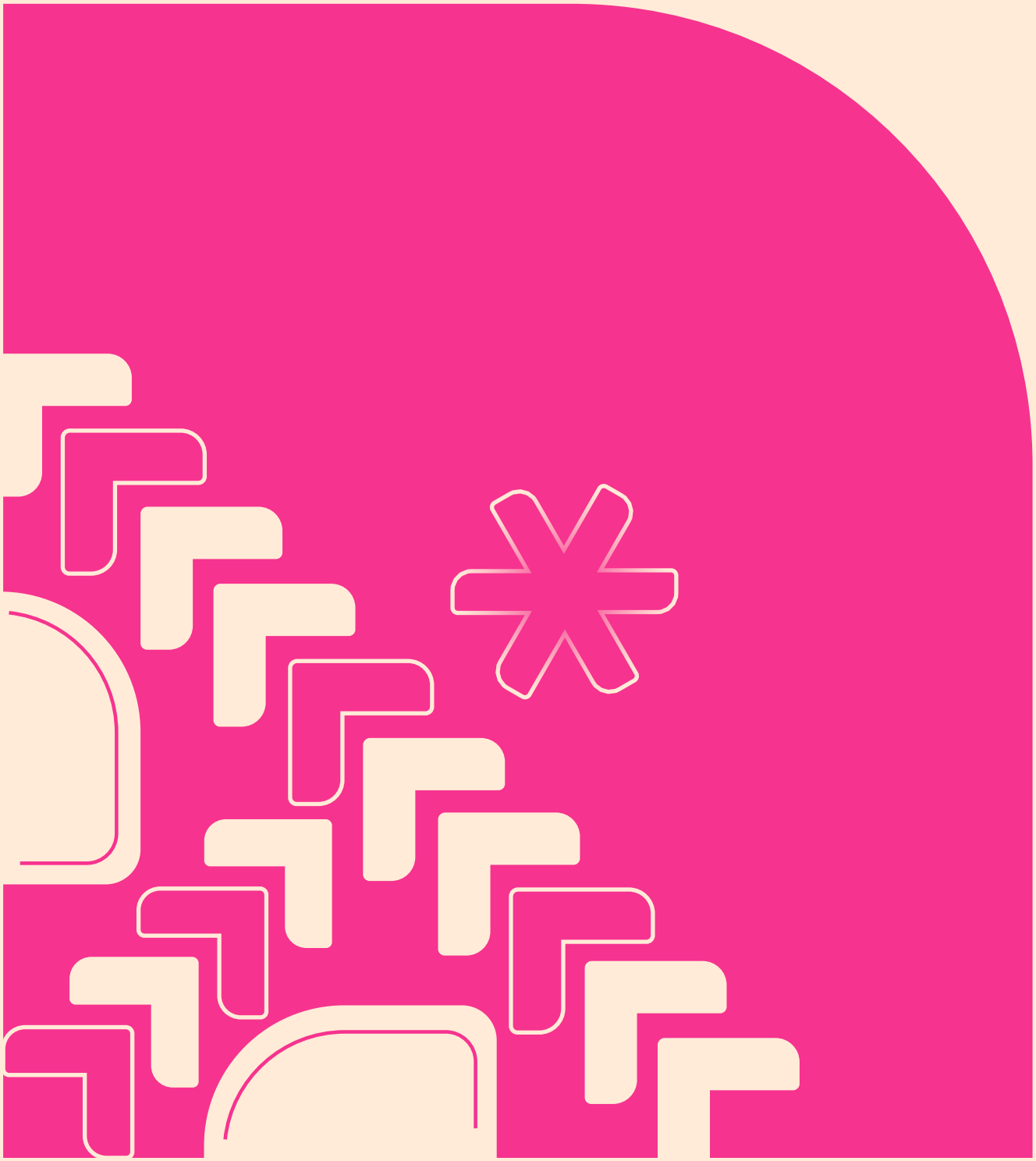
Nota Técnica

Instituto de Pesquisa em Direito & Tecnologia do Recife

PL 2628/2022



FICHA TÉCNICA

Realização:

Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec

Equipe:

Coordenação:

Marcos Cesar M. Pereira

Autores:

Luana Batista
Marcos César M. Pereira
Mariana Canto
Pedro Amaral
Pedro Silva Neto
Raquel Lima Saraiva
Rhaiana Valois

Revisão:

André Lucas Fernandes
Raquel Lima Saraiva

Projeto gráfico:

Estúdio Puya!

Como citar:

IP.REC - INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. Nota Técnica Sobre O PL Nº 2628/2022. Recife: IP.rec, 2024.

Comentário à versão do Relator

No dia 05 de novembro foi disponibilizada a versão do relator Senador Flávio Arns (PSB/PR) do Projeto de Lei nº 2628/2022. Na nossa análise, a versão do relator não trouxe mudanças significativas no texto. Apesar das poucas modificações, algumas merecem destaque enquanto novidades positivas.

Dentre uma das novidades está o acréscimo do parágrafo único no artigo 7º, que determina que fornecedores de produtos ou serviços de tecnologia da informação não deverão tratar dados de crianças e adolescentes de forma a contribuir com violações à privacidade e outros direitos protegidos. No mesmo direcionamento, o § 2º do artigo 19 determina que dados coletados para fins de verificação de idade devem ser utilizados única e exclusivamente para tal finalidade. Ambas adições representam avanço no direito à privacidade de crianças e adolescentes, mas que poderiam ser ainda maiores, sobretudo no § 2º, caso houvesse a exclusão dos dados após a verificação da idade.

Outro avanço significativo para privacidade de crianças e adolescentes foi a adição do inciso VIII do artigo 11, que determina que fornecedores de produtos ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças permitam o controle e desabilitação de ferramentas de inteligência artificial não essenciais para o sistema. Com o avanço de tal tecnologia, sobretudo em redes sociais, avança também o tratamento de dados de crianças e adolescentes nas plataformas, sem o conhecimento ou consentimento significativo, além de, por muitas vezes, tais plataformas dificultarem o cancelamento do consentimento. Por isso, é importante garantir medidas de *opt out* para proteção da privacidade de crianças e adolescentes.

Neste sentido, consideramos que o texto abaixo ainda segue relevante para garantir que crianças e adolescentes estejam protegidas no ambiente online. Diversos pontos de melhorias que foram apontadas na nossa Nota Técnica poderiam ser adotadas para um PL ainda mais robusto e garantidor dos direitos de crianças e adolescentes.

1. Introdução

Esta Nota Técnica trata do Projeto de Lei n° 2628/2022, de autoria do Senador Alessandro Vieira (MDB/SE), que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. O PL tem como fundamentos "a prevalência absoluta do interesse das crianças e adolescentes, a condição peculiar de pessoa em desenvolvimento biopsíquico e a proteção contra a exploração comercial indevida" e pretende regular "todo produto ou serviço de tecnologia da informação direcionado ou que possa ser utilizado por crianças e adolescentes, disponíveis em território nacional".

O projeto incide sobre produtos e serviços de tecnologia da informação, monitoramento infantil, jogos eletrônicos, publicidade em meio digital, redes sociais e reporte de violações aos direitos de crianças e adolescentes. A relação com os direitos das crianças e adolescentes é um dos pontos quentes na regulação de plataformas, principalmente no Norte Global. Em 2023, foi

aprovado o Online Safety Act, no Reino Unido. Há iniciativas similares na Comissão Europeia, nos Estados Unidos e no Canadá.

Nesta nota, abordamos problemas e soluções relacionados à regulação de serviços, transparência, privacidade, proteção de dados, monitoramento e controle parental da proposta brasileira em questão.

2. Regulação de serviços e transparência

Observando outras experiências de regimes internacionais de proteção às crianças online, o *Age-appropriate design code* do Reino Unido, resultante do *Data Protection Act* (ICO - UK, 2018)[1], adotou a expressão "provável acesso por", em vez de termos mais restritivos. Essa definição buscou abarcar tanto os serviços que são voltados para crianças e adolescentes, quanto aqueles que não são especificamente destinados a esse público, mas que são de provável acesso por ele - direcionamento também adotado no PL.

O Código considera que, "para que um serviço seja 'provável' de ser acessado, a possibilidade de que isso aconteça precisa ser mais provável do que não provável" (idem, p. 31). Dessa forma, reconhecem "a intenção do Parlamento de abranger os serviços que as crianças utilizam de fato, mas não ampliamos a definição para abranger todos os serviços aos quais as crianças poderiam eventualmente ter acesso" (Ibid.). Diferentemente do PL, o Código estabelece dois parâmetros para identificar a probabilidade de um serviço ser acessado por crianças e adolescentes: i) a natureza e o conteúdo do serviço, e se isso gera um apelo particular para as crianças; e ii) a forma como o serviço é acessado de quaisquer medidas tomadas para impedir que as crianças consigam esse acesso.

Os autores do Código recomendam medidas diversas para lidar com a possibilidade de acesso por crianças e adolescentes. Caso os provedores dos serviços acreditem que eles não devem ser acessados por crianças e adolescentes, deve-se buscar impedir ou evitar seu acesso (caso em que o Código não se aplica), ao invés de torná-lo acessível às crianças e adolescentes (*child-friendly*). Caso os serviços não sejam direcionados para crianças e adolescentes, mas também não sejam inadequados para que eles o utilizem, os provedores devem avaliar o quanto o serviço é atraente para esse público. Nesse caso, a definição "provável acesso por" será aplicada. O Código argumenta que os provedores devem ter bom senso para identificar o grau de provável acesso por crianças e adolescentes, e tomar as medidas adequadas a partir desse conhecimento.

Já em sua seção sobre a produção de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), o Código estabelece que os provedores devem "considerar o potencial impacto nas crianças e qualquer dano ou prejuízo que seu tratamento de dados possa causar – seja físico, emocional, de desenvolvimento ou material" (2018, p. 47). Deve ser avaliado se o tratamento de dados pode causar, permitir ou contribuir para o risco de: danos físicos; aliciamento on-line ou outra exploração sexual; ansiedade social, problemas de autoestima, bullying ou pressão dos colegas; acesso a

[1] ICO - UK (Information Commissioner 's Office); Instituto de Tecnologia e Sociedade do Rio, Instituto Alana (Trad.). **Design Apropriado para a Idade: Código de Práticas para Serviços On-line.** 2018. Disponível em: https://itsrio.org/pt/publicacoes/design-apropriado-para-a-idade-codigo-de-praticas- para-servicos-on-line/. Acesso em: 14 mar. 2024.

conteúdo nocivo ou inapropriado; desinformação ou restrição indevida de informações; incentivo à tomada de riscos excessivos ou comportamento insalubre; comprometimento da autoridade ou responsabilidade dos pais; perda de autonomia ou de direitos (incluindo o controle sobre dados); uso compulsivo ou distúrbios de déficit de atenção; tempo excessivo de tela; padrões de sono interrompidos ou inadequados; exploração econômica ou pressão comercial injusta; ou qualquer outra desvantagem econômica, social ou de desenvolvimento significativa.

Para avaliar o nível de risco, os provedores devem considerar tanto a probabilidade, quanto a gravidade de qualquer impacto sobre as crianças, levando-se em conta que "as necessidades e a maturidade das crianças serão diferentes de acordo com suas idades e estágios de desenvolvimento" (Ibid.).

Acreditamos que a aplicação do conceito de "provável acesso por" crianças e adolescentes, a identificação do nível de risco de tratamento de dados e outros pontos do Código do Reino Unido podem oferecer modelos para a adoção de gradações de probabilidades de usos e riscos no PL 2628/2022. O Código também endereça, em diversas seções, medidas específicas para as diferentes faixas etárias de crianças e adolescentes que acessam os serviços online. **Defendemos que esse direcionamento seja adotado no PL 2628, através da alteração do art. 1º, expandindo o conceito de "provável acesso por" para que a probabilidade de uso, a atratividade, os riscos oferecidos (através do tratamento de dados e da exposição indevida a conteúdos e comunicações) e as particularidades das diferentes faixas etárias de crianças e adolescentes sejam levadas em conta, ou através do apontamento de um órgão estatal a quem caiba a incubência de estabelecer gradações de provável acesso.**

Entendemos, também, que o parágrafo único do art. 5º deste PL é problemático. Este dispositivo prevê a obrigatoriedade de serviços não desenhados ou adequados a crianças e adolescentes empregarem "mecanismos para ativamente impedir o uso" por este público. Para isso, seria necessária a aplicação de medidas intrusivas e excessivas de coleta de dados, verificação de identidade e monitoramento de uso. Esse fator se torna ainda mais crítico tendo em vista o disposto no art. 1° sobre a aplicação excessivamente ampla do PL. Por isso, recomendamos a supressão do parágrafo único do art. 5º.

Nesse sentido, o art. 6º do PL dispõe que produtos ou serviços de tecnologia da informação que são direcionados ou que possam ser utilizados por crianças e adolescentes deverão tomar medidas razoáveis no desenho e operação dos produtos ou serviços, elencando os riscos que devem ser mitigados. Entretanto, não há no PL um dispositivo que fale sobre como as medidas serão avaliadas.

Em diálogo com o PL 2630/2020[2], (popularmente conhecido como PL das *Fake News*), que institui a "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet", o PL também tem enquanto dispositivo a avaliação e mitigação, por parte de plataformas, de riscos sistêmicos decorrentes dos produtos ou serviços. No entanto, diferentemente do PL 2628/2022, o PL 2630/2020 obriga às plataformas enquadradas no PL que publiquem relatórios de avaliação e atenuação dos riscos sistêmicos, sob risco de sanção administrativa. Por isso, **recomendamos a**

[2] BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.630, de 27 de abril de 2023. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: Câmara dos Deputados, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2358879. Acesso em: 15 mar. 2024.

adoção de publicação de relatórios de avaliação e atenuação de riscos identificados pelas plataformas, como medida de transparência por parte de empresas, demonstrando a conformidade com o PL 2630/2020.

Além disso, defendemos também que o rol de parâmetros estabelecidos para os relatórios semestrais de transparência, elaborados por provedores de aplicação que possuam mais de um milhão de usuários crianças e adolescentes registrados, seja ampliado. De acordo com o art. 22 do PL 2628, os relatórios deverão conter informações sobre canais de denúncia e sistemas e processos de apuração, número de denúncias recebidas e de conteúdos e contas moderadas, as medidas adotadas para combater atos ilícitos e a criação de contas infantis, aprimoramentos técnicos para a proteção de dados pessoais e da privacidade das crianças e adolescentes, bem como das técnicas para auferir o consentimento dos responsáveis. Apesar de trazer pontos importantes, **acreditamos que, neste rol, poderiam ser adicionadas outras obrigações de transparência, como a previsão de haver a avaliação e a atenuação dos riscos identificados pelas plataformas digitais**.

3. Privacidade e proteção de dados

O tema da privacidade e proteção de dados de crianças e adolescentes é muito sensível e demanda uma reflexão profunda, já que o tratamento de dados pessoais deste público pode ter sérias consequências em termos de desenvolvimento de suas personalidades. Por isso, chamamos especial atenção aos dispositivos que tratam deste tema e autorizam a coleta e o tratamento de dados de crianças e adolescentes, a fim de complementar o que tão bem expressa a própria Lei Geral de Proteção de Dados.

Entendemos, primeiramente, que poderia ser ressaltada, ao longo do texto do PL, mas mais especificamente **no art. 4º, a minimização da coleta de dados,** no espírito de proteção do público-alvo do PL, assim como, no mesmo artigo, a **inclusão da privacidade como padrão** em todas as operações que envolvem o desenvolvimento de ferramentas voltadas para este público ou de provável acesso por ele. Neste mesmo espírito, faz-se necessária a **exclusão do art. 17**, já que não é seguro deixar a cargo das plataformas as regras para o tratamento de dados de crianças e adolescentes, inclusive porque tais regras encontram-se estabelecidas na LGPD e nas regulamentações posteriores da ANPD, devendo, na especificidade, ser complementadas por este projeto de lei. Tais medidas já seriam um bom ponto de partida para a proteção da privacidade de crianças e adolescentes em plataformas digitais, mas outras mais específicas também poderiam ser adotadas, robustecendo ainda mais esse arcabouço protetivo.

Uma delas é a **exclusão imediata dos dados utilizados para fins de verificação de idade.** Este é um tema de difícil discussão, já que, do ponto de vista técnico, ainda existem dificuldades atreladas ao desenvolvimento de formas menos intrusivas de chegar a esta finalidade. Portanto, como medida de mitigação de tamanha agressão à proteção de dados pessoais neste ponto, **propomos a inclusão, no art. 18, da obrigação, para as plataformas, de descartar imediatamente os dados coletados para esta finalidade, não permitindo, em nenhuma hipótese, seu uso para finalidades diversas**.

Além disso, cumpre notar que o PL 2628/2022 apresenta um conceito para redes sociais que é muito semelhante ao que consta no PL 2630/2020. No entanto, não traz a importante definição de mensageria instantânea, como faz o PL das *Fake News*, distinguindo-as das demais plataformas digitais, dado seu funcionamento mais específico. A distinção entre redes sociais e os serviços de mensageria é fundamental, uma vez que, em função das peculiaridades deste último, as obrigações estabelecidas para um nem sempre poderão ser as mesmas para o outro, sob o risco de prejudicar a privacidade e a comunicação dos cidadãos brasileiros como um todo.

O art. 17 do PL, por exemplo, estabelece que as plataformas de redes sociais devem monitorar e vedar, no âmbito e no limite técnico de seus serviços, conteúdos que visem à atração evidente de crianças (§ 2°). Já o art. 21 do PL 2628/2022 atualmente propõe que produtos ou serviços de tecnologia operem sistemas e processos que garantam que o provedor ou fornecedor relatem os conteúdos de exploração sexual infantil, detectados ou não.

Na ausência de uma diferenciação clara sobre os serviços, é possível que aplicativos como Whatsapp, Telegram e Signal sejam considerados redes sociais e se tornem obrigados a incorporar mecanismos de monitoramento de conteúdos, colocando em risco a criptografia de ponta-a-ponta adotada nesses serviços, que, além de garantir a privacidade de crianças e adolescentes, protege-os de atores mal intencionados, bem como os dados transmitidos nas plataformas.

Por essa razão, recomendamos a necessidade de **inclusão de uma definição para mensageria instantânea**, como a proposta no PL 2630/2020. No **art. 20**, recomendamos que o dispositivo não seja aplicado para estes mesmos serviços, por riscos à privacidade e segurança de crianças e adolescentes e, no limite, de todos os usuários. Por fim, no mesmo artigo, recomendamos que produtos ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças e adolescentes não sejam obrigados a reduzir o nível de segurança dos seus sistemas, a fim de cumprir obrigações no caput deste artigo.

É necessário encontrar alternativas às propostas como a do art. 20, que poderiam enfraquecer a privacidade e segurança das crianças, adolescentes e dos usuários de forma geral. Uma delas é o estímulo a processos de design que produzam ambientes digitais adequados e seguros para os jovens, onde eles possam desenvolver suas potencialidades de forma saudável e construtiva. Para tal fim, a adoção de técnicas de design persuasivo (*nudge*) deve ter sempre por fim o melhor interesse da criança e o fortalecimento da segurança e da privacidade.

O *nudge* é utilizado com frequência em públicos de todas as faixas etárias para estimular subconscientemente o consumo de produtos e a reprodução de comportamentos negativos, estes últimos chamados de padrões obscuros (dark patterns). Tais táticas são especialmente perigosas para crianças e adolescentes, que encontram-se em estágio de desenvolvimento psicomotor. Essa é razão pela qual defendemos que o PL: **a) traga uma definição específica para o termo *nudge*, com o objetivo de vetar o uso de técnicas de design persuasivo potencialmente negativas para crianças e adolescentes; b) traga também uma definição de padrões obscuros; e c) estimule a adoção de técnicas de design a favor do melhor interesse e da proteção dos direitos das crianças e adolescentes que fazem uso do serviço, incluindo a sua privacidade e segurança online.**

Feitas essas alterações, entendemos que o PL atenderia melhor à proteção da privacidade e da proteção de dados de crianças e adolescentes no âmbito digital.

4. Monitoramento e controle parental

O PL n° 2628/2022 tem um capítulo sobre esses serviços, assim definidos no art. 2º, inciso III: "produto ou serviço de tecnologia da informação destinado ao acompanhamento, por pais ou responsáveis, das ações executadas por crianças e adolescentes em ambientes digitais, a partir do registro ou da transmissão de imagens, sons, informações de localização, de atividade ou outros dados". Ressaltamos a necessidade de cuidado com o tema, dada a grande intrusividade e o potencial de violação de direitos à privacidade, à proteção de dados e à segurança, entre outros.

Além do risco de uso malicioso de serviços de monitoramento, esse tipo de solução tecnológica tende a aumentar a vulnerabilidade de dispositivos e sistemas, driblando a segurança até das comunicações criptografadas de ponta-a-ponta. Ao criar mecanismos que têm controle sobre o dispositivo, esses serviços aumentam sua superfície de ataque. Os serviços de monitoramento têm muito menos incentivos e recursos para sanar suas vulnerabilidades.

Algumas dessas falhas de segurança são consideradas de médio e alto risco, como: i) capturas e compartilhamento de tela; ii) registro de chamadas e de texto; iii) remoção de arquivos feita de forma não segura. No âmbito da rede, há risco em: i) utilização de protocolos antigos e com menor segurança (por exemplo, HTTP); ii) ausência de autenticação correta de API, e; iii) má implementação de *trust managers*, elemento fundamental na avaliação de assinaturas e certificados de segurança em conexões online (Blancaflor et al, 2021; Ali et al, 2021)[3]. Isso coloca crianças e adolescentes em risco ao permitir aos invasores ter total controle do aplicativo de monitoramento infantil, dos dados do usuário e, até, acesso à rede da residência (Ali et al, 2021; Ali et al, 2020)[4].

Outro risco é que tais produtos e serviços geralmente têm seus modelos de negócio baseados também na exploração dos dados coletados para fins de monitoramento, pelos responsáveis, das crianças e adolescentes. Ou seja, podem vulnerabilizar pelo acesso privilegiado aos recursos do sistema e aos dados sensíveis, extensivamente coletados e usados para fins comerciais.

O PL n° 2628/2022 busca proteger a privacidade, a segurança e o direito à informação das crianças e adolescentes, apontando, no art. 13º, que tais serviços devem garantir a inviolabilidade

---

[3] BLANCAFLOR, Eric B.; ANNE J. ANSON, Gerardine; MAE V. ENCINAS, Angela; HUPLO, Kiel C. T.; MARIN, Mark A. V.; ZAMORA, Stephany L. G. A Vulnerability Assessment on the Parental Control Mobile Applications' Security: Status based on the OWASP Security Requirements. *In*: **Proceedings of the International Conference on Industrial Engineering and Operations Management**. Singapore, Singapore: IEOM Society International, 2021. Disponível em: <https://index.ieomsociety.org/index.cfm/article/view/ID/1258>. Acesso em: 18 dez. 2023.
ALI, Suzan; ELGHARABAWY, Mounir; DUCHAUSSOY, Quentin; MANNAN, Mohammad; YOUSSEF, Amr. Parental Controls: Safer Internet Solutions or New Pitfalls? **IEEE Security & Privacy**, v. 19, n. 6, p. 36–46, 2021. Disponível em: <https://ieeexplore.ieee.org/document/9435190/>. Acesso em: 18 dez. 2023.

[4] ALI, Suzan; ELGHARABAWY, Mounir; DUCHAUSSOY, Quentin; MANNAN, Mohammad; YOUSSEF, Amr. Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions. *In*: **Annual Computer Security Applications Conference**. Austin USA: ACM, 2020, p. 69–83. Disponível em: <https://dl.acm.org/doi/10.1145/3427228.3427287>. Acesso em: 18 dez. 2023.
_____. Parental Controls: Safer Internet Solutions or New Pitfalls? **IEEE Security & Privacy**, v. 19, n. 6, p. 36–46, 2021. Disponível em: <https://ieeexplore.ieee.org/document/9435190/>. Acesso em: 18 dez. 2023.

das informações armazenadas e transmitidas aos pais, informar às crianças e aos adolescentes o monitoramento em curso e a orientação pelo melhor interesse da criança e pelo desenvolvimento progressivo de suas capacidades. Inclusive, como apontado no relatório "Privacidade e Proteção" (CRIN e Defend Digital Me, 2023)[5], a vigilância parental pode ter efeitos negativos no desenvolvimento da autonomia das crianças e adolescentes e também efeito contraprodutivo em relação à sua exposição a riscos online.

Vale salientar que grande parte dos abusos e violências que crianças e adolescentes sofrem são realizados por pessoas próximas, como familiares. Mecanismos de monitoramento podem vulnerabilizar ainda mais crianças e adolescentes ao dar mais poder para seus abusadores. É necessário que qualquer legislação sobre a proteção de crianças e adolescentes em ambientes digitais evite as armadilhas comuns, como as falhas da oposição entre criptografia e proteção de crianças e adolescentes. Além disso, deve-se ressaltar que, sendo dever da família, da sociedade e do Estado prezar pela proteção de crianças e adolescentes, não se deve jogar toda a responsabilidade apenas na figura de pais e mães, sob risco de vulnerabilizar o elo mais fraco.

Como sabemos, contudo, não é fácil controlar as finalidades dos usuários ao usar qualquer tecnologia. O sequestro de função é uma prática comum entre usuários. Vale relembrar que diversos desses serviços se valem de justificativas mais nobres, como a proteção de crianças e adolescentes, mas propagandeiam seu potencial de vigiar parceiros românticos, atuando como *stalkerwares*, ou seja, software que permite a perseguição online sem conhecimento da vítima. Aqui, é de especial preocupação as tecnologias servirem de facilitadoras para violências baseadas em gênero.

Como forma de garantir a segurança dos dados sensíveis, em sintonia com o art. 5º deste PL, que prevê que as configurações para as crianças e adolescentes devem ser as mais protetivas para sua privacidade e proteção de dados, e o respeito ao direito fundamental à privacidade e proteção de dados pessoais, recomendamos **a adição dos seguintes parágrafos ao art. 13:**

> § 3º Os serviços de monitoramento devem implementar criptografia ponta-a-ponta para tráfego e armazenamento dos dados, visando acesso aos dados apenas por parte dos responsáveis;
>
> § 4º Todo serviço de monitoramento de dispositivos disponível em território nacional deve informar, de maneira clara, frequente e inequívoca, ao usuário do dispositivo monitorado sobre a atividade de monitoramento em curso;

Além disso, enfatizamos a necessidade de reconhecimento ao longo do PL do princípio do desenvolvimento progressivo de crianças e adolescentes. Este se encontra presente ao longo do texto como diretrizes para produtos ou serviços de tecnologia da informação, mas não enquanto um princípio do PL. Como o próprio princípio informa, crianças e adolescentes desenvolvem capacidades e autonomias de forma progressiva, sendo necessário considerar necessidades diferentes para faixas etárias diferentes.

[5] CRIN (Child Rights International Network); defenddigitalme; IP.rec (Instituto de Pesquisa em Direito e Tecnologia do Recife) (Trad.). **Privacidade e Proteção: Uma abordagem do direito das crianças à criptografia.** 2023. Disponível em: https://ip.rec.br/wp-content/uploads/2023/11/Privacy-and- Protection-Traducao-Portugues-v1.pdf. Acesso em: 14 mar. 2024.

Considerando esse princípio, apontamos como relevante o PL adotar maiores salvaguardas para uma visão ao longo do texto que considere a multiplicidade de experiências de faixas etárias diferentes, sobretudo envolvendo a utilização de ferramentas de controle parental. A adoção de uma visão monolítica, tanto para crianças como para adolescentes, na aplicação dessas ferramentas corre o risco de restringir o desenvolvimento progressivo deles, assim como direitos como o direito à privacidade e à liberdade de expressão.

Legislações como o Age Appropriate Design Code, do Reino Unido, realizam uma importante distinção de faixas etárias, para formulação de serviços e produtos que sejam adequados para diferentes faixas etárias. A divisão do Código realiza divisão de faixas etárias como: 0 - 5 anos; 6 - 9 anos; 10 - 12 anos; 13 - 15 anos; e 16 - 17 anos. Cada uma dessa etapa representaria o ganho de autonomia no mundo e, consequentemente, criticidade e responsabilidades.

A divisão em faixas etárias favorece ainda o direcionamento de informações para os adolescentes sujeitos ao projeto de lei. É possível pensar, a partir da divisão em faixas etárias, as melhores formas de informar e que tipo de informações devem estar disponíveis, concretizando, ao mesmo tempo, o princípio do desenvolvimento progressivo.

Nesse sentido, sugerimos **a inclusão, no parágrafo único do art. 2°, das faixas etárias acima elencadas, e a consequente adequação dos textos dos art. 8°, 11 (incluindo até uma gradação de controle parental de acordo com a faixa etária) e 15 para contemplar distinções, de acordo com cada faixa etária, sobre quais informações devem estar disponíveis e como elas devem ser apresentadas.**

5. Conclusões e recomendações

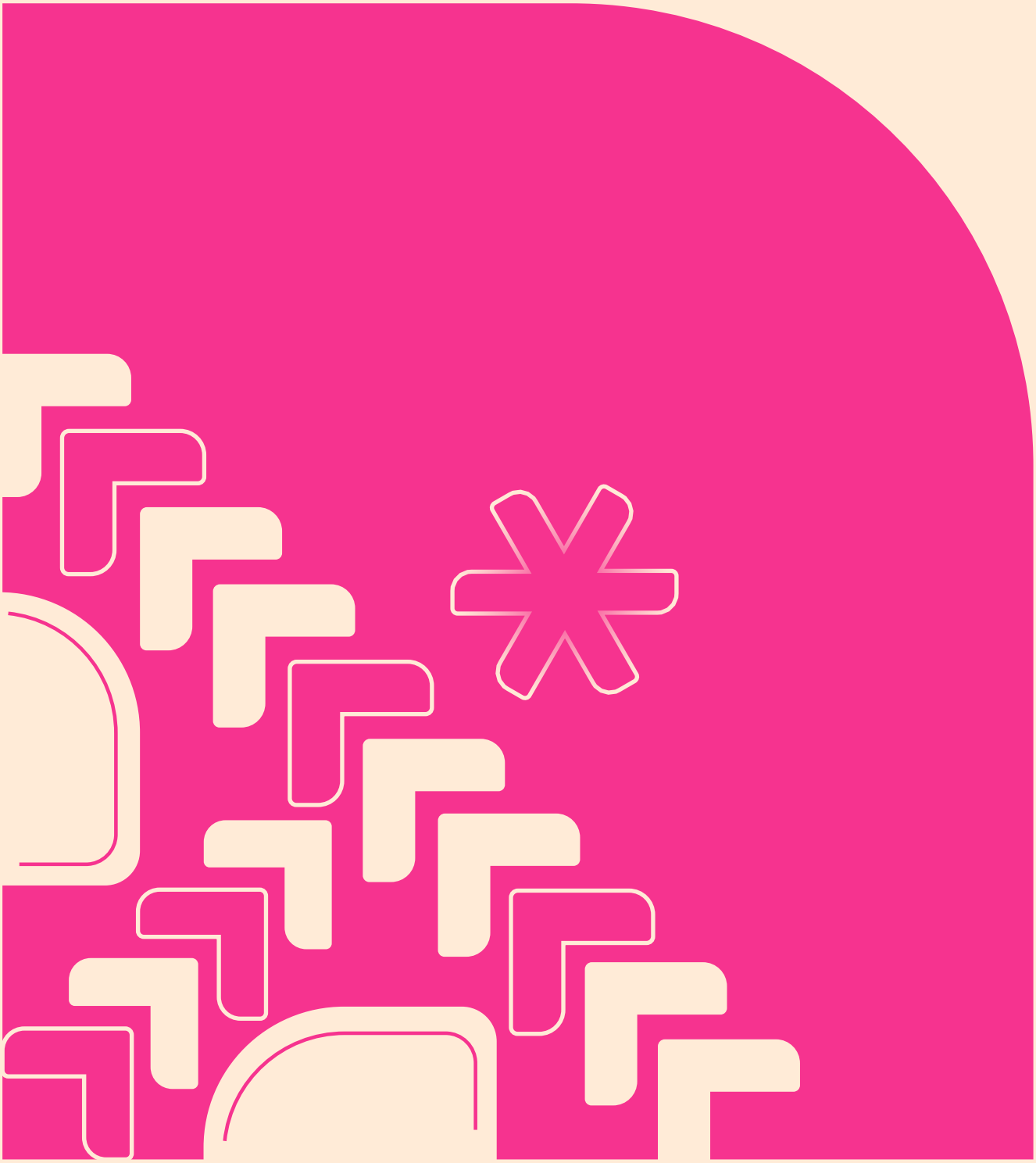
Para sintetizar, listamos aqui as recomendações de alteração no texto do PL 2628/2022, a fim de torná-lo mais protetivo a crianças e adolescentes:

Artigo do PL	**Recomendação**	**Texto alternativo**
Art. 1º	Adição de parágrafo e inciso	§ 1º: Para fins desta lei, provável acesso por crianças e adolescentes será considerada por meio da avaliação da: I - Probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação de crianças e adolescentes II - A facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação.

Art. 2º	Adição de definições	VII - mensageria instantânea: aplicação de Internet cuja principal finalidade seja o envio de mensagens instantâneas para destinatários certos e determinados, incluindo a oferta ou venda de produtos ou serviços e aquelas protegidas por criptografia de ponta-a-ponta, com exceção dos serviços de correio eletrônico; VIII - técnica de design persuasivo (nudge): técnica aplicada na interface do produto ou serviço de tecnologia da informação para induzir o usuário a realizar determinado comportamento, podendo ser utilizada para realização de ações benéficas ou prejudiciais aos seus interesses e preferências positivas ou negativas; IX - Padrões obscuros (dark patterns): técnica de design persuasivo (nudge) em interface de produto ou serviço de tecnologia da informação que visa enganar, prejudicar ou causar danos ao usuário. Parágrafo único: Para os fins desta lei, será considerada a divisão dos usuários nas seguintes faixas etárias: 0 - 5 anos; 6 - 9 anos; 10 - 12 anos; 13 - 15 anos; e 16 - 17 anos.
Art. 4º	Adição de inciso	e VII - a minimização da coleta e proteção de dados pessoais
Art. 5º	Supressão do parágrafo único	
Art. 6º	Adição de inciso e parágrafos	Art. 6º (...) VI - utilização de padrões obscuros (dark patterns). § 1°: Os provedores adotarão as seguintes medidas de atenuação razoáveis, proporcionais e eficazes, direcionadas aos riscos de que trata o art. 6°: I - adaptar a concepção, características ou funcionamento dos serviços, incluindo os sistemas e interfaces; II - adaptar os termos de uso e os critérios e métodos de aplicação; III - adaptar os processos de moderação de conteúdos, incluindo a rapidez e a qualidade do processamento de notificações e quando necessário aplicar remoção de conteúdo, garantidos os procedimentos previstos no Capítulo III; IV - testar e adaptar os sistemas algorítmicos, incluindo os sistemas de priorização e recomendação, de publicidade de plataforma;

		V - reforçar os processos internos, recursos, testes, documentação ou supervisão de qualquer uma das suas atividades; VI - adaptar a interface para prover mais informação aos usuários; e VII - tomar medidas específicas para proteger os direitos de crianças e adolescentes, incluindo adoção e aprimoramento dos sistemas de verificação da idade, desenvolvimento e promoção de ferramentas de controle parental ou de notificação de abusos ou busca de apoio por parte de crianças e adolescentes, conforme o disposto no Capítulo X. § 2º Quando as medidas referidas no § 1° envolverem o uso de sistemas automatizados, essas deverão contemplar salvaguardas que se mostrem apropriadas e eficazes, especialmente por meio de supervisão humana com vistas a garantir a precisão, a proporcionalidade e a não discriminação ilegal ou abusiva. § 3º Os provedores, na forma do regulamento, devem apresentar o relatório de avaliação e atenuação de riscos.
Art. 7º	Adição de parágrafo	Parágrafo único: Quando relevante, faz-se recomendado o uso de técnicas de design persuasivo (nudge) para o melhor interesse da criança, incluindo sua privacidade e segurança.
Art. 8º	Adição de inciso	e IV - Adaptar seus sistemas, processos e interfaces considerando a autonomia progressiva de crianças e adolescentes, conforme as faixas etárias dispostas no art. 2º, parágrafo único, desta lei.
Art. 11	Adição parágrafo	§ 5º Ferramentas de controle parental deverão considerar a autonomia progressiva de crianças e adolescentes, conforme as faixas etárias dispostas no art. 2º, parágrafo único, desta lei.
Art. 13	Adição de parágrafo	§ 3º Os serviços de monitoramento devem implementar criptografia ponta-a-ponta para tráfego e armazenamento dos dados, visando acesso aos dados apenas por parte dos responsáveis; § 4º Todo serviço de monitoramento de dispositivos disponível em território nacional deve informar, de maneira clara, frequente e inequívoca, ao usuário do dispositivo monitorado sobre a atividade de monitoramento em curso;

Art. 15	Modificação de parágrafo	§ 1º É obrigatória a viabilização de desativação de ferramentas de interação dos usuários e sua gerência por meio dos sistemas de controle parental, caso disponível, levando em consideração a autonomia progressiva de crianças e adolescentes de acordo com as faixas etárias constantes do art. 2º, parágrafo único, desta lei.
Art. 18	Supressão	
Art. 19	Adição de parágrafo	§ 2°: Os dados coletados para fim de verificação de idade devem ser descartados imediatamente após a conclusão da referida atividade, não podendo ser utilizados em outras operações.
Art. 20	Adição de parágrafo	§ 3°: Este artigo não se aplica a plataformas de mensageria instantânea.
Art. 23	Adição de inciso	VII - avaliação e atenuação de riscos identificados pelas plataformas.



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife