Autoridade Nacional de Proteção de Dados (ANPD)
Tomada de Subsídios: Tratamento de Dados Pessoais de Crianças e Adolescentes
Comments of Computer & Communications Industry Association (CCIA)[1]

I. Principle of best interest

1. In addition to the aspects covered in Statement CD/ANPD nº 01/2022 and in the Guidance on the legal hypothesis of legitimate interest, which issues related to the principle of best interest require specific guidance or regulation by the ANPD?

What is in the best interests of any individual child should be determined by parents, not dictated by politicians or private businesses. When considering the principle of best interest, it is also important to consider challenges with operationalization at scale, and avoiding creating moving goalposts for compliance. The benefit of a dynamic marketplace is that online businesses are able to tailor their services and products to what is most relevant and useful to their specific audience. Private online businesses are not able to coherently or consistently make diagnostic assessments of users, including their mental and physical health.

I. Princípio do melhor interesse

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

O que é de melhor interesse para cada criança deve ser determinado pelos pais e não ditado por políticos ou empresas privadas. Ao considerar o princípio do melhor interesse, também é importante considerar os desafios da operacionalização em escala e evitar a criação de metas móveis que impeçam a conformidade. A vantagem de um mercado dinâmico é que as empresas online são capazes de adaptar os seus serviços e produtos ao que é mais relevante e útil para o seu público específico. As empresas privadas que operam online não são capazes de fazer avaliações diagnósticas dos usuários de forma coerente ou consistente, incluindo a sua saúde física e mental.

2. Are there specific situations or contexts in the processing of personal data of children and adolescents that require greater attention and detail regarding the principle of best interests? If so, indicate which situations or contexts were identified and the main issues to be addressed.

Children are entitled to a higher level of security and privacy in their online experiences. Our

[1] Submitted on July 16, 2024 in Portuguese via https://www.gov.br/participamaisbrasil/tscriancaeadolescente. Each question and answer is available in this document both in English and then the Portuguese translation as submitted.

industry has been actively engaged in various initiatives to integrate robust protective design features into their websites and platforms. The companies we represent are leading the effort to implement settings and parental tools to individually tailor younger users' online use to the content and services that are suited to their unique lived experience and developmental needs.

Some examples can be found here: https://ccianet.org/wp-content/uploads/2023/02/General-Child-Safety-Mechanisms_Fact-Sheet.pdf

2. *Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.*

As crianças têm direito a um nível mais elevado de segurança e privacidade nas suas experiências online. Nossa indústria tem se envolvido ativamente em diversas iniciativas para integrar recursos robustos de design de proteção em seus sites e plataformas. As empresas que representamos lideram esforços para implementar configurações e ferramentas de controle parental para adaptar individualmente a utilização online dos usuários mais jovens aos tipos de conteúdos e serviços mais adequados à sua experiência de vida única e às suas necessidades de desenvolvimento.

Alguns exemplos podem ser encontrados aqui: https://ccianet.org/wp-content/uploads/2023/02/General-Child-Safety-Mechanisms_Fact-Sheet.pdf

II. Consent

1. **What criteria or parameters must be observed to obtain "specific and prominent" consent from parents or legal guardians?**

Generally, consent refers to a clear affirmative act that represents a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including through electronic means, or any other unambiguous affirmative action such as a verbal statement if using a home smart device.

The particular method a business chooses to implement to obtain consent from a consumer, including a parent or guardian, will depend upon a variety of considerations: security and privacy, accessibility and equity, and other risks such as user hesitancy to provide certain personal information. However, in some circumstances, there is no explanation of how a company can verify the relationship between a young user and the consenting adult, especially if the consenting parent or guardian does not have an account.

II. Consentimento

1. *Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?*

De maneira geral, o consentimento se refere a um ato claro e afirmativo que representa um aceite específico, informado e inequívoco dado livremente pelo consumidor para processar seus dados pessoais. O consentimento pode incluir uma declaração por escrito, inclusive por meio eletrônico, ou qualquer outra ação afirmativa inequívoca, como uma declaração verbal, se estiver usando um dispositivo doméstico inteligente (smart device).

O método específico que uma empresa escolhe implementar para obter o consentimento de um consumidor, incluindo de um dos pais ou guardião, dependerá de uma variedade de considerações: segurança e privacidade, acessibilidade e equidade, e outros riscos como a hesitação do usuário em fornecer determinadas informações pessoais. Mas, em algumas circunstâncias, não há explicação sobre como uma empresa pode verificar a relação entre um jovem utilizador e o adulto que consentiu, especialmente se o pai, mãe ou tutor que consentiu não tiver uma conta na respectiva plataforma.

2. **Considering good practices, available technologies and the principles of the LGPD, in particular the principles of purpose, necessity and adequacy, as well as the legal requirement to adopt "all reasonable efforts", what measures and mechanisms do controllers should they adopt, especially in the digital environment, to enable and verify that consent was provided by the child's parents or guardians?**

Businesses that provide digital services or products directed to children or younger users utilize various methods for obtaining parental or guardian consent before collecting the child's personal information. Whether they provide a website or mobile gaming application, such organizations must use a method that is reasonably designed in light of available technology to ensure that the person giving consent is the child's parent. The identification process can consist of: calling a phone to a toll-free number or live video conference; providing government-issued ID to check against a database; processing a credit or debit card to provide notice to the adult user; or providing a set of knowledge-based questions.

As technology continues to advance, so may the methods chosen by a business. This flexible standard provides businesses with sufficient guidance to continue developing and improving their services.

However, implementation challenges still exist. For instance, many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions — including in Brazil where it's common to have multiple surnames. Further, some households may not be proficient in the same language(s) as their children, are not technologically savvy, or work multiple jobs. This raises serious equity concerns, especially considering those households that lack the necessary government identification or other mechanisms to access an online service or platform — blocking teens from accessing helpful services and age-appropriate information.

2. *Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?*

As empresas que fornecem serviços ou produtos digitais direcionados a crianças ou usuários mais jovens utilizam vários métodos para obter o consentimento dos pais ou responsáveis antes de coletar as informações pessoais da criança. Seja um website ou uma aplicação de jogo móvel, essas organizações devem utilizar um método que seja razoavelmente concebido à luz da tecnologia disponível para garantir que a pessoa que dá o consentimento é o responsável da criança. O processo de identificação pode consistir em: ligação telefônica para um número gratuito ou videoconferência ao vivo; fornecimento de identidade emitida pelo governo para verificação em um banco de dados; processamento de um cartão de crédito ou débito para avisar o usuário adulto; ou o fornecimento de um conjunto de perguntas baseadas em conhecimentos específicos.

À medida que a tecnologia continua a avançar, o mesmo acontece com os métodos escolhidos por uma empresa. Este padrão flexível fornece às empresas orientação suficiente para continuarem a desenvolver e melhorar os seus serviços.

No entanto, ainda existem desafios de implementação. Por exemplo, muitos pais e responsáveis legais não compartilham o mesmo sobrenome de seus filhos devido a um novo matrimônio, adoção ou outras decisões culturais ou familiares – inclusive no Brasil, onde é comum ter vários sobrenomes. Além disso, alguns familiares podem não ser proficientes em outras línguas além do português, não têm conhecimentos tecnológicos ou têm vários empregos. Isto levanta sérias preocupações sobre equidade, especialmente tendo em conta os familiares que não possuem a identificação governamental necessária ou outros mecanismos para acessar um serviço ou plataforma online – impedindo os adolescentes de ter acesso a serviços úteis e informações adequadas à sua idade.

3. **In the case of adolescents, must obtaining consent, especially in the digital environment, comply with the provisions of civil law regarding civil capacities, following the general rule of representation and assistance from parents or guardians? Or is it possible to consider, in line with the principle of best interests, the progressive autonomy of these holders to, in certain contexts and situations, provide consent to the processing of their personal data without the need for representation or assistance from parents and legal guardians?**

Due to the nuanced ways in which children and adolescents use the internet, it is imperative to appropriately tailor such treatments to respective age groups. Thus, determining what constitutes a reasonable effort to obtain consent is even more challenging for non-child

content. For example, if a 16-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

Ultimately, the 16-year-old who is researching rainforest preservation efforts will also access and use the same online encyclopedia, blog, or video channel as adults with similar research interests. Any parental consent requirement that conditions access to such online materials must account for their specific needs and interests, including the ability for teens to provide their own consent, in using these important and beneficial digital tools and services.

3. *No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?*

Devido às diferentes formas como as crianças e os adolescentes utilizam a Internet, é imperativo adaptar adequadamente esses tratamentos às respectivas faixas etárias. Assim, determinar o que constitui um esforço razoável para obter consentimento é ainda mais desafiador para conteúdos não infantis. Por exemplo, se um jovem de 16 anos estiver realizando uma pesquisa para um projeto escolar, espera-se que ele encontre, aprenda e consiga discernir uma variedade maior de materiais do que uma criança de 7 anos na Internet jogando videogames. Isto também permitiria que aqueles com mais de 13 anos, que utilizam a Internet de forma muito diferente dos seus pares mais jovens, continuassem a se beneficiar dos seus recursos.

Em última análise, o jovem de 16 anos que está pesquisando, por exemplo, esforços de preservação da floresta tropical também acessa e usa a mesma enciclopédia, blog ou canal de vídeo on-line que adultos com interesses de pesquisa semelhantes. Qualquer requisito de consentimento dos pais que condicione o acesso a tais materiais online deve ter em conta as suas necessidades e interesses específicos, incluindo a capacidade dos adolescentes fornecerem o seu próprio consentimento na utilização destas ferramentas e serviços digitais importantes e benéficos.

III. Internet games and applications

1. **What principles, parameters and safeguards, including design measures, must be observed when processing personal data of children and adolescents by digital platforms, in order to ensure respect for their best interests, promote and ensure high levels of privacy and protection of personal data and mitigate the risks arising from the use of these platforms?**

Any approach to youth online safety and privacy must recognize and account for the inherent differences among online platforms and services. While policymakers hope an overarching solution will emerge to address all the risks associated with online services and platforms, there is no panacea for keeping young users safe across the diverse internet ecosystem. Rather than a best interest standard, any potential framework for youth online safety needs to have a risk-based approach that enables organizations to take the necessary actions in light of the evolving risks and dangers most relevant to their specific environment and users.

Otherwise, a best-interest approach would provide little compliance guidance and clarity to organizations by inviting subjective, vague considerations. Humans in general, especially children, have very nuanced opinions surrounding what may be harmful to them. The diverse lived experiences of children, teens, and adults vary significantly, leaving businesses without a comprehensive roadmap to navigate each user's unique perspective. Determining the optimal solutions for the well-being of each and every young individual engaging with an online platform poses a serious feasibility challenge.

III. Jogos e aplicações de internet

1. *Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?*

Qualquer abordagem à segurança e privacidade online dos jovens deve reconhecer e ter em conta as diferenças inerentes entre as plataformas e os serviços online. Embora os líderes políticos esperem que surja uma solução abrangente para resolver todos os riscos associados aos serviços e plataformas online, não existe uma solução universal para manter os jovens usuários seguros em todo o diversificado ecossistema da Internet. Ao invés de um padrão de "melhor interesse", qualquer potencial diretiva para a segurança online dos jovens precisa de ter uma abordagem baseada no risco que permita às organizações tomar as medidas necessárias à luz dos progressivos riscos e perigos mais relevantes específicos ao seu ambiente e usuários.

Caso contrário, uma abordagem de melhor interesse forneceria pouca orientação e clareza de conformidade às organizações, dando azo a considerações subjetivas e vagas. Pessoas em geral, especialmente as crianças, têm opiniões muito diferenciadas sobre o que pode ser prejudicial para elas. As diversas experiências vividas por crianças, adolescentes e adultos variam significativamente, deixando as empresas sem um roteiro abrangente para navegar pela perspectiva única de cada usuário. Determinar as soluções ideais para o bem-estar de cada jovem envolvido numa plataforma online representa um sério desafio de viabilidade.

2. **Considering that the processing of personal data must be limited to that**

strictly necessary for the purpose for which it is intended, what are the good practices and techniques available and appropriate for verifying the age of users of digital platforms?

While various age assurance methods, such as age verification and parental consent, are available, each approach comes with its own set of challenges and trade-offs.

Though the intention to keep kids safe online is commendable, some mandates can be counterproductive to that initiative by requiring more data collection about young people. Specifically, age verification technology still faces serious technical challenges that likely undermines the safety and privacy of its users. 404 Media recently reported on the breach of an age verification provider, exposing sensitive information: https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/

More accurate methods often require the collection of additional personal data, potentially conflicting with a service's privacy commitments to users and legal obligations. Mandates to collect and retain additional sensitive information about users creates serious and unnecessary cybersecurity risks for organizations and users. If businesses were forced to collect age verification data, that would paradoxically force companies to collect a higher volume of data on children. Businesses may be forced to collect personal information they don't want to collect and consumers don't want to give, and that data collection creates extra privacy and security risks for everyone.

Age verification requirements raise serious questions regarding conflicts with data minimization principles and other consumer data privacy protection measures. To effectively conduct age verification, businesses would be required to collect additional data — including collecting and storing their geolocation data to ensure they do not reside outside of the state when confirming that they are of age to be using these services, which would result in additional volumes of data specifically about children. The need to collect additional volumes of data would effectively apply to all users by nature of needing to discern between adult and children or adolescent users. Further, parents or guardians of younger users would likely be required to provide sensitive financial information and personal identifiable information when consenting to and providing age-verification on behalf of younger users.

France's data protection agency recently analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security. That report is available in English at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

2. *Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?*

Embora estejam disponíveis vários métodos para se garantir a idade de alguém, como a verificação da idade e a obtenção do consentimento dos pais, cada abordagem apresenta o seu próprio conjunto de desafios e pontos positivos e negativos.

Embora a ideia de manter as crianças seguras online seja louvável, algumas medidas podem ser contraproducentes para essa iniciativa, exigindo um recolhimento maior de dados sobre os jovens. Especificamente, a tecnologia de verificação de idade ainda enfrenta sérios desafios técnicos que provavelmente prejudicam a segurança e a privacidade dos seus utilizadores. 404 Media relataram recentemente a violação de um provedor de verificação de idade, expondo informações confidenciais (link em inglês): https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/

Métodos mais precisos muitas vezes exigem a coleta de dados pessoais adicionais, potencialmente em conflito com os compromissos de privacidade de um serviço para com seus usuários e com suas obrigações legais. A obrigatoriedade de coletar e reter informações confidenciais adicionais sobre os usuários cria sérios e desnecessários riscos de cibersegurança para organizações e usuários. Se as empresas fossem forçadas a recolher dados de verificação da idade isso, paradoxalmente, forçaria as empresas a recolherem um volume maior de dados sobre crianças. As empresas podem ser forçadas a recolher informações pessoais que não querem recolher e os consumidores não querem dar, e esse recolhimento de dados cria riscos adicionais de privacidade e segurança para todos.

Requisitos de verificação da idade levantam sérias questões relativas aos conflitos com os princípios de minimização de coleta de dados e outras medidas de proteção à privacidade dos dados dos consumidores. Para realizar de maneira eficaz medidas de verificação da idade, as empresas seriam obrigadas a recolher dados adicionais – incluindo o recolhimento e o armazenamento dos seus dados de geolocalização para garantir que não residam fora do estado ao confirmar que têm idade para utilizar estes serviços, o que resultaria em um volume maior de dados especificamente sobre crianças. A necessidade de recolher volumes adicionais de dados seria efetivamente aplicada a todos os usuários, pela natureza da necessidade de discernir entre utilizadores adultos e crianças e adolescentes. Além disso, os pais ou responsáveis de usuários mais jovens provavelmente seriam obrigados a fornecer informações financeiras confidenciais e informações de identificação pessoal ao consentirem e fornecerem verificação de idade em nome de usuários mais jovens.

A agência francesa de proteção de dados analisou recentemente várias soluções existentes de verificação de idade online, mas descobriu que nenhuma das opções poderia satisfazer três padrões principais: 1) fornecer uma verificação suficientemente confiável; 2) permitir a cobertura completa da população; e 3) respeitar a proteção dos dados, privacidade e segurança dos indivíduos. Esse relatório está disponível em inglês em: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

3. **What specific limitations must be observed when collecting personal data from children and adolescents via digital platforms, considering the provisions of art. 14, § 4, of the LGPD and, among other aspects, the nature of the data collected and the purpose of the processing, such as the formation**

of behavioral profiles?

These methods can also lead to disparities among users, particularly for those lacking eligible government-issued IDs or access to financial institutions necessary for verification, potentially discriminating against specific demographic groups. Further, smaller companies may lack the financial resources to implement such verification frameworks. Enhancing confidence in the knowledge of a specific user's age causes implications for safeguarding their privacy rights, ensuring their access to information, and preserving their freedom to engage in digital experiences without constraints.

3. *Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?*

Esses métodos também podem levar a diferenciação entre os usuários, especialmente aqueles que não possuem documentos de identificação emitidos pelo governo ou acesso às instituições financeiras necessárias para verificação, potencialmente discriminando grupos demográficos específicos. Além disso, as pequenas empresas podem não ter recursos financeiros para implementar tais dispositivos de verificação. Aumentar a confiança em se saber a idade de um usuário específico tem implicações na salvaguarda dos seus direitos de privacidade, garantindo o seu acesso à informação e preservando a sua liberdade de participar em experiências digitais sem restrições.

4. **What mechanisms and good practices can be adopted to increase the control of parents and guardians over the processing of personal data of children and adolescents in the digital environment?**

As discussions of child safety and privacy online continue, leading technology companies are working jointly and independently to advance online safety. These critical undertakings include joint work in organizations like the Digital Trust & Safety Partnership, the Technology Coalition, and the Family Online Safety Institute, among others, whose collective efforts promote child safety online and provide resources for parents to foster safer digital experiences for young persons. In addition, many companies have developed their own products and tools to advance this goal, providing resources to parents with additional clarity and information but avoiding the confusion and costs associated with an overly prescriptive parental consent requirement.

4. *Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?*

À medida que continuam as discussões sobre segurança e privacidade infantil online, as

principais empresas de tecnologia estão trabalhando tanto em conjunto quanto de forma independente para promover a segurança online. Estes empreendimentos críticos incluem o trabalho conjunto em organizações como a Digital Trust & Safety Partnership, a Technology Coalition e o Family Online Safety Institute, entre outras, cujos esforços coletivos promovem a segurança infantil online e fornecem recursos para que os pais possam fornecer experiências digitais mais seguras para os jovens. Além disso, muitas empresas desenvolveram os seus próprios produtos e ferramentas para alcançar este objetivo, fornecendo recursos com maior clareza e informações aos pais, mas evitando a confusão e os custos associados a um requisito de consentimento parental excessivamente prescritivo.

5. **What good practices related to transparency and providing information in a simple, clear and accessible way can be observed by digital platforms regarding the processing of personal data of children and adolescents?**

Businesses should be able to provide this information in a simple, clear, and accessible way. Imposing redundant, separate requirements that would create unnecessary confusion for parents and businesses. Parents would encounter longer and repetitive consent requests that may introduce consent fatigue and importantly, reduce their understanding of the data practices presented. Businesses would face mounting compliance costs for each additional disclosure, which again would provide no substantial benefits to parents.

By allowing businesses to provide such information in a single page or location, businesses can also inform families of the countless tools and options available to them for their safety. These include comprehensive guides for families that provide details and guidance on how to create a supervised account for kids, setting the right parental controls for one's family, and finding balance with technology online.

5. *Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?*

As empresas devem ser capazes de fornecer essas informações de forma simples, clara e acessível, sem a imposição de requisitos redundantes e separados que criariam uma confusão desnecessária para pais e empresas. Os pais encontrariam solicitações de consentimento mais longas e repetitivas que podem causar fadiga de consentimento e, principalmente, reduzir a sua compreensão das práticas de coleta de dados apresentadas. As empresas enfrentariam custos crescentes de conformidade para cada divulgação ou formulário adicional, o que, mais uma vez, não traria benefícios substanciais aos pais.

Ao permitir que as empresas forneçam essas informações numa única página ou local, as empresas também podem informar as famílias sobre as inúmeras ferramentas e opções disponíveis para a sua segurança. Isso inclui guias completos para famílias, os quais fornecem detalhes e orientações sobre como criar uma conta supervisionada para crianças,

definir os controles parentais corretos para a família e encontrar equilíbrio com a tecnologia online.

6. Are there other issues related to the processing of personal data of children and adolescents that deserve clarification or additional regulation?

The widespread benefits and more importantly, opportunities provided and created by such technologies need to be considered. A unique strength of the internet is that it opens so many doors for countless people with different socio-economic backgrounds. Future innovation and social progress rest on these generations, and while all the benefits may not be immediately known, the return in the long run for allowing the younger generation to learn about new topics or get involved in local social causes is immeasurable.

Social media has also been found to encourage collaborative learning that teaches children and teens about the importance of appreciating different perspectives and views to better understand the world. This in turn helps spark their curiosity and discover areas of interest to them. Social media has also played an important role in digital media literacy. Importantly, research demonstrates that it is critical to help kids learn to navigate digital spaces on their own. Social-emotional skills like empathy, kindness, and personal responsibility, which are crucial for offline interactions, can also be taught to enhance online interactions. Even for younger children, character education through digital citizenship is gaining traction in practice. According to a study on school children in the United States, 62% of K-2 teachers and 69% of grade 3-5 teachers report using some digital citizenship curriculum, with competencies related to developing positive character features being most common, such as understanding cyberbullying and hate speech.

Restrictions on access to information online could undermine and impede this progress and future advancements, especially to users seeking communities of support and raise concerns about vulnerable users (i.e., children in abusive households or those without access to supportive communities in their physical location). Relatedly, such provisions raise free expression concerns by limiting access to lawful speech.

The Computer & Communications Industry Association ("CCIA") is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks.

We appreciate the opportunity to provide input and are always happy to be a resource.

Materials in English that may be of use to ANPD can be found at the following links:

https://project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification/

https://project-disco.org/privacy/a-guide-for-how-not-to-pursue-child-protection-online/

https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/

https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf

6. *Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?*

Os benefícios generalizados e, mais importante ainda, as oportunidades proporcionadas e criadas pelas tecnologias de informação e comunicação devem ser consideradas. Um ponto forte único da Internet é que ela abre muitas portas para inúmeras pessoas com diferentes origens socioeconômicas. A inovação futura e o progresso social dependem desta integração e, embora todos os benefícios possam não ser imediatamente conhecidos, o retorno a longo prazo de permitir que a geração mais jovem aprenda sobre novos temas ou se envolve em causas sociais locais é imensurável.

Descobriu-se também que as redes sociais incentivam a aprendizagem colaborativa que ensina crianças e adolescentes sobre a importância de se valorizar diferentes perspectivas e pontos de vista para compreender melhor o mundo. Isso, por sua vez, ajuda a despertar sua curiosidade e o descobrimento de áreas de interesse para eles. As redes sociais também desempenharam um papel importante na alfabetização digital. É importante ressaltar que pesquisas mostram ser fundamental ajudar as crianças a aprenderem a navegar nos espaços digitais por conta própria. Habilidades socioemocionais como empatia, gentileza e responsabilidade pessoal, que são cruciais para interações offline, também podem ser ensinadas para melhorar as interações online. Mesmo para as crianças mais novas, o ensino de valores através da cidadania digital está ganhando força na prática. De acordo com um estudo sobre crianças em idade escolar nos Estados Unidos, 62% dos professores do ensino fundamental e médio e 69% dos professores do 3º ao 5º ano relataram usar algum currículo de cidadania digital, sendo as competências relacionadas ao desenvolvimento de características positivas de caráter as mais comuns, como a compreensão do cyberbullying e do discurso de ódio.

As restrições ao acesso à informação online podem minar e impedir este progresso e avanços futuros, especialmente para os usuários que procuram comunidades de apoio, e levantam preocupações sobre os utilizadores mais vulneráveis (ou seja, crianças em lares abusivos ou aqueles sem acesso a comunidades de apoio na sua localização física). Da mesma forma, tais disposições levantam preocupações sobre a liberdade de expressão, limitando o acesso ao discurso legal.

A CCIA é uma associação comercial internacional sem fins lucrativos, que representa uma ampla variedade de empresas de comunicação e tecnologia. Há mais de 50 anos, a CCIA promove mercados abertos, sistemas abertos e redes abertas.

Agradecemos a oportunidade de participar dessa tomada de subsídios e estamos sempre dispostos a fornecer maiores informações.

Materiais em inglês que podem ser úteis à ANPD podem ser encontrados nos seguintes links:

https://project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification/

https://project-disco.org/privacy/a-guide-for-how-not-to-pursue-child-protection-online/

https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/

https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf