OUTUBRO, 2021

Proteção de Dados de Crianças e Adolescentes

Sugestões para adoção de diretrizes de boas práticas pela ANPD

AUTORAS

Ana Carolina Brochado Teixeira

Anna Cristina de Carvalho Rettore

EDITORAÇÃO E REVISÃO

Celina Bottino

Christian Perrone

Janaina Costa

Realização:

ITS

Sumário

Sumário interativo: clique para redirecionamento

Resumo Executivo

Introdução

A proteção de dados de crianças e adolescentes é tema de relevância reconhecida internacionalmente, sendo objeto de análise e regulamentação específica por parte das autoridades de proteção de dados ao redor do mundo. Nesse sentido, o tema não pode escapar à atenção da Autoridade Nacional de de Proteção Dados (ANPD), sendo uma oportunidade para desempenhar o papel de ator fundamental na promoção de uma cultura de proteção de dados no país e tornar-se órgão de referência internacional, notadamente no Sul Global, com relação à proteção dos dados pessoais de crianças e adolescentes.

À luz do estudo de boas práticas "Proteção de Dados de Crianças e Adolescentes: O Cenário Brasileiro e Experiência Internacionais"[1], que investigou o tema da proteção de crianças e adolescentes em ambientes digitais em âmbito internacional, bem como o arcabouço normativo brasileiro, tornou-se possível formular algumas sugestões de caminhos para melhor garantir que os dados pessoais de crianças e adolescentes sejam adequadamente protegidos em ambiente digital no país.

Mais do que isso, considerando-se que o art. 32 da Lei Geral de Proteção de Dados (LGPD) prevê expressamente que a Autoridade Nacional poderá sugerir a adoção de padrões e boas práticas para o tratamento de dados pessoais pelo Poder Público, enquanto o art. 50 §3° lhe autoriza a reconhecer e divulgar regras de boas práticas e de governança adotadas por controladores e operadores, tem-se que os possíveis caminhos aqui delineados podem, como de fato se esper a, auxiliar a composição de eventual diretrizes sob a forma de um Guia de Padrões e Boas Práticas a ser elaborado pela Autoridade Nacional de Proteção de Dados Brasileira (ANPD).

Em outros termos, as sugestões adiante apresentadas servem, a um só tempo, como especificações de boas práticas com respaldo internacional trazidos pelo relatório precedente, que desde logo podem ser adotadas por quaisquer agentes de tratamento de dados, públicos ou privados, bem assim como uma proposta à ANPD para o conteúdo de um guia oficial de diretrizes a ser por ela publicado.

De saída, ressalva-se que especificamente a regulação da propaganda dirigida ao público infantojuvenil é uma das áreas sobre as quais os países e organismos internacionais analisados buscam estabelecer critérios mas que acabam por não ter aplicabilidade ao caso brasileiro: o CDC e a Resolução 163 do CONANDA já estabelecem como abusiva qualquer comunicação mercadológica e publicidade à criança e ao adolescente, não há que se falar em estabelecer limites ou regulação a esse tipo de propaganda.

Quanto ao mais, muitas das diretrizes internacionais analisadas podem ser adotadas no Brasil, pois os problemas e os riscos do uso inseguro da internet são, a priori, os mesmos nos mais diversos países do mundo, observando-se apenas seu agravamento nos casos de baixo acesso à educação e parcas condições econômicas, que acabam por reduzir as possibilidades de cuidado parental, uma das formas de minimizar os perigos aos quais a população menor de idade pode se submeter.

Assim, o propósito desta análise é complementar e avançar o escopo trazido pela investigação do arcabouço protetivo da população infantojuvenil pelo direito brasileiro paralelamente aos padrões e boas práticas adotadas em âmbito internacional, abordados no relatório "Boas Práticas: Proteção de Dados de Crianças e Adolescentes". Em consonância com este esforço comparativo das melhores práticas internacionais para promover, pela via da atuação da Autoridade Nacional de Proteção de Dados uma regulação moderna e protetiva dos direitos das crianças e adolescentes. Este documento busca delinear possíveis caminhos para garantir que serviços online protejam adequadamente os dados pessoais de crianças e adolescentes no Brasil. Foram usados como referência as seguintes publicações:

- Information Comissioner's Office (Autoridade de proteção de dados do Reino Unido) - Age appropriate design: a code of practice for online services. Editado em dezembro de 2020 e sob consulta até março de 2021
- Data Protection Commission (Autoridade de proteção de dados da Irlanda) - Fundamentals for a Child-Oriented Approach to Data Processing
- Commission Nationale de l'Informatique et des Libertés(Autoridade de proteção de dados daFrança) - 8 Recommandations pour renforcer la protection des mineurs en ligne
- UNICEF - The Case for Better Governance of Children's Data: A Manifesto
- UNICEF - Children's Online Privacy and Freedom of Expression: Industry Toolkit

- Comitê das Nações Unidas pelos Direitos da Criança - General comment No. 25 on children's rights in relation to the digital environment
- Fundação Getúlio Vargas - Guia de Proteção de Dados Pessoais – Crianças e Adolescentes

Para tanto, o relatório está dividido em 2 grandes partes.

Na primeira parte, analisamos o papel da ANPD na definição de diretrizes para o tratamento de dados pessoais de crianças e adolescentes em ambientes digitais no Brasil.

Na segunda parte, focamos em sugestões concretas para elaboração de diretrizes e boas práticas de governança para proteção de dados pessoais de crianças e adolescentes pela ANPD.

1. O papel e a atuação da ANPD na definição de diretrizes quanto à aplicação da LGPD ao tratamento de dados pessoais de crianças e adolescentes

Diante do arcabouço protetivo estruturado pelo ordenamento brasileiro, que, dentre outras lacunas, não dispõe de forma específica sobre os instrumentos a serem empregados para garantir a verificação de idade e sobre a obtenção do consentimento nos termos legais, é importante que haja iniciativas regulatórias, assim garantindo não apenas que o consentimento dado seja de fato pelos pais, quando for o caso, como também que a estrutura da rede seja adequada às crianças e adolescentes, pois o objetivo é proteger as crianças na internet e não da internet. O Comentário nº 25 sobre os Direitos das Crianças em Ambiente Digital, pelo Comitê dos Direitos das Crianças das Nações Unidas, deixa clara a necessidade de se estabelecer diretrizes de boas práticas – uma obrigação reconhecida ao Poder Público brasileiro no art. 29, parágrafo único, do Marco Civil da Internet e no art. 32 da LGPD, bem como recomendada aos controladores e operadores nos artigos. 50 e 51 da LGPD – para garantia da inclusão digital de crianças e adolescentes mediante uma navegação segura:

> Estados Partes devem divulgar informações e conduzir campanhas de conscientização sobre os direitos da criança no ambiente digital, focando particularmente naquelas cujas ações têm um impacto direto ou indireto sobre as crianças. Devem promover programas educacionais para crianças, mães, pais e cuidadores, o público em geral e os formuladores de políticas para aumentar seu conhecimento dos direitos da criança em relação às oportunidades e riscos associados aos produtos e serviços digitais. Esses programas devem incluir informações sobre como as crianças podem se beneficiar de produtos e serviços digitais e desenvolver sua alfabetização e habilidades digitais, como proteger a privacidade das crianças e prevenir a vitimização e como reconhecer uma criança que é vítima de danos perpetrados online ou off-line e responder adequadamente. Esses programas devem ser informados por meio de pesquisas e consultas com as crianças, mães, pais e cuidadores.[2]

Decerto que o zelo pelos dados de crianças e adolescentes não deve ser imposto somente ao núcleo familiar, pois ele deve competir, em primeiro lugar, ao próprio Poder Público e empresas privadas que realizam coleta e tratamento de dados, que são os agentes hiper suficientes nessa relação. Afinal, a busca pelo atendimento ao melhor interesse da criança e do adolescente também compete ao Estado e à sociedade. Em razão disso, foi recentemente publicado Manifesto em defesa da melhoria da governança de dados de crianças e adolescentes pela UNICEF, clamando pelo aperfeiçoamento da regulamentação e imposição de deveres e sanções nesse sentido. Em tradução livre:

> Esse Manifesto clama para que governos imponham regulamentação mais efetiva a empresas de modo que o ônus da proteção de dados passe das crianças para os próprios governos e empresas. Modelos distributivos de governança de dados devem ser estimulados a fim de garantir às crianças oportunidade de participação, colaboração e co-criação. Às crianças também devem ser garantidos mecanismos significativos de reparação pela violação dos direitos à proteção de seus dados. Governos também devem estabelecer normas que restrinjam a reutilização de dados em poder do setor público, e impor obrigações aos serviços intermediários de tratamento de dados, baseando-se na Lei Europeia de Governança de Dados, a qual estabelece requisitos publicamente verificáveis para a reutilização de dados, a fim de que seja não-discriminatória, proporcional e objetivamente justificável.[3]

Nota-se que a LGPD apresenta diretrizes gerais para proteção dos dados de crianças e adolescentes no ambiente digital, especialmente quando sujeita o tratamento dos dados ao princípio do melhor interesse, quando exige o consentimento específico e destacado de pais ou responsáveis de crianças, e quando impede o condicionamento da presença online ao fornecimento de mais dados que o necessário. Além disso, examinadas as demais normas que tratam do tema no Brasil (Convenção dos Direitos da Criança e do Adolescente e os Comentários da ONU, Constituição Federal, Estatuto da Criança e do Adolescente, Código de Defesa do Consumidor, Resolução do CONANDA e o Marco Civil da Internet), identificou-se que, conquanto esse vasto arcabouço legislativo preveja diversos instrumentos de proteção, persiste uma insuficiência de vetores seguros para orientar práticas que resguardem a privacidade e demais direitos fundamentais no ambiente digital especificamente no caso desses sujeitos, atendendo seu melhor interesse.[4]

Diante da emergência da presença ativa de crianças e adolescentes nesse ambiente, da relevância em suas vidas e desenvolvimento e, especialmente, da complexidade dos direitos e decisões envolvidas, torna-se necessária uma maior especificidade com relação às práticas que melhor se prestam à defesa de seus interesses.

Aqui, em complemento ao estudo hermenêutico de toda a proteção conferida pelo ordenamento jurídico brasileiro, bem como de experiências internacionais do relatório anterior,[5] elaborou-se um conjunto de sugestões de boas práticas que podem, desde logo, ser voluntariamente adotadas por agentes de tratamento de dados de crianças e adolescentes. No entanto, mais além, as sugestões aqui referidas podem compor efetivamente um guia de padrões e diretrizes para o tratamento de dados de crianças e adolescentes a ser elaborado e publicado pela ANPD. Pretende-se que as regras de comportamento esperado dos agentes de tratamento fiquem mais claras e ampliando, com isso, a sua exigibilidade, o que apenas tem a beneficiar os sujeitos alvos de proteção: crianças e adolescentes.

Ademais, ante a ausência de recomendações de boas práticas por autoridades reguladoras na América Latina, verifica-se a pertinência de a ANPD assumir o pioneirismo na regulação no continente latino-americano. Somado a isso, as interações por meio de dispositivos tecnológicos foram internsificadas em razão do distanciamento social imposto pela pandemia da COVID-19. A maior exposição de crianças e adolescentes ao uso contínuo e essencial do ambiente digital, seja para ensino escolar remoto, seja para diversão e relacionamento com amigos e familiares, evidencia a necessidade de regras claras para a proteção de crianças e adolescentes.

Trata-se de um fenômeno mundial. No entanto, em países nos quais há uma regulação de boas práticas na internet, a tutela dos dados pessoais de crianças e adolescentes está muito mais resguardada, pois desenvolvedores de aplicações na internet estão sujeitos à regulação de conduta e padrões, de forma que tais direitos estão efetivamente protegidos.

Por esse motivo, é urgente que a ANPD alavanque a regulação da matéria, por meio da edição de diretrizes e padrões para o tratamento de dados pessoais de crianças e adolescentes, pois o Brasil e demais países da América Latina ainda carecem de uma regulamentação mais específica nesse ponto. Diante da plena vigência da LGPD, é mais do que necessário que os direitos nela previstos alcancem a máxima efetividade, o que só será possível por meio de uma regulação clara, que oferte balizas de condutas e práticas principalmente aos desenvolvedores de aplicações e fornecedores de serviços digitais.

Um mergulho no direito internacional mostrou que diversos países têm instituído orientações para empresas e desenvolvedores de serviços online para a adoção de boas práticas,[6] no sentido de estruturar uma governança na internet que condicione a rede ao cumprimento de sua função de contribuir para o desenvolvimento infantojuvenil, reduzindo os riscos e protegendo os dados. A ANPD pode estabelecer posição de vanguarda ao tomar a frente de uma semelhante atuação na América Latina.

1.1 Medidas a serem consideradas pela ANPD para efetivação do direito à proteção de dados de crianças e adolescentes

Além da edição das diretrizes mencionadas, mostra-se também necessário ampliar a proteção da população infantojuvenil por outros meios, inclusive políticas públicas, para consolidá-la como global e integral. É essencial que sejam desenvolvidas formas para que a Internet ofereça todo seu potencial de aprendizado e interação para a população infantojuvenil de um modo que seja coerente com o sistema protetivo. Sugere-se, dessa forma, também as seguintes medidas para adoção pela ANPD, novamente, à luz do que é efetuado por autoridades com semelhante função em âmbito internacional:

a. promover conscientização e fiscalização, inclusive sobre as sanções administrativas legalmente previstas, com regulamentação de sanções específicas para prejuízos do processamento de dados a crianças e adolescentes, de advertências a multas em percentual do faturamento do negócio, a serem estabelecidas a partir da análise dos riscos aos quais foram submetidos crianças e adolescentes usuários do serviço, bem como o esforço do prestador para se adaptar às condutas determinadas;

b. exigir que o prestador de serviços empreenda esforços razoáveis considerando-se a tecnologia disponível, e que realize um Relatório de Impacto à Proteção de Dados (RIPD) sempre que o serviço envolver o processamento de dados de crianças e adolescentes, salvo se se tratar de dados de baixíssimo risco;[7]

c. realizar consultas públicas sobre processamento de dados pessoais de crianças e adolescentes, viabilizando-se a participação desses sujeitos, que pode se dar de diferentes formas, como por exemplo, por intermédio de suas escolas, as quais também contenham elementos informativos sobre o tema

destinando-se à educação e conscientização sobre proteção de dados a exemplo do que foi realizado pelas autoridades de proteção de dados da França, Irlanda e do Reino Unido como parte essencial do processo de elaboração de seus guias de práticas para o tratamento de dados de crianças e adolescentes.[8] Finalmente, deve-se permitir que os jovens e suas comunidades tenham o direito de falar e serem ouvidos, com efetivo poder de influência, uma boa prática confirmada pelo exemplo do Comitê das Nações Unidas pelos Direitos da Criança para elaboração do Comentário Geral n.º 25 da Convenção dos Direitos da Criança e do Adolescente sobre direitos das crianças no ambiente digital.[9]

d. atentar-se à regulamentação da atuação de *adtechs* (*advertising technology industries*), organizações como agências e redes publicitárias, corretores de dados, analistas de dados, divulgadores e compradores, que processam, em grande volume e velocidade, de forma praticamente invisível, dados obtidos por tecnologias de rastreamento com o objetivo de, a partir de muitos "pedaços" de dados pessoais de um indivíduo, propiciar anúncios sob medida baseando-se no que se sabe e pode ser inferido a respeito dele) no país;

e. estimular que a governança de dados leve em conta diferentes experiências das crianças e adolescentes, reconhecendo-as como um grupo heterogêneo com características que se alteram à medida de seu crescimento e de seu perfil de origem. Em outros termos, individualidades, capacidades e circunstâncias de cada jovem (idade, gênero, deficiência, localização geográfica, origem étnica e perfil socioeconômico) devem ser consideradas pelas estruturas de governança de dados, com flexibilidade suficiente para adaptar-se ao desenvolvimento de cada um e para não os marginalizados;

f. promover meios para que os interesses de crianças e adolescentes em procedimentos administrativos, judiciais e mecanismos de reparação sejam representados, fazendo a integração desses interesses ao trabalho das autoridades de proteção de dados, bem como garantir a presença de instituições de direitos humanos e direitos das crianças e adolescentes para receber e investigar demandas colocadas por crianças e seus representantes;

g. ter pessoal treinado para identificar vítimas, com medidas que precisam abranger múltiplos espaços e serem *child-friendly*, a fim de prevenir a revitimização no contexto investigativo, policial e judicial, o que pode demandar proteção especial de confidencialidade. A reparação deve incluir restituição, compensação e satisfação, e pode demandar pedido de desculpas, correção, remoção de conteúdo e acesso a serviços terapêuticos, dentre outras medidas;

h. garantir recursos adequados à implementação de estruturas de governança de dados inclusivas para crianças e adolescentes, com emprego de pessoal capacitado e conhecedor dos direitos infanto-juvenis, bem como a provisão de fundos para supervisão regulatória; disseminação de informações sobre os direitos de crianças e adolescentes no ambiente digital, com programas educacionais que destaquem benefícios para o desenvolvimento de habilidades e aprendizado; promoção da educação digital sobre a proteção de dados e da privacidade, a evitação de danos e formas de resposta e defesa;

i. promover educação sobre a importância do direito à privacidade e a ameaça que mesmo ações bem-intencionadas podem significar, bem como sobre formas de protegê-los ao mesmo tempo em que se respeita sua privacidade, com monitoramento proporcional ao desenvolvimento da criança e do adolescente, sempre sopesando a necessidade de proteção e o respeito à autonomia. Com relação às ferramentas de controle parental, é necessário promover medidas de conscientização que estimulem o uso e conhecimento a seu respeito, fornecendo suporte aos pais e responsáveis já que não são necessariamente autoexplicativos;

j. promover educação de crianças e adolescentes sobre o ambiente digital e sua estrutura, práticas negociais, estratégias de persuasão e usos de processamento automático de dados pessoais e vigilância;

k. aplicar políticas inovadoras de governança de dados, com o uso de dados pessoais das crianças e adolescentes por autoridades públicas da forma mais eficaz ao mesmo tempo em que resguarda seus direitos, para resolver problemas complexos e acelerar resultados em seu benefício;

l. preencher lacunas urgentes de conhecimento no campo da governança de dados, que demandam investimento em pesquisa, a fim de garantir que as políticas de governança se baseiem em estudos empíricos;

m. fortalecer a colaboração internacional pela governança de dados pessoais de crianças e promover o compartilhamento de políticas e de conhecimento entre países.

Com isso exposto, passa-se ao detalhamento da compilação de sugestões que representam o objetivo primordial do presente documento: a elaboração de diretrizes de boas práticas pela ANPD direcionadas aos agentes de tratamento de dados pessoais de crianças e adolescentes em ambiente digital no Brasil.

2. Sugestões para elaboração de diretrizes de boas práticas e de governança

2.1 Os destinatários de um guia de diretrizes pela ANPD

Inicialmente, nos moldes de guias internacionais, é importante explicitar a quem se destinam e de quem se espera a adoção das boas práticas recomendadas. O *Age appropriate design code* (editado pela ICO - autoridade britânica) se destina a provedores de serviços online destinados ou suscetíveis de serem acessados por crianças e adolescentes.[10] Dessa forma, entende-se que no caso brasileiro os destinatários devem ser:

a. pessoas jurídicas de direito público, que têm como obrigação primária, em decorrência da legislação pátria e internacional, a proteção dos direitos à privacidade e liberdade de expressão de crianças online;
b. fornecedores de produtos e serviços no ambiente digital (aplicativos, programas, websites, jogos, redes sociais, fóruns, mecanismos de busca, serviços de streaming, brinquedos conectados, aparelhos com ou sem tela, inclusive serviços educacionais etc.) – especialmente os desenvolvedores, designers de experiência do usuário e engenheiros de sistema – que processem dados pessoais e que possam despertar o interesse de acesso por crianças e adolescentes;
c. instituições de ensino, que tratam dados de seus alunos menores de idade;
d. hospitais, médicos pediatras e outros profissionais da saúde que armazenem dados sensíveis de crianças e adolescentes;
e. demais empresas e negócios que possam vir a lidar com dados pessoais de crianças e adolescentes.

2.2 Detalhamento de quais dados pessoais de crianças e adolescentes são protegidos: especificação do objeto da proteção

Como visto, a LGPD trata especificamente de dados de crianças e adolescentes somente no art. 14, sendo relevante a adoção, como boa prática, de uma especificação bastante direta sobre a amplitude e abrangência da proteção dos dados que se pretende.

É, por isso, relevante explicitar as informações inferidas a partir de outras e do comportamente online dessa populaçao também que são alvo da proteção tanto quanto os dados pessoais de crianças e adolescentes coletados diretamente. Portanto, também os agentes de tratamento de dados aqueles que não coletem diretamente dados de crianças e adolescentes, mas façam uso de dados inferidos ou de análises do comportamento de um grupo, por exemplo, devem atentar-se aos mesmos cuidados dos que façam a coleta e uso direto, exatamente porque dados indiretos também são dados pessoais.

Além disso, é importante observar que mesmo que seja prestado consentimento pelo adolescente ou pelos pais da criança, nos moldes previstos pelo art. 14 da LGPD, isso não muda a condição de vulnerabilidade desses sujeitos autorizando que, uma vez prestado consentimento, sejam tratados como se adultos fossem. A obtenção do consentimento não autoriza ao agente de tratamento de dados descuidar-se de demais diretrizes de proteção de dados de crianças e adolescentes, sendo certo que, em se tratando de dados pertencentes à população infantojuvenil, não há possibilidade de transacionar sobre a “política de dados”, devendo ainda assim serem mantidas as diretrizes de sigilo, armazenamento e tratamento estabelecidas pela LGPD, com as especificidades para o caso de crianças e adolescentes aqui sugeridas como boas práticas.

2.3 Especificação dos direitos de crianças e adolescentes com relação ao tratamento de seus dados pessoais

É importante que os agentes de tratamento de dados conheçam, de forma específica, quais direitos são garantidos às crianças e adolescentes com cujos dados eles lidam, por se tratar de uma questão abrangente, a fim de que tomem medidas efetivas para promovê-los e divulgá-los de forma acessível em suas plataformas. Os direitos adiante elencados guardam consonância

com as previsões do art. 6° e 18 da LGPD (voltados à população como um todo), e costumam ser elencados por órgãos internacionais como de especial atenção no caso de crianças e adolescentes:

a. Transparência, permitindo ao usuário saber quem possui seus dados pessoais e por quê;
b. Direito de acessar e ter uma cópia de seus dados;
c. Direito de corrigir ou completar dados;
d. Direito de apagar seus dados;
e. Direito de portabilidade, passando de um controlador para outro;
f. Direito de limitar ou restringir o uso de seus dados;
g. Direito de objetar ao processamento de seus dados;
h. Direito à privacidade: desativação padrão de tecnologias de monitoramento e vigilância, coletas de dados para perfilamento, tomada de decisões automática sem envolvimento humano, uso excessivo de controles parentais e compartilhamento de seus dados, seja por serviços digitais, seja por familiares ou amigos.[11]
i. Direito de acesso à informação, não podendo o acesso ser condicionado ao fornecimento de dados pessoais, em consonância, inclusive, com a determinação do art. 14 §4° da LGPD;
j. Direito à liberdade de expressão, cabendo, sempre que possível, garantir às crianças e adolescentes que exerçam diretamente seus direitos em lugar de seus pais ou responsáveis, caso seu estágio de desenvolvimento indique que já tenham condições de assunção responsável da sua vontade;
k. No caso de prestação de serviços de aconselhamento a crianças e adolescentes no ambiente digital (suporte relacionado à saúde e bem-estar físico, mental, sexual ou reprodutivo), não deve haver exigência de consentimento parental para que possam ter acesso ao serviço, ressalvando-se, todavia, que só deve ser oferecido a partir de 12 anos de idade, quando já considerados adolescentes pela lei brasileira.
l. Para o exercício dos direitos decorrentes da proteção de dados diretamente pelo titular, entende-se como boa prática admitir-se a idade mínima de 12 anos, na linha do que prevê o ECA, pois a partir daí a lei brasileira já considera se tratar de um adolescente, e tendo-se em conta, principalmente, que o regime das incapacidades deve ser relativizado para a prática de atos existenciais.[12]

À luz da experiência internacional, deve-se também admitir a possibilidade de se proceder a uma avaliação de competência da criança ou adolescente tendo como parâmetro seu melhor interesse pois, isoladamente, a idade não deve ser tida como métrica confiável para o exercício de direitos, com possibilidade de que crianças e adolescentes de idade maior ou menor que a faixa recomendada possuam ou careçam da competência esperada.

2.4 Diretrizes para o desenvolvimento de serviços no ambiente digital que possam ser acessados por crianças e adolescentes: posturas de adoção recomendada

Como ensina a experiência internacional, desde o desenvolvimento do serviço digital é importante que a proteção de dados de crianças e adolescentes esteja em mente, razão pela qual a adoção de determinadas posturas é altamente recomendável e deve ser esperada. A propósito, o primeiro parâmetro do Age appropriate design code preconiza que o melhor interesse da criança deve ser consideração primária "para o design e desenvolvimento de serviços online que podem ser acessados por crianças e adolescentes".[13] Por sua vez, o guia irlandês tem como um de seus fundamentos também: os provedores de serviços online que rotineiramente processam dados pessoais de crianças devem, por design e por padrão, ter um nível alto e consistente de proteção de dados incorporado em todos os seus serviços.

Inicialmente, importa que exista uma consideração primária ao melhor interesse da criança e do adolescente desde antes do início do desenvolvimento do serviço e em todas as suas etapas, não podendo os interesses dos provedores de serviços interferir na proteção do melhor interesse da criança e do adolescente.

Também se espera que assumam a responsabilidade de seu papel de promoverem a proteção dos dados de crianças e adolescentes sem lhes restringir o acesso às oportunidades de interação e desenvolvimento que tais serviços lhes proporcionam, de modo que não fiquem limitados apenas entre duas opções igualmente prejudiciais: adesão à exigência de disponibilização de dados ou impossibilidade de uso do serviço. Por isso, compete ao desenvolvedor reconhecer que a responsabilidade pela proteção de dados não deve ser da criança ou adolescente, mas dos próprios prestadores,

sejam governos ou empresas privadas, a quem compete garantir que o uso de dados pessoais seja apropriado à idade do usuário, tenha em conta seu melhor interesse e respeite seus direitos, prestando o devido suporte a pais e adolescentes.

Uma boa prática que serve, por um lado, a auxiliar o desenvolvedor no cumprimento dos deveres aqui recomendados, e por outro, como meio de comprovar sua efetiva preocupação com a adoção das posturas recomendadas, é a produção de um Relatório de Impacto à Proteção de Dados (RIPD), nos termos do art. 5º, XVII da LGPD, antes do início do desenvolvimento de serviço que vá ou possa processar dados de crianças e adolescentes. Um RIPD auxilia a identificar e mitigar os riscos que podem ser causados pelo processamento de dados a direitos e liberdades de crianças e adolescentes usuários, e que facilita a conformação às determinações legais e recomendações da ANPD. Boas práticas para a produção de um RIPD são mais detalhadas posteriormente.

Recomenda-se, outrossim, que se identifique se o público do serviço é ou pode vir a ser de crianças e adolescentes, e se haverá coleta de seus dados, sugerindo-se as seguintes medidas para essa identificação: verificar a natureza do serviço; seu conteúdo visual; o uso de personagens animados ou atividades e incentivos voltados para crianças e adolescentes; conteúdo de música ou outros tipos de áudio; a idade de modelos; a presença de celebridades jovens ou que gerem apelo em crianças e adolescentes; a linguagem e outras características do serviço; se há anúncios voltados para crianças e adolescentes; a idade de usuários em serviços semelhantes; e a realização, se possível, de pesquisa independente com o propósito de identificação do público.

Aqui, é importante reforçar que cabe ao agente de tratamento dos dados atentar-se não apenas se seu público-alvo é de crianças e adolescentes, mas se pode acabar por vir a ser, isto é, se o ambiente digital criado poderá despertar a atenção e interesse de crianças e adolescentes ainda que isso não seja o objetivo primário, o que pode ser feito a partir da adoção das medidas acima apontadas. A importância dessa verificação reside no fato de que a ausência de definição do público infantojuvenil como alvo primário não dispensa o agente de tratamento da proteção dos dados pessoais desses sujeitos com os quais venha a lidar.

Caso o desenvolvedor do serviço não opte por identificar se seu público terá crianças e adolescentes, ou não opte por tomar medidas para a verificação de idade, então deverá fornecer proteção de dados padrão para todos os usuários do serviço. Assim, sejam crianças ou adolescentes, sejam adultos, todos os usuários serão alvo de ampla proteção de dados nos padrões exigidos para crianças e adolescentes.

No entanto, caso opte por diferenciar entre usuários adultos e crianças/adolescentes, compete ao desenvolvedor implementar meios para verificação de idade do usuário e obtenção de consentimento parental. A opção por identificar usuários crianças e adolescentes depende do grau de acerto possível, exigindo-se que esse grau de acerto seja tanto maior quanto maiores os riscos postos pelo processamento de dados aos seus direitos e liberdades. Formas para essa identificação são sugeridas posteriormente, à luz da experiência internacional.

Ressalva-se que o simples estabelecimento de idade mínima teórica para uso do serviço não é suficiente. Se um prestador determina que seu serviço não deve ser usado por crianças abaixo de certa idade, deverá prover meios para verificação etária; e se entender que não há como fazê-lo, então deve garantir que, caso venha a ser acessado por crianças e adolescentes abaixo dessa idade, os dados desse usuário serão protegidos.

Quanto aos dados pessoais de crianças e adolescentes que cheguem a ser coletados e/ou tratados, não podem ser utilizados de modo que possa prejudicar seu bem-estar ou contrariar normas em vigor. Como exposto, o uso sempre deve se dar à luz de seu melhor interesse.

No caso de brinquedos e aparelhos conectados (produtos), recomenda-se as mesmas práticas relativas ao desenvolvimento de serviços, acrescendo-se observação específica, todavia, para que informações sobre o uso de dados pessoais sejam destacadas já nos atos de compra/venda e da montagem do produto. Compete ao prestador, ainda, ser capaz de demonstrar que tomou medidas para verificação de idade do usuário e obtenção de consentimento parental, pois a prestação do serviço torna exigível essa responsabilidade.

Por fim, compete ao prestador garantir meios para que os dados pessoais sejam armazenados apenas por “tempo razoável”, efetuando essa previsão de razoabilidade e, desde logo, informando amplamente qual será o tempo específico para armazenamento dos dados em sua plataforma.

2.5 Indicação de formas de verificação de idade do usuário e de obtenção de consentimento parental

É de grande importância que o agente de tratamento de dados busque meios efetivos para uma apuração da real idade do usuário do serviço online, pois a isso grande parte das vezes se vincula a estratificação da proteção dos dados oferecida. Os meios mais atuais para essa apuração, identificados à luz da experiência internacional analisada, são:

a. autodeclaração (com possibilidade de uso de medidas técnicas como o impedimento de alteração da idade declarada após negativa de acesso);
b. uso de inteligência artificial (para verificar, por exemplo, se o uso é compatível com a idade autodeclarada);
c. verificação por terceiro;
d. confirmação de idade de dependentes por usuário titular, quando for o caso; e
e. o uso de 'identificadores fortes', isto é, a exigência de apresentação de documento oficial de identificação, o que se sugere seja feito apenas quando absolutamente necessário, pois crianças e adolescentes podem não possuir tais documentos, resultando-se em indevido impedimento de acesso a serviço apropriado para suas idades, bem como porque causa impacto à privacidade de adultos.

Além disso, é também extremamente importante que se dê especial atenção às formas de obtenção do consentimento parental, para que possa verificar se ele é genuinamente dado pelos pais da criança ao adolescente. A LGPD estabelece no art. 14 §5° que cabe ao controlador "realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis", mas não detalha os meios para fazê-lo. Por isso, também a partir do que vem sendo recomendado e realizado por organismos internacionais, entende-se como boas práticas a adoção das seguintes medidas:

a. Verificar o risco em determinado tratamento de dados: se o processamento de dados for de baixo risco, entende-se admissível apenas verificar o consentimento parental por um e-mail de confirmação; para processamentos de maior risco sugere-se outras medidas, como: consentimento por e-mail ou mensagem de celular; pagamento de valor simbólico por cartão

de crédito ou outro; ligação gratuita para serviço disponibilizado com pessoal treinado para verificação do consentimento; comunicação por videoconferência com o mesmo propósito; fornecimento de documento de identidade a ser compatibilizado com base de dados oficial e posteriormente deletado; transmissão segura de documento de identidade pelos pais, por exemplo, com criptografia, para garantir confidencialidade das trocas; resposta a perguntas concernentes à idade dos pais e não dos filhos; e comparação de foto enviada pelo genitor com foto de um documento oficial por tecnologia de reconhecimento facial; uso de organização de terceiros que fornece identidades digitais e certificados de idade; especificação da data de nascimento do filho pelos pais e os limites do consentimento para uma plataforma acessível pelos serviços online aos quais o filho menor pretende acessar; emissão de um passe de acesso ao filho menor que permite que ele acesse serviços online, após a verificação da sua idade na presença dos pais. Caberá ao prestador determinar qual das medidas é apropriada e proporcional ao tipo de processamento que se pretende, decisão a ser sempre revisada na medida do avanço da tecnologia;

b. Parâmetros para avaliação de risco: para avaliar se o risco do processamento de dados é baixo ou alto, recomenda-se analisar o tipo de dado sendo processado, se de saúde, imagem, vídeo, contatos, religião, orientação sexual; a sensibilidade dos dados, se especiais, financeiros, de terceiros; o tipo de serviço sendo oferecido, se de armazenamento de vídeos ou imagem, educação, saúde, comunicação com conhecidos ou desconhecidos, jogos, compras; acessibilidade dos dados por terceiros, se o serviço se presta a publicizar dados pessoais ou elementos de dados pessoais; se o processamento de dados tem continuidade sendo compartilhado com outras organizações e as razões para fazê-lo (anúncios, marketing, perfilamento); devendo a verificação mais criteriosa possível ocorrer para serviços cujo acesso por crianças e adolescentes é ilegal, como imagens ou vídeos adultos e jogos de azar.

c. Consentimento granular: garantir a possibilidade do consentimento não ser integral, podendo ser parcial. Ou seja, pode-se conferir o consentimento de forma granular apenas para determinadas atividades ou a determinadas pessoas (oferecendo-se opções de consentimento em separado e permitindo a seleção apenas das opções desejadas), excluindo-se por exemplo autorização para compartilhamento de dados;

2.6 Diretrizes para o desenvolvimento de conteúdo de serviços no ambiente digital voltado para crianças e adolescentes, ou que possa a ser por eles acessados

São boas práticas recomendadas para toda e qualquer pessoa física ou jurídica que ofereça um serviço digital ao público infantojuvenil a orientação para que esse serviço contenha determinadas especificidades.

É muito importante garantir transparência das informações, termos e políticas de privacidade do serviço, nos termos do art. 14 §§2° e 6° da LGPD e, mais especificamente: deixá-los em destaque, fazê-los concisos e em linguagem clara, apropriada à idade e com explicações pontuais sobre o uso de dados pessoais sempre que esse uso acontecer, em todos os níveis, mesmo se fornecido consentimento pelos pais ou pelo adolescente. Essas políticas devem conter o nome de todos os operadores que coletam e armazenam os dados das crianças, quais dados são coletados, se a coleta é ativa ou passiva, os usos concretos e potenciais dos dados e se são disponibilizados para terceiros. A depender do caso, a informação pode ser prestada de forma não textual, simplificando o entendimento (desenho, fluxograma, áudio, vídeo, por exemplo), com facilitação de acesso a canal para dúvidas e suporte.

Além disso, devem ser disponibilizadas ferramentas online em destaque e acessíveis para que crianças e adolescentes exerçam seu direito à proteção de dados, e possam reclamar ou tirar dúvidas, assim atendendo determinação do art. 41 §2°, I da LGPD.

Já a configuração padrão do serviço deve ser neutra e de alta privacidade, salvo se demonstrada razão para outro tipo de configuração em consideração ao melhor interesse da criança e do adolescente. A proteção de dados deve estar incorporada em todas as etapas desde o seu desenvolvimento. Não deve competir ao usuário desativar configurações de geolocalização, de monitoramento, de compartilhamento automático de seus dados, de rastreamento (como *cookies*), perfilamento ou tomada de decisões automáticas

em seu lugar. Caso venham a ser coletados, "é importante esclarecer como é realizado o tratamento, se são utilizados *cookies* de sessão (expiram ao fechar o navegador) e/ou *cookies* persistentes (permanecem no computador até que sejam excluídos) e para quais finalidades. Deve-se explicitar a possibilidade de remoção ou desabilitação de *cookies*, e.g. persistentes, e por meio de qual ferramenta, podendo-se esclarecer que ao fazer isso, algumas áreas da plataforma poderão não funcionar corretamente".[14]

A coleta e armazenamento de dados pessoais deve ser a mínima necessária para a prestação do serviço com o qual a criança ou adolescente pode interagir. Devem ser apresentadas opções, separadamente, para escolha dos elementos que se deseja ativar, por exemplo, categorizando-se dados coletados para cada atividade, pois cada uma pode demandar dados diferentes, tornando desnecessária a coleta de todos por todo o tempo. Sugere-se, ainda, avisos sobre o uso e cessação da coleta de dados quando eles deixam de ser necessários.

Não devem ser compartilhados dados de crianças e adolescentes com terceiros sem consentimento específico, atendendo-se disposição do art. 7° §5° da LGPD, salvo se demonstrada importante razão para fazê-lo em consideração ao melhor interesse da criança e do adolescente. A título exemplificativo da possibilidade de compartilhamento de dados da população infantojuvenil prescindindo-se de consentimento, em 3 de maio de 2021 foi publicado o Decreto-Lei 16/21, que promulgou tratado do Mercosul para a criação de base de dados compartilhada sobre crianças e adolescentes em situação de vulnerabilidade, a fim de combater crimes como o tráfico e sequestro de menores.[15] No caso, serão disponibilizadas pelos países signatários informações sobre o paradeiro de crianças e adolescentes, bem como comunicados de restrições à saída do país de origem, os quais poderão ser acessados somente por autoridades competentes.[16]

Recomenda-se que a geolocalização esteja desativada por padrão, salvo forte razão em contrário para fazê-lo considerando o melhor interesse da criança e do adolescente. Quando ativada, isso deve ser sinalizado ao usuário de maneira perceptível, devendo ser automaticamente desativada após o final de cada sessão.

Por fim, se o serviço online possuir ferramenta de controle parental, seu uso deve ser informado à criança ou adolescente em linguagem apropriada à sua idade. Enquanto ativado o monitoramento de atividade online ou de localização, tal deve ser sinalizado de maneira perceptível à criança ou adolescente.

Além disso, quando da idealização das ferramentas de controle parental, é necessário balanceá-las com o direito à privacidade e liberdade de expressão da criança e do adolescente. Os mecanismos de controle não devem substituir a comunicação com os filhos: ao contrário, é recomendável conscientizar diretamente crianças e adolescentes sobre os riscos postos pelo ambiente digital, de modo que o controle possa ser exercido em parceria e por meio de comunicação transparente.[17]

Análise específica de *benchmarking* requisitada pela Comissão Europeia em 2017 identificou não haver uma única ferramenta de controle parental que atenda todas as preocupações dos genitores, exigindo seja feita uma análise caso a caso, segundo as necessidades e o dispositivo a se monitorar, bem como a adoção de uma combinação de ferramentas.[18]

2.7 Diretrizes para prestação de serviços no ambiente digital que possam ser acessados por crianças e adolescentes: posturas repudiadas

Algumas condutas devem ser evitadas por colocar os dados em risco ou causarem prejuízo às crianças e adolescentes, sendo essa listagem meramente exemplificativa.

Por exemplo, entende-se que a opção de perfilamento deve estar desativada por padrão, salvo se houver forte razão em contrário para fazê-lo considerando o melhor interesse da criança e do adolescente. O perfilamento só deve ocorrer se tomadas as medidas adequadas para proteção da criança ou adolescente de quaisquer efeitos prejudiciais, pois o perfilamento com finalidade de *marketing* comportamental e para tomada de decisões automáticas pelo usuário criança ou adolescente é proibido no Brasil.

Outrossim, não devem ser utilizadas técnicas de encorajamento (*nudge techniques*) para direcionar ou estimular crianças e adolescentes a fornecer dados pessoais desnecessariamente, ou para reduzir/desativar a proteção aos seus dados pessoais, tampouco para incentivar sua permanência online. O mesmo se aplica a práticas baseadas em *neuromarketing*, *emotional analytics*, anúncios imersivos e realidades virtuais ou aumentadas para promoção de produtos, aplicações e serviços.

No mesmo sentido, mecanismos automáticos de busca ou sistemas de recomendações não devem priorizar conteúdo pago com motivação comercial ou política, sobrepondo-se às escolhas da criança e do adolescente ou ao seu direito à informação, à formação e expressão de opinião no ambiente digital.

É de extrema importância, ademais, que as maiores dificuldades postas ao tratamento de dados de crianças e adolescentes não acabe por resultar na exclusão desses sujeitos ou piora de sua experiência. Isto é, se o serviço é direcionado ou pode ser usado por crianças e adolescentes, a existência de obrigações a serem cumpridas para proteção de seus dados não pode ser superada mediante a sua simples exclusão ou piora de sua experiência, atendendo-se assim inclusive a determinação do §4° do art. 14 da LGPD.

Aliás, é relevante a preocupação com a possibilidade de que crianças e adolescentes sejam estimulados a mentirem suas idades se tiverem a percepção de que a verificação as impede de ter acesso à modalidade "mais completa" do serviço, resultando na contraproducente piora da proteção aos seus dados pessoais, o que reforça a necessidade de que não sejam excluídas do acesso ao argumento de proteção de seus dados, especialmente no caso de serviços que motivam sua busca pela plataforma. O operador não deve poder condicionar a participação da criança ou adolescente ao fornecimento de mais dados que o necessário, em consonância com o §4° do art. 14 da LGPD, prática essa aplicável também aos órgãos e entidades públicas, tal como reconhece o Guia de Boas Práticas para Implementação na Administração Pública Federal referente à LGPD: "Caso os órgãos e entidades públicas desenvolvam jogos, aplicações de internet ou outras atividades semelhantes voltadas ao público infantojuvenil, a coleta de dados pessoais dos jovens deverá restringir-se ao estritamente necessário à atividade proposta".[19]

2.8 Orientações para a elaboração de um Relatório de Impacto à Proteção de Dados (RIPD): um passo-a-passo da proteção de dados pessoais de crianças e adolescentes que documenta a boa atuação do agente

A pessoa física ou jurídica que pretende lançar um serviço digital deverá verificar, antes do lançamento do serviço, se crianças e adolescentes irão ou poderão acessá-lo e de quais idades. Em caso positivo, é recomendável a elaboração de um RIPD. Esse relatório deverá especificar, por exemplo:

a. quais serão as formas de identificá-las, que dados serão obtidos, se deve haver preocupação em evitar perigos e quais, e quais os interesses comerciais presentes;

b. deve ser descrita a natureza, o propósito e o contexto do processamento de dados, incluindo-se se o serviço é direcionado a crianças e adolescentes ou o quanto é provável que elas queiram acessá-lo, planos de controle parental, verificação de idade, obtenção de consentimento, os benefícios para crianças e adolescentes, os interesses comerciais envolvidos, se haverá perfilamento, geolocalização, técnicas de encorajamento, processamento de dados sensíveis, diretos ou inferidos (e, nesses últimos casos, tratando-se de medidas não recomendadas para crianças e adolescentes, como será evitado que se apliquem a crianças e adolescentes ou, em último caso, justificando-se razão pela qual atenderiam seu melhor interesse), se existe razão para preocupação com riscos a serem causados à criança e adolescente, suas responsabilidades legais como processador de dados, bem como pesquisas e consultas realizadas para o desenvolvimento em prol do melhor interesse dos usuários infantojuvenis;[20]

c. devem ser ouvidos pais, crianças e adolescentes, representantes governamentais e de associações de proteção aos interesses de crianças e adolescentes para a elaboração do serviço, com registro no relatório;

d. deve-se, também, identificar e avaliar riscos potenciais, bem como meios para reduzi-los, a saber: possibilidade de o serviço causar danos emocionais, situações de *bullying*, acesso a conteúdo inadequado para a idade, encorajamento de comportamentos perigosos, excessivo uso de tela, prejudicar a autoridade parental e perda de autonomia pelo uso de dados;

Por fim, é importante fazer o registro e a publicação da conclusão a que se chegou, junto a quaisquer planos adicionais que se pretenda adotar.[21] Se houver algum risco elevado que se entenda não poder ser mitigado, é importante consultar previamente a ANPD a fim de prosseguir com o desenvolvimento e lançamento do serviço.[22]

Como se observa desse detalhamento, o desenvolvimento desse relatório incentiva ao agente de tratamento de dados a observar, documentadamente, uma série de passos no sentido de atentar-se à efetivação da proteção de dados de crianças e adolescentes desde o planejamento do desenvolvimento do serviço propriamente dito, auxiliando a identificação e a mitigação dos riscos que o processamento de dados pretendidos podem colocar a direitos e liberdades de crianças e adolescentes usuários. Assim, presta-se a facilitar o cumprimento dos deveres esperados ao mesmo tempo em que comprova a diligência do agente pela adoção de medidas recomendadas.

3 Conclusão

No estudo anterior, "Proteção de Dados de Crianças e Adolescentes: O Cenário Brasileiro e Experiência Internacionais,"[23] é possível vislumbrar um movimento internacional de buscar regulamentar de maneira mais efetiva a proteção de dados de crianças e adolescentes e encontrar algumas reflexões acerca de como o ordenamento pátrio poderia se beneficiar daquele esforço comparativo e se utilizar das melhores práticas internacionais para promover, pela via da regulação pela autoridade nacional de proteção de dados, uma regulação moderna e protetiva dos direitos das crianças e adolescentes.

Neste documento, a partir da análise precedente, são apresentadas sugestões concretas para uma regulação de proteção de dados de crianças e adolescentes a ser propiciada pela ANPD, depuradas das melhores práticas internacionais e dos principais desafios encontrados para efetivação da LGPD, em consonância com o arcabouço brasileiro protetivo dos direitos das crianças e adolescentes.

Assim, as sugestões apresentadas servem, a um só tempo, como especificações de boas práticas com respaldo internacional trazidos pelo relatório precedente, que desde logo podem ser adotadas por quaisquer agentes de tratamento de dados, públicos ou privados, bem como uma proposta de diretrizes que poderiam vir a compor uma regulamentação por parte da ANPD.

Notas

1

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. Proteção de Dados de Crianças e Adolescentes: O Cenário Brasileiro e Experiência Internacionais. Agosto 2021. Rio de Janeiro: Instituto de Tecnologia e Sociedade. Disponível em: https://itsrio.org/pt/publicacoes/relatorio-de-boas-praticas-protecao-de-dados-de-criancas-e-adolescentes/. Acesso em 30.09.2021

2

COMITÊ DOS DIREITOS DA CRIANÇA DAS NAÇÕES UNIDAS. Comentário geral nº 25 (2021) sobre os Direitos das Crianças em relação ao ambiente digital, p. 7. Trad.: Instituto Alana. São Paulo: Criança e Consumo. Disponível em https://criancaeconsumo.org.br/wp-content/uploads/2021/04/comentario-geral-n-25-2021.pdf. Acesso em 28.05.2021.

3

BYRNE, Jasmina; DAY, Emma; RAFTREE, Linda. The Case for Better Governance of Children's Data: A Manifesto. Mai. 2021. Nova York: Office of Global Insight and Policy, United Nations Children's Fund. Disponível em: https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto. Acesso em: 28 mai. 2021. Traduzido do original: "This Manifesto calls for governments to impose stronger regulations on companies in order to shift the onus for data protection from children to companies and governments. Distributive models of data governance should be promoted in order to provide opportunities for child participation, collaboration, and co-creation. Children should also be afforded meaningful redress mechanisms for violations of data rights. Governments themselves must also put in place rules to restrict the reuse of children's data held by the public sector, and to impose obligations on data intermediary services, drawing on the new European Data Governance Act, which requires publicly available conditions for the re-use of data that are non-discriminatory, proportionate and objectively justified".

4

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. Proteção de Dados de Crianças e Adolescentes: O Cenário Brasileiro e Experiência Internacionais. Agosto 2021. Rio de Janeiro: Instituto de Tecnologia e Sociedade. Disponível em: https://itsrio.org/pt/publicacoes/relatorio-de-boas-praticas-protecao-de-dados-de-criancas-e-adolescentes/. Acesso em 30.09.2021

5

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. Proteção de Dados de Crianças e Adolescentes: O Cenário Brasileiro e Experiência Internacionais. Agosto 2021. Rio de Janeiro: Instituto de Tecnologia e Sociedade. Disponível em: https://itsrio.org/pt/publicacoes/relatorio-de-boas-praticas-protecao-de-dados-de-criancas-e-adolescentes/. Acesso em 30.09.2021

6

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. Proteção de Dados de Crianças e Adolescentes: O Cenário Brasileiro e Experiência Internacionais. Agosto 2021. Rio de Janeiro: Instituto de Tecnologia e Sociedade. Disponível em: https://itsrio.org/pt/publicacoes/relatorio-de-boas-praticas-protecao-de-dados-de-criancas-e-adolescentes/. Acesso em 30.09.2021

7

Dados de baixíssimo risco são aqueles que não envolvem dados sensíveis, armazenamento de dados, que não são acessíveis por terceiros, não são publicizados nem têm seus elementos levados a público e que não são compartilhados com outras organizações.

8

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. Proteção de Dados de Crianças e Adolescentes: O Cenário Brasileiro e Experiência Internacionais. Agosto 2021. Rio de Janeiro: Instituto de Tecnologia e Sociedade. Disponível em: https://itsrio.org/pt/publicacoes/relatorio-de-boas-praticas-protecao-de-dados-de-criancas-e-adolescentes/. Acesso em 30.09.2021

9

"In addition to considering children's needs and perspectives, policy makers should give children a voice in the international debates on technology regulation. Laws and international instruments should be adopted with these ideas in mind, as a fundamental way of ensuring that children's perspectives and needs are considered and respected." Vide : Viola de Azevedo Cunha, Mario (2017). Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy, Innocenti Discussion Papers no. 2017-03, UNICEF Office of Research - Innocenti, Florence.

10

INFORMATION COMMISSIONER 'S OFFICE. Design Apropriado para a Idade: Código de Práticas para Serviços On-line. Trad.: Instituto de Tecnologia e Sociedade. Rio de Janeiro. Disponível em: https://somos.itsrio.org/relatorio-ico. Acesso em 30.09.2021.

11

Aliás, a esse respeito, o Guia de Boas Práticas para a Proteção de Dados de Crianças e Adolescentes publicado pela Fundação Getúlio Vargas contém a seguinte indicação sobre disponibilização de dados como notas e frequência do filho adolescente aos genitores: "caso os responsáveis legais entrem em contato com a instituição de ensino para verificar notas e frequência do adolescente, ocorrendo oposição do titular, recomenda-se que os dados não sejam fornecidos sem a sua autorização, determinação de autoridade competente ou ordem judicial. Veja que, nessas situações é muito recorrente que estejam envolvidos conflitos familiares e jurídicos, como disputa de guarda, alienação parental, entre outros".11 Paralelamente, o art. 1.584 §6° do Código Civil determina que "[q]ualquer estabelecimento público ou privado é obrigado a prestar informações a qualquer dos genitores sobre os filhos destes, sob pena de multa de R$ 200,00 (duzentos reais) a R$ 500,00 (quinhentos reais) por dia pelo não atendimento da solicitação". Aí, tem-se em confronto o direito à privacidade do titular e o poder-dever da autoridade parental, com a solução devendo partir da análise do que atende ao melhor interesse da criança e do adolescente e admitindo-se, mediante as circunstâncias do caso concreto, que a própria instituição de ensino reclame intervenção judicial.

Com relação ao direito à privacidade de crianças e adolescentes, também é importante observar o compartilhamento de dados (informações, imagens, vídeos) dos filhos pelos pais, que devem se atentar à possibilidade de sharenting, um tipo de violação da privacidade e do melhor interesse exatamente de quem se deve proteger. Recomenda-se ao agente de tratamento de dados, inclusive, desestimular a prática, ou promover espaços explicativos sobre essa prática e seus prejuízos em sua plataforma;Para uma análise sobre o sharenting em tempos de quarentena, confira-se: MEDON, Filipe. (Over)sharenting: a superexposição da imagem e dos dados da criança na internet e o papel da autoridade parental. In: DADALTO, Luciana; TEIXEIRA, Ana Carolina Brochado. Autoridade parental: dilemas e desafios contemporâneos. 2ª ed. Indaiatuba: Foco, 2021, p. 351-375.

12

PERLINGIERI, Pietro. La personalità umana nell'ordinamento giuridico. Camerino-Napoli: Edizioni Scientifiche Italiane, 1972; RODRIGUES, Rafael Garcia. A pessoa e o ser humano no novo Código Civil.

In TEPEDINO, Gustavo (Coord.). A parte geral do Código Civil: estudos na perspectiva civil-constitucional. Rio de Janeiro: Renovar, 2003, p.24; TEIXEIRA, Ana Carolina Brochado. Integridade psíquica e capacidade de exercício. Revista Trimestral de Direito Civil, v. 33, p. 3-36, 2008; MEIRELES, Rose Melo Vencelau. Autonomia privada e dignidade humana. Rio de Janeiro: Renovar, 2009; MENEZES, Joyceane B. A capacidade dos incapazes: o diálogo entre a Convenção da ONU sobre os direitos da pessoa com deficiência e o Código Civil Brasileiro. In Direito Civil Constitucional: A ressignificação da função dos institutos fundamentais do Direito Civil Contemporâneo e suas consequências. Org.: Carlos Eduardo P. Ruzyk, Eduardo Nunes de Souza, Joyceane B Menezes e Marcos Ehrhardt Junior. Florianópolis: Conceito, 2014, p.51-74; LÔBO, Paulo. Direito Civil. Parte geral. São Paulo: Saraiva, 2010; SÁ, Maria de Fátima Freire; MOUREIRA, Diogo Luna. A Capacidade dos Incapazes: saúde mental e uma releitura da teoria das incapacidades no direito privado. 1. ed. Rio de Janeiro: Lumen Juris, 2011.

13

INFORMATION COMMISSIONER 'S OFFICE. Design Apropriado para a Idade: Código de Práticas para Serviços On-line. Trad.: Instituto de Tecnologia e Sociedade. Rio de Janeiro. Disponível em: https://somos.itsrio.org/relatorio-ico. Acesso em 30.09.2021.

14

FUNDAÇÃO GETÚLIO VARGAS. Guia de Proteção de Dados Pessoais – Crianças e Adolescentes, p. 25. Out. 2020. Disponível em https://portal.fgv.br/sites/portal.fgv.br/files/criancas_e_adolescentes.pdf. Acesso em 05.06.2021.

15

Por outro lado o mercosul estabeleceu no início desse ano regras para o tráfego transfronteiriço de dados pessoais, vide: https://www.conjur.com.br/2021-fev-17/opiniao-festa-protecao-dados-america-sul

16

JÚNIOR, Janary. Congresso promulga acordo para proteção a crianças e adolescentes no continente. In: Folha de Pernambuco. 03.05.2021. Disponível em https://www.folhape.com.br/politica/congresso-promulga-acordo-para-protecao-a-criancas-e-adolescentes-no/182172/. Acesso em 05.06.2021.

17

EUROPEAN COMISSION. Benchmarking of parental control tools for the online protection of children, p. 5. 2017. Disponível em https://digital-strategy.ec.europa.eu/en/library/benchmarking-parental-control-tools-online-protection-children. Acesso em 05.06.2021. O Governo Federal brasileiro disponibiliza orientações sobre ferramentas de controle parental em: https://www.justica.gov.br/seus-direitos/classificacao/Controle-parental.

18

EUROPEAN COMISSION. Benchmarking of parental control tools for the online protection of children, p. 6. 2017. Disponível em https://digital-strategy.ec.europa.eu/en/library/benchmarking-parental-control-tools-online-protection-children. Acesso em 05.06.2021.

19

GOV.BR. Guia de Boas Práticas para Implementação na Administração Pública Federal – Lei Geral de Proteção de Dados, p. 30. Ago. 2020, 2ª ed. Disponível em https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em 05.06.2021.

20

INFORMATION COMISSIONER'S OFFICE. Age appropriate design: a code of practice for online services, p. 29. 02.09.2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em 05.06.2021.

21

INFORMATION COMISSIONER'S OFFICE. Age appropriate design: a code of practice for online services, p. 29. 02.09.2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em 05.06.2021.

22

INFORMATION COMISSIONER'S OFFICE. Age appropriate design: a code of practice for online services, p. 29. 02.09.2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em 05.06.2021.

23

https://itsrio.org/pt/publicacoes/relatorio-de-boas-praticas-protecao-de-dados-de-criancas-e-adolescentes/

Sobre os autores

Ana Carolina Brochado Teixeira
Doutora em Direito Civil pela UERJ. Mestre em Direito Privado pela PUC Minas. Coordenadora da Revista Brasileira de Direito Civil – RBDCivil. Professora de Direito Civil do Centro Universitário UNA. Advogada.

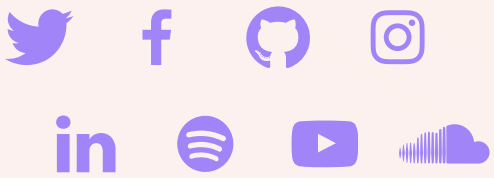
Anna Cristina de Carvalho Rettore
Mestre em Direito Privado pela PUC Minas. Advogada.

Celina Bottino
Mestre em direitos humanos pela Universidade de Harvard. Foi pesquisadora da Human Rights Watch em Nova York. Supervisora da Clínica de Direitos Humanos da FGV Direito-Rio. Foi consultora da Clínica de Direitos Humanos de Harvard e pesquisadora do ISER. Diretora de projetos do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Christian Perrone
Pesquisador Fulbright (Universidade de Georgetown, EUA). Doutorando em Direito Internacional (UERJ); Mestre em Direito Internacional (L.L.M/ Universidade de Cambridge, Reino Unido). Ex-Secretário da Comissão Jurídica Interamericana da OEA. Coordenador da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Janaina Costa
Advogada. Pós-Doutoranda em Direito Digital (UERJ); Mestre em Desenvolvimento Econômico e Social pelo IEDES - Paris 1 Panthéon-Sorbonne; Bacharel em Direito (UFMG). Ex-diretora da Diretoria de Convênios e Prestação de Contas da SEC de Minas Gerais. Pesquisadora Sênior da área de Direito e Tecnologia Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Acesse nossas redes



itsrio.org