Notas Explicativas

Comentário Geral n.º 25 (2021) sobre os direitos das crianças em relação ao ambiente digital (*)

(*) A presente tradução para língua portuguesa deste documento foi elaborada pelo **Departamento de Cooperação Judiciária e Relações Internacionais** (DCJRI) da Procuradoria-Geral da República de Portugal, com base na versão em língua inglesa disponível na página da ONG 5Rights Foundation. **Este trabalho constitui uma tradução não oficial pela qual o DCJRI assume plena responsabilidade. Esta tradução não implica, contudo, a manifestação de qualquer posição, da parte da PGR ou de qualquer um dos seus elementos, relativamente a questões, alegações, factos ou indivíduos referidos nas presentes Notas Explicativas.**

Estas notas explicativas têm como objetivo aprofundar o conhecimento e apresentar exemplos tangíveis, da vida real, para ilustrar as disposições do Comentário Geral n.º 25, elaborado pelo Comité dos Direitos da Criança das Nações Unidas.

O ambiente digital abrange uma ampla variedade de circunstâncias e contextos interligados e não é possível captá-los a todos. Estas notas pretendem antecipar questões e assinalar abordagens que foram trazidas ao nosso conhecimento e refletem as preocupações concretas suscitadas no decorrer dos processos de estudo e redação.

O texto baseia-se nas contribuições apresentadas ao Comité dos Direitos da Criança das Nações Unidas por grupos de peritos, crianças e membros do grupo diretor da ONG 5Rights, bem como nas 142 contribuições para a consulta e os *workshops* envolvendo 709 crianças em 28 países. Embora as presentes Notas Explicativas e as contribuições que lhes serviram de base não tenham a autoridade do próprio comentário geral, contextualizam-no melhor e agradecemos a todos os participantes pelas suas valiosas contribuições.

Muitas contribuições referem o significado da Covid-19. Embora a pandemia tenha acelerado a adoção e utilização das tecnologias digitais por algumas crianças e alargado as suas interações e o tempo passado em linha, a dependência das crianças do mundo digital é anterior e perdurará muito para além dos efeitos da pandemia. A Covid-19 aumentou a dependência das crianças de múltiplas tecnologias digitais para o exercício dos seus direitos básicos à educação, informação e participação. Contudo, a pandemia tornou também evidente o fosso digital existente entre os que têm e os que não têm acesso a meios digitais, em cada país e a nível internacional. A pandemia exacerbou também e assim ampliou desigualdades pré-existentes ao nível da educação, as quais constituem uma preocupação a curto e longo prazo. Uma questão reiteradamente colocada é a de saber quanto tempo levará até que o acesso às tecnologias digitais seja considerado um direito fundamental de todas as crianças.

Como as tecnologias digitais influenciam de várias formas e cada vez mais as vidas das crianças, é fundamental considerar todo o espetro dos direitos da criança e todos os tipos de impactos da tecnologia digital, tanto agora como no futuro. O Comentário Geral n.º 25 faz precisamente isto.

A numeração das Notas Explicativas acompanha a numeração dos parágrafos do Comentário Geral n.º 25. As Notas não substituem o Comentário Geral e limitam-se a dar explicações e exemplos relacionados com o texto do Comentário Geral. Esperamos que, nos próximos meses, outros ajudem a acrescentar exemplos de boas práticas e pedimos aos leitores, particularmente colegas do Sul Global, para que nos apoiem no esforço de tornar este documento mais rico e mais representativo.

5Rights, Grupo Diretor

Março de 2021

Notas Explicativas

I. Introdução

1. Mais de 1000 crianças foram consultadas durante a elaboração deste comentário geral. Contribuíram para o documento In our Own Words, versão para crianças do comentário, podendo um resumo das respetivas opiniões ser encontrado na obra Our Rights in a Digital World. As suas opiniões foram levadas em conta pelo Comité dos Direitos da Criança das Nações Unidas e encontram-se refletidas no Comentário Geral n.º 25.

2. As definições das tecnologias referidas podem ser encontradas no glossário (Anexo 1). Muitas pessoas consideram que o ambiente digital é o que sucede num computador ou smartphone e, obviamente, é. Mas o ambiente digital é um ambiente complexo e em contínua e rápida evolução que envolve muitas tecnologias interligadas, algumas das quais podem estar nas mãos das crianças enquanto que outras não são diretamente possuídas por elas mas, ainda assim, influenciam as suas vidas. Os direitos da criança serão no futuro influenciados por tecnologias que ainda não existem.

Além disso, mesmo que determinada criança não seja utilizadora de certa tecnologia digital, os seus direitos podem ser influenciados devido à sua utilização por terceiros. A lista constante do Anexo 1 ilustra a variedade de tecnologias digitais que compõem o ambiente digital, mas não é exaustiva. Os direitos da criança são pertinentes relativamente a todas as ações e impactos do ambiente digital, constantes ou não da lista, e para todas as atuais ou futuras tecnologias[1]. Dada a rapidez da mudança e evolução tecnológica, e os desafios que acompanham tais mudanças, é altamente provável que "novas" tecnologias futuras continuem a ter impacto nos direitos da criança de múltiplas formas. Nesse sentido, este Comentário Geral deve ser visto como um guia para a interpretação da Convenção sobre os Direitos da Criança, a utilizar numa viagem contínua e não um itinerário para aqui e agora.

3. As crianças que vivem em sociedades interligadas estão a descobrir que a tecnologia medeia e influencia a maior parte das áreas das suas vidas. Cada vez mais, os governos podem usar AI para afetar recursos ou serviços, distribuí-los ou proporcionar acesso aos mesmos. Por exemplo, na África do Sul, os requerimentos de subsídios para famílias afetadas pela Covid-19 só podem ser apresentados por via eletrónica[2]. Plataformas de ensino à distância podem ser usadas no ensino ou talvez um cartão de identificação "inteligente" ou sistema biométrico possa ser utilizado para identificar uma criança num transporte público

[1] Para recursos sobre a natureza evolutiva do ambiente digital ver, por exemplo, https://www.cigionline.org/.

[2] https://www.gov.za/covid-19/individuals-and-households/social-grants-coronavirus-covid-19.

ou permitir-lhe o acesso a um edifício. As crianças estão também a utilizar muitos produtos e serviços que as ligam à família, amigos e outros. Estes produtos são frequentemente desenhados para adultos e têm fins comerciais, incluindo processamento de dados, bem como características suscetíveis de afetar negativamente a experiência da criança ou violar os seus direitos.

Da mesma forma, os sistemas tecnológicos podem ser utilizados para difundir conhecimentos ou distribuir serviços às crianças de formas que as beneficiem e favoreçam ou reforcem os seus direitos. Serviços mediados pela tecnologia podem proporcionar oportunidades genuínas para melhorar a inclusão ou ultrapassar a desigualdade ou desvantagem. Mas, mesmo aqui, os utilizadores só parcialmente compreendem os sistemas, pelo que estes apresentam riscos conhecidos e desconhecidos. Por exemplo, na Austrália a utilização de AI para detetar fraudes na área da segurança social demonstrou ser pouco fiável e levou ao cancelamento dos pagamentos a muitas famílias[3]. As formas através das quais sistemas de AI semelhantes processam informação e tomam decisões são muitas vezes opacas para as pessoas que sofrem o impacto de tais tecnologias. A AI é frequentemente utilizada no recrutamento[4]: fazendo juízos automatizados acerca da adequação de um candidato a determinado trabalho ou oportunidade educativa ou decisões que alteram o percurso de vida no âmbito do sistema de justiça. As crianças, ou seus pais, nem sempre têm consciência do impacto das tecnologias automatizadas. Consequentemente, muitas crianças sentem-se ansiosas para saber se podem ou não confiar no mundo digital.

4. Um acesso significativo e seguro às tecnologias digitais pode ajudar a criança a florescer[5]. As tecnologias digitais permitem que as crianças contactem entre si na prossecução dos seus interesses, podem ajudá-las a aceder a serviços e ambientes que contribuem para o respetivo desenvolvimento e constituem um ambiente que permite a sua participação na vida cívica e cultural. Por exemplo, tal como acima referido, no primeiro pico da pandemia em 2020, 1,6 mil milhões de crianças em idade escolar de todo o mundo não podiam ir à escola[6]. Enquanto as crianças com acesso ao mundo digital conseguiram participar no ensino à distância, para muitas crianças sem acesso ou com acesso comprometido (dispositivos partilhados, limites ao tráfego de dados) as oportunidades de aprendizagem foram reduzidas. As desigualdades no acesso (ou a falta de inclusão digital equitativa) contribuem para as desigualdades educativas já existentes[7].

---

[3] https://www.theguardian.com/technology/2019/oct/16/automated-messages-welfare-australia-system.
[4] https://www.bbc.co.uk/news/business-55932977.
[5] https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_ACCESS.pdf.
[6] https://www.weforum.org/agenda/2020/12/covid19-education-innovation-outcomes.
[7] https://unctad.org/system/files/official-document/dtlinf2020d1_en.pdf.

O acesso só por si não é suficiente. É preciso que as crianças disponham de meios seguros e fiáveis para utilizar as tecnologias de formas que lhes permitam realizar os seus direitos, mitigando os riscos que acompanham tal acesso.

> "Atualmente não estamos a usar qualquer tecnologia digital para nos expressarmos, mas gostaríamos de o fazer se tivermos os conhecimentos ou acesso aos mesmos no futuro"
>
> *Etiópia, idade e género desconhecidos*[8]

5. O Comentário Geral n.º 25 não surge no vazio. Já tem havido contribuições importantes para a análise da interseção entre a tecnologia e os direitos humanos. Este Comentário Geral parte de tais conhecimentos e experiências incluindo documentos fundamentais das Nações Unidas como os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos[9], e reforça-os através de consultas abrangentes para examinar as implicações concretas para os direitos humanos das crianças relativamente às empresas[10], e tendo em conta outros documentos das Nações Unidas[11]. Deve ser feita uma referência especial às consultas com crianças[12].

6. O Comentário Geral n.º 25 refere outros Comentários Gerais e Protocolos Facultativos à Convenção sobre os Direitos da Criança que fornecem detalhes adicionais sobre questões concretas, nomeadamente:

- Comentário Geral n.º 2: Papel das Instituições Nacionais Independentes de Direitos Humanos na Proteção e Promoção dos Direitos da Criança
- Comentário Geral n.º 5 (2003): Medidas Gerais de Aplicação da Convenção sobre os Direitos da Criança
- Comentário Geral n.º 7 (2005): Implementação dos direitos da criança na primeira infância
- Comentário Geral n.º 9 (2006): Direitos das crianças com deficiência
- Comentário Geral n.º 14 (2013) sobre o direito da criança a que o seu interesse superior seja primacialmente tido em conta (artigo 3.º, n.º 1)
- Comentário Geral n.º 16 (2013), sobre as obrigações do Estado relativamente ao impacto do setor empresarial nos direitos da criança
- Comentário Geral n.º 17 (2013) sobre o direito da criança ao repouso, tempos livres, brincar, atividades recreativas, vida cultural e artística (art.º 31.º)

---

[8] *Our Rights in a Digital World*, p. 10.
[9] HR/PUB/11/04 https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[10] http://childrenandbusiness.org/
[11]. *Children's Consultation report*.
[12] Disponíveis aqui: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=5&DocTypeID=11.

- Comentário Geral n.º 19 (2016) sobre orçamentos públicos para a realização dos direitos da criança (art.º 4.º)
- Comentário Geral n.º 20 (2016) sobre a realização dos direitos da criança durante a adolescência
- Comentário Geral n.º 21 (2017) sobre crianças em situações de rua
- Comentário Geral n.º 24 (2019) sobre os direitos da criança no sistema de justiça para crianças
- Diretrizes sobre a implementação do Protocolo Facultativo relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil (2019)[13]

II. Objetivo

7. O Comentário Geral n.º 25 enuncia de que forma os direitos da criança se aplicam no ambiente digital. Ajudará os Estados a compreender que passos são necessários para respeitar, proteger e garantir os direitos da criança em todos os ambientes, incluindo o ambiente digital.

III. Princípios gerais

8. A Convenção sobre os Direitos da Criança identifica os seguintes quatro direitos como princípios gerais que deverão ser tidos em conta na implementação de todos os outros direitos e relativamente a todos os aspetos da interação das crianças com serviços e produtos digitais.

A. Não discriminação

9. Cada vez mais, as crianças necessitam de ter acesso a tecnologia digital para se desenvolverem e florescerem. É necessário que os Estados levem a cabo pogramas específicos para assegurar um acesso equitativo, nomeadamente às crianças que possam não ter banda larga ou equipamento em casa. Por exemplo, o Projeto Isizwe proporciona hotspots de WiFi dedicados nas escolas de Curro, na África do Sul[14]. É também necessário que as crianças disponham das competências necessárias para utilizar a tecnologia disponível.

Os Estados deverão incluir, nos Planos Nacionais de Ação ou Desenvolvimento, um guia para abordar e colmatar quaisquer desigualdades digitais, especialmente para raparigas, crianças das comunidades mais pobres, crianças das áreas rurais e/ou remotas e crianças carecidas de conteúdos relevantes nas redes, particularmente falantes de outras línguas que não o inglês. Sempre que possível,

---

[13] https://www.ohchr.org/Documents/HRBodies/CRC/CRC.C.156_OPSC%20Guidelines.pdf.
[14] https://www.commscope.com/globalassets/digizuite/470-300-cs-project-isizwe.pdf.

os Estados devem impor obrigações de acesso universal e garantir que as crianças têm acesso a planos de dados económicos ou gratuitos para poderem efetuar trabalhos escolares e participar. Caso seja improvável que as crianças tenham acesso privado e pessoal a dispositivos digitais e ao ambiente digital, os governos devem garantir acesso público. Contudo, o acesso público ou partilhado a dispositivos digitais e ao ambiente digital raramente constituirá, a longo prazo, uma alternativa adequada ao acesso privado e individual. Embora os Estados variem na sua capacidade de proporcionar acesso digital ao grande público, a questão é que as crianças, e especialmente determinados subgrupos de crianças, não devem ser discriminadas no planeamento e fornecimento de tais serviços.

10. A discriminação pode assumir muitas formas. Algumas crianças são completamente excluídas da participação em ambientes digitais; por exemplo, as raparigas que enfrentam restrições nas suas sociedades podem também sofrer restrições no acesso ao ambiente digital.[15]

> "As raparigas parecem ter menos acesso à Internet do que os rapazes...Há uma discriminação no acesso com base no género...As raparigas não possuem de facto o seu próprio telefone e têm acesso limitado à Internet comparando com os rapazes, que podem aceder em cafés com Internet, os quais são em geral unicamente para rapazes."
>
> Jordânia, notas de moderador de workshop[16]

Em alguns contextos, as crianças têm sido forçadas a sair de ambientes digitais devidos a abusos cometidos nas redes[17], ou podem ser objeto de discriminação devido a suposições e decisões de sistemas digitais mais alargados suscetíveis de conduzir a discriminação estrutural ou indireta (por exemplo, a utilização de um algoritmo na correção de exames no Reino Unido em 2020, que baixou desproporcionalmente as notas dos alunos de zonas de baixos rendimentos contra as previsões dos professores).[18]

11. A discriminação deve ser combatida sob todas as suas formas, quer seja cometida por sujeitos individuais quer por uma instituição ou em resultado do próprio ecossistema digital. O Comité apela aos Estados para que tomem medidas políticas e legislativas proactivas para promover a igualdade de acesso de todas as crianças à Internet e às tecnologias digitais.

B. Interesse superior da criança

---

[15] https://plan-international.org/education/bridging-the-digital-divide.
[16] *Our Rights in a Digital World*, p. 13.
[17] *Our Rights in a Digital World*, p. 17.
[18] https://www.technologyreview.com/2020/08/20/1007502/uk-exam-algorithm-cant-fix-broken-system/.

12. O “interesse superior da criança” é um princípio que deverá ser aplicado às decisões que afetem crianças em ambiente digital. Quando existem interesses conflituantes entre, por exemplo, o direito dos adultos à liberdade de expressão nas redes e o direito à privacidade das crianças, os Estados deverão garantir que o interesse superior da criança ou crianças será tido “primacialmente em conta”. Por exemplo, o Comissário para a Informação do Reino Unido afirma, em relação à proteção dos dados de crianças, que “é contudo improvável que os interesses comerciais de uma organização se sobreponham ao direito da criança à privacidade”[19]. O princípio pode também ser aplicado para ajudar a encontrar respostas para situações em que existam tensões entre os diferentes direitos das crianças, por exemplo entre a liberdade de associação através de fóruns nas redes e o direito da criança à proteção contra o ciberbullying ou a exploração. Sempre que possível, a determinação do que constitui o interesse superior da criança deve também ter plenamente em conta as opiniões da própria criança.[20]

13. Deve ser dada voz às crianças na determinação do interesse superior da criança. Com frequência, o foco dos decisores políticos e da sociedade civil está exclusivamente na proteção das crianças em ambiente digital, mas as crianças têm uma ampla variedade de direitos e todos eles, incluindo o direito à participação, a liberdade de informação e a liberdade de pensamento, deverão ser igualmente tidos em conta. As crianças deverão também ser consultadas e são frequentemente muito claras quanto à forma como gostariam que o mundo digital incorporasse os seus direitos.

> “A tecnologia é muito importante e continuará a sê-lo no futuro...O mundo está a avançar, por isso devemos fazer o mesmo.”
>
> Croácia, rapariga, 12[21]

C. Direito à vida, sobrevivência e desenvolvimento

14. Existe um número significativo de riscos conhecidos e emergentes para as crianças mediados ou reforçados pelas tecnologias digitais. Os Estados deverão tomar todas as medidas para prevenir os riscos e proteger as crianças dos males suscetíveis de influenciar o seu desenvolvimento emocional ou a sua sobrevivência física. Os Estados devem impor aos fornecedores de serviços a obrigação de efetuar rotineiramente avaliações de risco para identificar os riscos subsumidos

---

[19] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/.

[20] https://digitalfuturescommission.org.uk/blog/the-best-interests-of-children-in-the-digital-world/.

[21] *Our Rights in a Digital World*, p. 4.

aos quatro C (Conteúdos, Contactos, Condutas e Contratos[22]) e adotar todas as medidas necessárias para mitigar os mesmos. Muitos Estados introduziram quadros legislativos e regulamentares para lidar com determinados riscos ou conjuntos de riscos. Por exemplo, 150 países aperfeiçoaram ou implementaram, nos últimos 15 anos, nova legislação de combate aos materiais que configuram abuso sexual de crianças[23], e a Comissão Europeia produziu um Código de Conduta sobre o discurso ilegal de ódio nas redes[24].

15. As crianças necessitam de interações diretas e contínuas com os seus pais ou cuidadores e outros familiares, especialmente numa idade precoce. O contacto cara a cara e físico é fundamental para todos os aspetos do respetivo desenvolvimento. A utilização de dispositivos digitais e as atividades baseadas em ecrãs não devem substituir tal contacto. Deve ser proporcionada formação aos pais e cuidadores para que compreendam o desenvolvimento da criança e o impacto das tecnologias digitais nesse desenvolvimento, com base em estudos reputados e avaliados, para todos os grupos etários como o Relatório sobre Infância Digital[25], que considera as necessidades e a autonomia dos vários grupos etários na sua interação com o ambiente digital.

D. Respeito pelas opiniões da criança

16. As crianças adotam desde cedo e com entusiasmo as tecnologias digitais. Os Estados devem indagar e ter em conta as opiniões das crianças sobre as questões que as afetam, incluindo a forma de potenciar as oportunidades que o ambiente digital oferece e de as ajudar a desenvolver as aptidões e oportunidades de participação na vida cultural e cívica.[26]

> "A tecnologia digital desempenha um papel porque, com [a sua] ajuda...podemos ligar-nos ao mundo e podemos formar uma identidade no mundo."
>
> Paquistão, rapaz, 13[27]

17. Os legisladores, empresas e organizações que criam, fornecem e governam o mundo digital devem consultar as crianças. As crianças têm muitas vezes opiniões

---

[22] https://www.riskyby.design/the-risks.
[23] https://www.icmec.org/csam-model-legislation/.
[24] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.
[25] https://5rightsfoundation.com/uploads/digital-childhood---final-report.pdf.
[26] https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/10_cases_of_child_participation_report.pdf.
[27] *Our Rights in a Digital World*, p. 7.

fortes e ideias criativas sobre a forma de maximizar benefícios e minimizar os aspetos negativos do mundo digital, podendo contribuir positivamente para a criação de um ambiente digital respeitador dos direitos.

> "Todos os websites devem obrigar a que inicies a tua conta em modo privado e podes decidir torná-la pública quando quiseres."
>
> Jovem, Reino Unido

18. A própria tecnologia digital pode ser usada para consultar as crianças. Por exemplo, a versão para crianças[28] deste Comentário Geral foi desenvolvida através de workshops virtuais e de um inquérito na Internet com questões abertas. Isto permitiu-nos consultar e chegar a 215 crianças de 28 países de forma rápida e fácil.

A consulta às crianças por meios digitais não pode resultar em violações da sua privacidade. Nem devem as crianças ser punidas devido às suas opiniões ou obrigadas a revelar os seus pensamentos. As crianças sem acesso a tecnologias digitais não devem ser excluídas da participação em consultas semelhantes: elas também têm opiniões sobre a forma como o mundo digital as pode ajudar a realizar os seus direitos.[29]

Como condição prévia a uma interação significativa com as crianças, pode ser necessário informá-las ou educá-las acerca das tecnologias digitais ou dos seus direitos.[30]

IV. Capacidades evolutivas

19. As capacidades e níveis de compreensão das crianças evoluem ao longo da infância e são influenciados pelo respetivo contexto, experiência, espectativas e oportunidades. O envolvimento ativo das crianças com as tecnologias digitais pode ajudá-las a desenvolver as suas capacidades em relação a uma ampla variedade de informação, facilitando a sua aprendizagem, a partilha de experiências e a participação na respetiva comunidade de formas suscetíveis de reforçar e fomentar o respetivo crescimento e compreensão. O contacto com outras pessoas, incluindo outras crianças, favorece a sua autonomia, autoestima e sentido de pertença e estimula-as no seu próprio desenvolvimento. Nem todas as crianças ou contextos são iguais. A forma como usam e experimentam o ambiente digital será diferente consoante o respetivo contexto e capacidades em evolução.

---

[28] https://5rightsfoundation.com/In_Our_Own_Words_Young_Peoples_Version_Online.pdf.
[29] https://www.coe.int/en/web/children/participation.
[30] https://digitalfuturescommission.org.uk/wp-content/uploads/2020/10/Children-and-Young-Peoples-Voices.pdf.

Os investigadores e decisores políticos ainda debatem os prós e contras do impacto da tecnologia no desenvolvimento infantil. Muitos países estabeleceram diretrizes sobre a utilização de tecnologia pelas crianças, embora centradas, na sua maioria, na proteção, sendo necessário dar mais atenção a orientações relativas à maximização dos benefícios do acesso.[31] As restrições etárias aplicáveis ao setor podem estar mal assinaladas, ser incoerentes ou aplicadas de forma diferente pelas diversas plataformas. Podem também ser pouco respeitadas ou orientadas por considerações comerciais que pouco tenham em conta o nível de desenvolvimento e compreensão da criança. Tal pode resultar na oferta generalizada, a crianças de todas as idades, de conteúdos e contactos impróprios para a idade.

Os Estados devem tomar todas as medidas possíveis para garantir que as crianças de diferentes idades são encorajadas a não se envolverem com produtos e serviços impróprios para a sua idade. Para conteúdos potencialmente nocivos, a classificação etária, sistema que identifique para que idade ou faixa etária um produto ou serviço pode ser adequado – por exemplo, o sistema Pan Europeu de Informação sobre Jogos (PEGI) indica a idade mínima para a qual um videojogo pode ser considerado adequado, com base em fatores como violência, conteúdos sexuais ou palavrões[32]. Estas ferramentas não devem impedir o acesso das crianças a conteúdos para o público em geral nem restringir indevidamente a amplitude e diversidade dos conteúdos a que podem aceder ou impedi-las de aceder a conteúdos concretos de que necessitem para o gozo dos seus direitos e liberdades cívicas.

Contudo, os Estados não se devem concentrar unicamente nos conteúdos – mas sim considerar as pressões e comportamentos que os serviços exigem das crianças. Guias relativos a estas pressões, incluindo *AI for Children*[33] da Unicef e *Risky by Design*[34] da 5Rights Foundation, sugerem a realização de avaliações de impacto nas crianças no âmbito do desenvolvimento de produtos e serviços tal como exemplificado pelo Comissário para a E-Segurança da Austrália[35].

20. Os produtos e serviços são frequentemente desenhados por adultos para adultos e não têm em conta as necessidades das crianças. Práticas digitais como serviços de *streaming*, comércio eletrónico e redes sociais promovem muitas vezes comportamentos e mundos que estão para além das capacidades da criança afetada. Por exemplo, as fontes de desinformação que promovem opiniões de extrema-direita no Facebook têm em média mais 65% de interação por seguidor

---

31 https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282019%293&docLanguage=En.

32 https://pegi.info/page/pegi-age-ratings.

33 https://www.unicef.org/globalinsight/featured-projects/ai-children

34 https://www.riskyby.design/introduction

35 https://www.esafety.gov.au/about-us/safety-by-design.

do que outras páginas de extrema direita, o que é significativo se as crianças não tiverem capacidade para compreender que algo é falso[36]. As crianças podem necessitar de diferentes tipos de proteção em diferentes momentos e por diferentes prestadores de serviços. Não se pode dar como adquirido que as crianças mais velhas necessitem de menos proteção, visto que muitas crianças mais novas são supervisionadas e as mais velhas podem aceder a uma variedade de produtos mais alargada.

Os Estados devem tomar medidas para garantir que os produtos, serviços e ambientes que as crianças de facto usam[37] e aqueles que são obrigadas a usar têm em conta as respetivas necessidades. Para garantir os direitos das crianças em ambientes digitais, os seus direitos e necessidades concretas devem ser tidos em conta em todas as fases, do desenho à implementação, com quadros jurídicos e de proteção de dados em vigor para defender os seus direitos nos sistemas tecnológicos.

As medidas podem ser introduzidas através de legislação, códigos de conduta, regulamentação – mas deverão ser obrigatórias e sujeitas a controlo público, mecanismos de responsabilização e vias de recurso. As crianças podem ter um pensamento sofisticado sobre as implicações positivas e negativas da tecnologia digital e oferecer contribuições valiosas para essa discussão. A participação das crianças nas consultas, incluindo nas discussões relativas ao ambiente digital, não deve ser reduzida a processos de consulta única meramente formais ou ser limitada a temas definidos pelos adultos, por exemplo o processo de consultas instituído pelo Conselho da Europa. Estas discussões devem ser contínuas. Os decisores deverão assegurar-se de que, sempre que a criança seja capaz de formar as suas próprias opiniões, estas sejam seriamente tidas em conta. A forma como as opiniões das crianças forem consideradas e incorporadas nas decisões deve ser dada a conhecer aos participantes nas consultas.

21. Os pais e cuidadores têm um papel único nas vidas das crianças e devem ser ajudados a compreender o mundo digital. Podem ser apoiados através de guias e serviços específicos para cada país, por exemplo as diretrizes globais da União Internacional de Telecomunicações[38]. A autonomia evolutiva, as capacidades e a necessidade de privacidade das crianças mudam à medida que estas crescem e se desenvolvem. É necessário apoiar os pais e cuidadores na aquisição de literacia e sensibilização digital. Esta sensibilização deve permitir que os pais/cuidadores

---

[36] Fontes noticiosas de extrema direita mais apelativas no Facebook, *Cybersecurity for Democracy*, março de 2021, https://medium.com/cybersecurity-for-democracy/far-right-news-sources-on-facebook-more-engaging-e04a01efae90.

[37] Veja-se o exemplo do WhatsApp, que só pode ser usado por maiores de 16 anos na Europa, mas que 14% das crianças entre os 12 e os 15 anos no Reino Unido utilizam: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf.

[38] https://www.itu-cop-guidelines.com/.

alcancem um equilíbrio adequado entre a proteção das crianças e o respeito da sua autonomia emergente, por exemplo, para os jovens que exploram a sua sexualidade; e os jovens que procuram aconselhamento/tratamento médico independentemente dos seus pais/cuidadores.

Embora os pais e cuidadores necessitem de apoio, os Estados devem também exigir que os fornecedores de serviços digitais ofereçam ou disponibilizem às crianças serviços apropriados às suas capacidades em evolução, nomeadamente tornando os adolescentes capazes de gerir o seu próprio acesso à informação, aos serviços e aos dados pessoais e digitais assim gerados. Reconhecendo que os diferentes Estados têm legislação interna e limites etários diferentes, os Estados deverão ainda assim garantir que a informação e as atividades respeitam os direitos de todas as crianças, incluindo o seu direito à privacidade e a serem protegidas da exploração comercial e da violência.

V. Medidas gerais de aplicação pelos Estados Partes

22. Serão necessárias estruturas legislativas e formais, por vezes antes da existência de indícios formais de risco ou dano – por exemplo, o *Duty of Care* proposto pelo *Carnegie UK Trust*[39], que visa prevenir danos e não responder após a ocorrência destes.

A. Legislação

23. Muitas leis ainda referem ou preveem um mundo analógico e deverão ser atualizadas para apoiar expressamente a aplicação e observância da lei nos ambientes digitais. Os Estados devem rever e atualizar a sua legislação interna para garantir que o ambiente é compatível com os direitos consagrados na Convenção e seus Protocolos Facultativos. Os Estados devem introduzir e implementar legislação para garantir que as empresas respeitam os direitos da criança e serão responsabilizadas se não o fizerem. Os Estados devem também introduzir leis e políticas que impeçam as empresas de contribuírem para violações dos direitos da criança e prevejam a reparação das violações se estas ocorrerem. Por exemplo, as empresas devem por em prática processos que assegurem a devida diligência ao nível dos direitos da criança.

Toda a legislação deve focar-se na identificação dos riscos e defesa dos direitos da criança antes da ocorrência do dano. A atualização e introdução de legislação exige recursos e deverá constituir uma prioridade política. Para além dos enquadramentos legislativos, os Estados devem investir na implementação

[39] https://www.carnegieuktrust.org.uk/blog/the-statutory-duty-of-care-and-fundamental-freedoms/.

reforçando os reguladores e organismos de aplicação da lei competentes e garantindo que os mesmos dispõem das competências legais e dos conhecimentos técnicos necessários para desenvolver a capacidade de defender os direitos da criança consagrados na legislação relevante.

> "Eu mudaria … as leis [para garantir] que as empresas não têm poder para utilizar e partilhar a informação pessoal das pessoas sem a sua autorização."
>
> Nova Zelândia, rapariga, 16[40]

B. Política e estratégia abrangente

24. Os acordos existentes sobre salvaguarda das crianças em circunstâncias concretas, como tráfico, exploração comercial ou do consumidor, legislação em matéria de saúde e segurança e outras, devem ser revistos para garantir que referem expressamente o ambiente digital. Em alguns casos, os governos podem desejar desenvolver uma política específica de Proteção das Crianças nas Redes, por exemplo como no Ruanda[41] e no Gana[42]. Estas políticas devem procurar melhorar a experiência digital das crianças e não impedi-las de aceder ao ambiente digital.

25. No equilíbrio de responsabilidades, é importante que as empresas proporcionem um ambiente que minimize os riscos para as crianças. O mundo físico e os mundos das redes sociais estão estreitamente interligados, o que significa que o que acontece "nas redes" provavelmente não ficará só por aí e o que acontece "fora das redes" provavelmente acabará por entrar nelas. As crianças vítimas de exploração sexual "fora das redes" podem ser revitimizadas devido à difusão da sua imagem na Internet. As imagens podem ser reproduzidas e reaparecer indefinidamente em larga escala. As crianças que possam ter produzido voluntariamente imagens sexualizadas de si próprias a sós ou com um parceiro, ou crianças que tenham sido aliciadas ou coagidas a praticar atividades sexuais nas redes podem, após os factos, ser vítimas de extorsão ou chantageadas com a ameaça de exposição pública para que cumpram novas exigências. É imperativo que todos quantos tenham responsabilidades ao nível da proteção das crianças compreendam o impacto da tecnologia digital. Os responsáveis pela criação das tecnologias digitais deverão compreender a responsabilidade que têm na proteção das crianças contra estes riscos.

---

[40] *Our Rights in a Digital World*, p. 26.
[41] http://www.xinhuanet.com/english/2019-07/22/c_138248409.htm#:~:text=Having%20come%20into%20force%20in,Ministry%20of%20ICT%20and%20Innovatio.
[42] http://childsafety.gov.gh/.

As políticas devem prever e promover a formação e orientação das crianças, pais e cuidadores, profissionais competentes e público. Tais programas devem promover a sensibilização para os direitos da criança e formas de os proteger. Devem existir programas dirigidos às crianças e em formatos adaptados às mesmas, tendo expressamente em vista desenvolver as aptidões digitais das crianças e promover o seu conhecimento das oportunidades apresentadas pelas tecnologias digitais. Estas medidas devem fazer com que as crianças sejam capazes de utilizar o ambiente digital de forma benéfica e segura. Todas as vítimas e sobreviventes devem conhecer as vias de recurso à sua disposição em caso de violação dos seus direitos e receber apoio adequado à idade para reivindicar tais direitos ou, em certas circunstâncias, ser indemnizadas por tal violação.

26. As crianças acederão ao ambiente digital em todos os locais onde vivam ou que visitem. Consequentemente, as medidas de proteção das crianças nas redes deverão ser concebidas para proteger as crianças de forma sistemática – contra a criação, o carregamento, a difusão ou a amplificação do dano – quer estejam, por exemplo, em casa, em cuidados alternativos, na escola ou em cibercafés. Isto significa efetuar avaliações de risco aquando do desenho dos produtos e serviços e desativar funcionalidades cujos riscos possam ultrapassar os benefícios para as crianças, por exemplo os serviços de mensagens diretas[43] ou a partilha da localização em tempo real com outros utilizadores[44].

Embora as crianças possam desempenhar um papel importante na sua própria proteção, incumbe aos Estados e às empresas fornecedoras de tecnologias digitais garantir que os serviços ou dispositivos que proporcionam ou promovem são seguros para as crianças. A segurança das crianças nas redes não pode jamais ser enquadrada como uma responsabilidade que recai sobretudo ou exclusivamente sobre a criança ou seus pais ou cuidadores. Desde o momento da primeira utilização, todos os serviços ou dispositivos deverão ser fornecidos de uma forma que os torne tão seguros para a criança e garantísticos dos seus direitos quanto possível e todos os desvios desta norma deverão ser claramente assinalados e as suas possíveis consequências explicadas.

C. Coordenação

27. Os Estados devem identificar ou estabelecer um organismo público, instituição ou regulador mandatado para monitorizar e coordenar as políticas e programas relacionados com os direitos da criança no ambiente digital. Os Estados podem atribuir a responsabilidade por tal coordenação aos ministérios que tutelam a família, as empresas, a educação ou a justiça, ou a outro organismo. A questão é

---

[43] https://www.riskyby.design/the-risks.
[44] https://www.theguardian.com/technology/2016/jul/10/pokemon-go-armed-robbers-dead-body.

que as obrigações do Estado relativamente aos direitos da criança no contexto do ambiente digital exigem cooperação interinstitucional, devendo um dos organismos ficar responsável pela coordenação. Tal organismo deverá dispor de recursos suficientes para cooperar com as empresas, a sociedade civil e outras organizações ou partes interessadas com vista à realização dos direitos da criança e à promoção da segurança das crianças em ambiente digital. Deverá também ser capaz de aproveitar o conhecimento relevante, tecnológico, jurídico e de outra natureza, existente no seio da administração pública e fora dela, conforme necessário – incluindo em ONG e organismos de âmbito local e internacional que trabalhem nas áreas dos direitos da criança[45] e dos direitos digitais[46], devendo o respetivo mandato incluir também a colaboração com outros governos e organizações internacionais, a fim de promover a interoperabilidade e padrões exigentes em matéria de políticas digitais. Deve ser financiado de forma transparente e o seu funcionamento supervisionado com independência (*vide* parágrafo 29). Este organismo deve ser avaliado de forma independente pela sua eficácia no cumprimento das respetivas obrigações, bem como pela sua adesão às normas de direitos humanos. Deve ser claro para todas as partes interessadas, incluindo crianças e pais/cuidadores, qual é o principal organismo de coordenação junto do qual podem procurar aconselhamento e ao qual devem dirigir as suas queixas.

D. Afetação de recursos

28. Para cumprir a obrigação de garantir que as crianças conseguem exercer os seus direitos em ambiente digital de forma plena, equitativa e segura, os Estados deverão disponibilizar os recursos necessários. O ambiente digital terá um impacto crescente e cada vez mais significativo nas vidas das crianças e os Estados deverão investir o suficiente para se assegurarem de que cada criança consegue beneficiar deste desenvolvimento sem discriminação.

29. Embora as empresas comerciais devam suportar os custos da satisfação das necessidades de segurança das crianças suas clientes, os Estados deverão garantir que as instituições públicas responsáveis por garantir a segurança das crianças nas redes têm os recursos necessários para implementar políticas e programas adequados para preservar e proteger os respetivos direitos em ambiente digital e recursos para monitorizar o cumprimento pelas empresas das respetivas obrigações, investigar abusos e, se necessário, julgar e assegurar a reparação do dano em caso de incumprimento[47].

---

[45] Por exemplo, https://www.crcasia.org/.
[46] Por exemplo, https://africadigitalrightshub.org/.
[47] https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

Estes recursos devem ser independentes e não sujeitos a formas diretas ou indiretas de *lobbying* ou outras formas de pressão resultante de influência política ou interesses comerciais suscetíveis de comprometer o "interesse superior" ou outros direitos das crianças.

E. Recolha de dados e investigação

30. Os desafios da proteção e promoção dos direitos da criança em ambiente digital estão a mudar rapidamente e é necessário compreender os riscos emergentes, as tendências dos utilizadores[48] e os impactos nas crianças através de dados atualizados – por exemplo, mediante a utilização do conjunto de ferramentas de pesquisa de acesso livre desenvolvido pelo projeto *Global Kids Online*[49]. Os Estados devem financiar e recolher dados abrangentes de uma forma respeitadora dos direitos, tendo particularmente em conta o impacto da tecnologia digital sobre os diferentes grupos de crianças. A investigação pode também ser utilizada para orientar intervenções e desenvolvimento de políticas que apoiem os direitos da criança em ambiente digital[50]. A investigação e recolha de dados públicos deverão respeitar todos os direitos da criança, incluindo os direitos à vida privada e à não discriminação. As próprias crianças devem participar no desenvolvimento da agenda de investigação, bem como no processo de investigação em si mesmo. Os Estados devem apoiar o crescente, mas muitas vezes mal sucedido, esforço para obter das empresas dados sobre a utilização dos respetivos serviços por crianças, seus efeitos e formas como as crianças denunciam/se queixam e em que números. Sempre que necessário, os Estados devem proporcionar aos investigadores acesso a dados anónimos acerca da utilização da tecnologia digital pelas crianças a fim de obter dados capazes de orientar as políticas.

F. Monitorização independente

31. O mandato da maioria das instituições nacionais de direitos humanos resulta da legislação e é imperativo que qualquer mandato para investigar e dar seguimento a queixas lhes confira também claramente competência para atuar no

---

[48] Por exemplo, "desafios" inseguros em redes sociais como o TikTok e o Instagram podem ser amplificados por algoritmos de recomendação, os quais podem fazer com que tais desafios se espalhem rapidamente e cheguem às crianças. Dois exemplos recentes de tais "desafios" arriscados são o *Blackout*, que levou à morte de uma menina de dez anos em Itália, bem como a difusão do vídeo de um suicídio no meio de vídeos de gatinhos e cachorrinhos.

[49] www.globalkidsonline.net/tools.

[50] https://www.unicef-irc.org/publications/1065-childrens-experiences-online-building-global-understanding-and-action.html.

contexto do ambiente digital. Contudo, dado o alcance e a escala do ambiente digital, juntamente com a natureza multifatorial dos direitos humanos e direitos da criança, é provavelmente inevitável que venham a estar envolvidos vários organismos na monitorização ou aplicação dos direitos da criança. Os Estados devem assim garantir que existe uma adequada coordenação e uma plena e pública delimitação dos papéis e responsabilidades dos diferentes organismos envolvidos.

F. Difusão de informação, sensibilização e formação

32. O Comentário Geral n.º 25 foi expressamente concebido para identificar as ações dos Estados e responsabilidades das partes interessadas que sejam necessárias para realizar os direitos da criança em ambiente digital. Para que estes se tornem efetivos, será necessário que todas as partes compreendam estas obrigações e deveres. Isto exige uma ampla sensibilização pública, incluindo, mas não unicamente, das crianças, pais e cuidadores, bem como formação específica para decisores políticos, empresas e todos quantos prestem serviços de primeira linha a crianças.

Os programas de sensibilização devem também ter em conta a experiência de vida e as opiniões das crianças. As campanhas de sensibilização pública devem abranger todo o tipo de riscos (anexo) e encorajar a criação de um ambiente respeitador dos direitos da criança. Em particular, devem ser feitos esforços para garantir que tais campanhas chegam além dos segmentos mais privilegiados da sociedade e incluem os grupos minoritários e em situação de desvantagem. Os pais e cuidadores necessitam de informação e competências para ajudarem a criar ambientes seguros para a participação digital das crianças, mas tal não isenta os governos ou empresas das suas responsabilidades para com as crianças e seus cuidadores nem transfere para outrem tais responsabilidades.

33. Os profissionais que trabalham com e para crianças em todos os ambientes, incluindo estabelecimentos de ensino, de saúde e saúde mental, serviços sociais, instituições de cuidados alternativos, organismos de aplicação da lei, sistema de justiça no seu conjunto e setor empresarial, e os que desenham sistemas informáticos para tais ambientes, devem receber uma formação que inclua a forma como o ambiente digital influencia os direitos da criança em múltiplos contextos, as formas como as crianças podem aceder e utilizar as tecnologias e o impacto que os sistemas informáticos podem ter no futuro da criança. Os Estados devem garantir que é proporcionada formação relevante, inicial e contínua.

Aqueles que desenvolvem tecnologias digitais (incluindo, mas não apenas, o setor tecnológico, organismos públicos e mundo académico) devem integrar a formação em matéria de direitos da criança nos programas nacionais de desenvolvimento de capacidades, programas pedagógicos e normas de desenho. Exemplo disto é a

Estratégia Nacional para a Infância da Finlândia[51], que utiliza a Convenção sobre os Direitos da Criança das Nações Unidas para considerar de que forma os direitos da criança devem informar todas as áreas da sociedade finlandesa. Os Estados devem proporcionar formação inicial e contínua para garantir que os profissionais continuam a par com as mais recentes tendências e conhecimentos.

Estes esforços de formação devem abranger princípios de desenho centrado na criança, proteção de dados e direitos da criança, sendo necessário que reconheçam e tomem medidas contra o abuso sexual de crianças. As funcionalidades que se sabe serem perigosas para as crianças devem ser claramente identificadas, por exemplo as que apresentam adultos a crianças ao acaso através de sugestões de amizade. As funcionalidades positivas que permitem às crianças exercer os seus direitos devem também ser identificadas e encorajadas, como serviços digitais para crianças que garantam a privacidade dos dados, para que possam obter apoio sem receio de contribuir para a respetiva identidade digital de uma forma que fuja ao seu controlo.

H. Cooperação com a sociedade civil

34. Muitas organizações da sociedade civil são ativas e conhecedoras dos direitos da criança e algumas organizações especializadas dispõem de conhecimento específico sobre certa área (ou áreas) dos direitos e/ou experiências digitais das crianças. Os Estados devem envolver tais organizações no desenvolvimento das suas políticas e programas para garantir que atingem o nível mais exigente possível na promoção e proteção dos direitos das crianças em relação ao ambiente digital. É improvável que os vários grupos ou interesses que representam ou defendem os direitos da criança venham alguma vez a estar em pé de igualdade, mas os Estados têm a responsabilidade de garantir que tais grupos dispõem dos meios necessários para desempenhar as suas tarefas a um nível satisfatório e que as suas opiniões, contribuições e conhecimentos especializados são ouvidos relativamente ao processo decisório.

I. Direitos da criança e setor empresarial

35. O Comentário Geral n.º 25 dirige-se aos Estados, mas o desenho e a gestão do mundo digital estão em larga medida nas mãos da indústria e outras organizações não governamentais. Por exemplo, em relação à proteção de dados, crianças que procuravam serviços de saúde mental constataram que os seus dados estavam a ser vendidos a terceiros[52] para fins publicitários e crianças não brancas foram mal

[51] https://minedu.fi/en/strategy-for-children.
[52] https://privacyinternational.org/node/3193.

identificadas por sistemas de reconhecimento facial treinados em caras brancas[53]. O Comentário Geral n.º 25 enuncia as formas como as empresas e outras organizações devem e podem realizar os direitos das crianças e que medidas os Estados devem exigir das empresas.

A efetiva avaliação das políticas depende muitas vezes das próprias empresas digitais e da investigação que estas financiam ou permitem, por exemplo ao disponibilizarem os dados a investigadores independentes. Os Estados devem garantir a possibilidade de levar a cabo estudos independentes com vista a obter contribuições bem informadas e baseadas na evidência que apoiem o desenvolvimento de políticas, por exemplo estabelecendo o domínio público sobre grandes conjuntos de dados para que organizações ou universidades envolvidas em formas adequadas de investigação lhes possam ter acesso.

36. Os Estados devem cumprir as suas responsabilidades garantindo que as empresas são obrigadas a fornecer produtos e serviços que não violem nenhum dos direitos da criança em qualquer ambiente. Devem ser tomadas providências para prevenir violações e, caso estas possam ocorrer ou tenham ocorrido, deverão existir, em regra, vias de queixa e de recurso acessíveis, rápidas e eficazes.

A prestação de aconselhamento a pais e crianças é útil, nomeadamente sobre a forma como as crianças podem utilizar produtos e serviços de formas que lhes sejam benéficas, embora este aconselhamento complemente e não substitua os serviços desenhados para proteger e antecipar a presença das crianças e as vias de recurso informais e formais.

37. Indivíduos e grupos coordenados podem tentar atentar contra os direitos da criança de formas regulares mas em crescendo, por exemplo através da desinformação sobre questões de saúde que leve a que crianças deixem de ser vacinadas[54], ou de formas agudas, por exemplo mediante a publicação de conteúdos que encorajem o suicídio[55]. Estes problemas podem ser amplificados pelo desenho e práticas empresariais das empresas de internet, que tendem a dar prioridade à difusão de informação (alcance), à interação com os utilizadores e à maximização do tempo passado nas redes, em detrimento da moderação ou da criação de uma experiência adequada à idade.

Os Estados têm a responsabilidade de proteger as crianças de atentados aos seus direitos e dos riscos conhecidos e emergentes e, caso sejam provocados danos, de agir de forma rápida e vigorosa para apreciar o caso, ressarcir e apoiar as crianças. Os Estados devem assegurar-se de que as empresas cumprem a sua

---

[53] https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.
[54] https://www.vox.com/recode/22319681/vaccine-misinformation-facebook-instagram-spreading
[55] https://www.bbc.co.uk/news/av/uk-46966009

responsabilidade de respeitar os direitos das crianças de uma forma que seja consistente, transparente, responsável e eficaz.

38. Os Estados devem exigir que as empresas exerçam a devida diligência relativamente aos direitos da criança, para que identifiquem, previnam e mitiguem o impacto das suas atividades nestes direitos, nomeadamente em todas as suas relações empresariais e no âmbito das operações globais. Dados os riscos acrescidos que o ambiente digital comporta para as crianças, tal deverá constituir uma prioridade e deve ser acompanhado de perto pelo Estado. Tanto quanto possível, a prestação de contas por parte das empresas sobre os resultados deste processo de devida diligência deve ser tornada pública e constituir uma fonte de aprendizagem e reflexão para informar as políticas. Os Estados devem levar a cabo avaliações de impacto[56] nos direitos da criança da legislação em vigor e em preparação a fim de garantir que o ambiente digital é compatível com a CDC e seus Protocolos Facultativos[57].

Os Estados devem, não só tomar medidas adequadas para "prevenir, monitorizar e investigar" violações dos direitos da criança pelas empresas no ambiente digital, mas também tomar medidas adequadas e elaborar legislação apropriada para agir quando as empresas comerciais de abstêm de proteger adequadamente as crianças de violações no âmbito dos seus ambientes digitais.

39. Para além da legislação nacional e dos tratados internacionais, é necessário que todos os agentes do ecossistema digital respeitem os direitos da criança. Os códigos de indústria, normas de desenho, condições de serviço e outras atividades levadas a cabo no desenvolvimento e fornecimento de produtos e serviços digitais devem ser respeitadores dos direitos.

A posse de enormes conjuntos de dados que possam ser usados para testar ou desenvolver novos produtos ou serviços é um meio fundamental para que as empresas digitais estabelecidas possam reforçar e alargar o seu domínio do mercado. Isto, juntamente com o efeito de rede, ajuda a criar e a manter monopólios que podem tornar as empresas imunes ao apelo para respeitar os direitos da criança.

Os Estados devem encorajar as empresas a desenvolver produtos e serviços digitais no "interesse superior da criança" e garantir que as providências que tomaram são transparentes e numa linguagem compreensível para as crianças e seus pais/cuidadores.

J. Publicidade comercial e *marketing*

[56] https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf.
[57] https://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx.

40. Muitos produtos e serviços são altamente comerciais e dependem do processamento dos dados dos utilizadores para gerar rendimento. O desenho tendente a otimizar ao máximo o processamento de dados pode ter um profundo impacto na interação da criança com o ambiente digital, naquilo que vê, como se altera o seu comportamento e quão intrusivo pode o serviço ser. Sobre este ponto, ONG e organismos de consumidores noruegueses têm vindo a desenvolver um trabalho amplamente respeitado[58]. Exemplos do impacto de tais padrões podem ser observados com serviços que oferecem conteúdos progressivamente mais extremos, sugerindo que os utilizadores acrescentem amigos ou falem com estranhos ou utilizando notificações em grande escala durante a noite de forma a interromper o sono, podendo assim alterar as vidas quotidianas dos seus utilizadores. Tais produtos e serviços podem não ser considerados respeitadores dos direitos e devem ser "atenuados", "desligados" ou regulados de forma compatível com os direitos da criança, por exemplo os direitos à privacidade, à vida interior ou a não ser vítima de exploração comercial.

> "Passar demasiado tempo na Internet faz com que as pessoas não brinquem, não socializem com os pais e amigos e provoca privação do sono e doença mental."
>
> Brasil, rapariga, 13[59]

Muitas destas características não são essenciais ao desempenho do produto e serviço que a criança está a utilizar, estando sim concebidas para dar prioridade a resultados que favorecem a empresa privada. Os Estados devem tomar providências para garantir que os resultados respeitam os direitos da criança.

41. No mundo digital, a publicidade assume muitas formas:

- Publicidade de contexto: integração subliminar de publicidade em conteúdos de Internet ou serviços digitais, fazendo com que os utilizadores permaneçam imersos no conteúdo e características do serviço e, simultaneamente, sejam expostos ao marketing e a mensagens da marca;
- Publicidade dirigida: prática de exibir determinados anúncios a certos utilizadores com base em dados recolhidos sobre estes últimos, por exemplo a sua atividade na Internet, compras, localização, género, idade, preferências, etc.;
- Colocação de produto: inclusão de produtos da marca em conteúdos não explicitamente destinados a publicidade, com a intenção de promover subtilmente tal produto;

---

[58] https://www.consumerwatchdog.org/sites/default/files/2018-06/2018-06-25%20Deceived%20by%20design%20-%20Final.pdf

[59] *Our Rights in a Digital World*, p. 39.

- Influenciadores: utilizadores de redes sociais com grande número de seguidores, que usam a sua plataforma para promover as suas opiniões e/ou produtos preferidos junto dos respetivos seguidores; e
- Conteúdo patrocinado: publicações em redes sociais criadas pelos utilizadores ao abrigo de contratos com marcas com vista à promoção dos respetivos produtos.

Todas as crianças (bem como muitos utilizadores adultos) têm dificuldade em identificar conteúdos pagos, o que as deixa vulneráveis à coação. Por exemplo, a indústria tabaqueira começou recentemente a usar influenciadores para promover cigarros a vapor. Muitos influenciadores têm públicos muito jovens[60].

Os Estados devem obrigar a que todos os conteúdos comerciais sejam claramente identificados e identificáveis e que toda a publicidade seja sempre apropriada. Por exemplo, o regulador do Reino Unido tem estado a trabalhar num enquadramento da publicidade adaptado à idade[61].

42. Os decisores políticos devem considerar a hipótese de adotar medidas especiais de proteção das crianças, como a proibição da utilização dos dados relativos às emoções das crianças para finalidades de *marketing* junto das próprias crianças ou seus pais. Por exemplo, se uma criança manifestar pensamentos de tristeza para o seu brinquedo, a publicidade dirigida aos seus pais de produtos destinados a fazer a criança feliz será contrária à ética e constituirá exploração e violação de privacidade.

A publicidade no mundo digital pode ser altamente personalizada. Por exemplo, em 2017 o Facebook partilhou dados relativos ao estado psicológico de jovens com os seus anunciantes[62]. Mesmo que as plataformas não deem indicações quanto ao estado mental das crianças, estas podem ser identificadas como tendo determinados interesses, por exemplo por exercício e desporto que, se identificados, permitem às empresas torná-las alvos de publicidade a produtos como suplementos alimentares, regimes dietéticos ou cirurgia estética.

A informação sobre qualquer forma de processamento de dados pessoais pode ser dada de forma concisa e clara aos pais ou cuidadores da criança. É aconselhável fornecer também uma versão adaptada às crianças da mesma informação. A obtenção do consentimento dos pais ou cuidadores não isenta as instituições privadas de seguir as normas relativas aos direitos da criança desde a fase de desenho[63] ou de defender o interesse superior da criança. Os Estados

---

[60] https://www.reuters.com/article/us-instagram-vaping-idUSKBN1YN15B.
[61] https://www.asa.org.uk/uploads/assets/uploaded/3af39c72-76e1-4a59-b2b47e81a034cd1d.pdf.
[62] https://www.marketwatch.com/story/facebook-says-it-doesnt-target-vulnerable-teens-with-ads-but-it-has-studied-them-2017-05-01.
[63] https://childrensdesignguide.org/.

devem dispor de uma legislação nacional rigorosa que impeça a utilização dos dados pessoais das crianças para as tornar alvos de publicidade.

K. Acesso à justiça e vias de recurso

43. Os sistemas digitais são frequentemente opacos e complexos e não é razoável esperar que pais e crianças lidem com as violações se tiverem de agir a título individual nem expor determinadas crianças a escrutínio para conseguir que os fornecedores de serviços digitais tomem medidas. Existe uma desproporcional diferença de poder entre uma criança e as empresas multinacionais. Muitas vezes, também não é claro em que jurisdição o processo deve ser instaurado. A legislação deve proporcionar um enquadramento claro para o acesso à justiça e às vias de recurso, como os recursos, responsabilidades e sanções enunciadas no Regulamento Geral sobre a Proteção de Dados da UE[64].

Muitos dos termos publicados (nomeadamente, mas não só, os termos e condições, regras comunitárias e avisos de privacidade) são longos, legalistas e pouco claros – as crianças utilizadoras, seus pais ou cuidadores não conseguem, em geral, compreendê-los. A informação deve ser fornecida de forma concisa e clara, em formatos que a criança aprecie e que sejam facilmente compreendidos pela criança, seus pais ou cuidadores. O fornecimento de informação em formatos acessíveis não é suficiente, devendo a informação apresentada respeitar os direitos da criança.

44. Para que as crianças tenham acesso à justiça, é necessário legislação robusta, acesso a ajuda especializada e disposições que permitam a ação coletiva. Tal ação deve ser gratuita, segura, confidencial, sensível, atempada e adaptada às crianças. É importante notar que o conhecimento dos direitos é uma questão autónoma e diferente do acesso à justiça. Os Estados devem estabelecer mecanismos para responsabilizar as empresas e não deixar aos indivíduos o ónus de demandar judicialmente empresas multinacionais.

Adicionalmente, é problemático que as comunidades de aplicação e regulação não disponham de formação suficiente para apoiar as crianças no mundo digital, com todas as suas complexidades, potenciais danos e complicações jurisdicionais. Há uma necessidade urgente de garantir formação especializada a funcionários responsáveis pela aplicação da lei, advogados, procuradores e juízes e de assegurar a designação de serviços especializados para satisfazer as necessidades concretas das crianças e que tais serviços sejam adequadamente financiados e acessíveis às crianças em condições de igualdade e sem discriminação.

Os dados relativos a crianças no sistema de justiça são particularmente sensíveis e exigem salvaguardas e proteções adicionais. Os registos das crianças em contacto

[64] https://gdpr-info.eu/chapter-8/.

com o sistema de justiça penal devem ser mantidos em condições de rigorosa confidencialidade e fechados a terceiros, exceto as pessoas diretamente envolvidas na investigação e julgamento do caso. Adicionalmente, qualquer forma de recurso ou procedimento para responder a violações dos direitos da criança e a abusos de crianças em ambiente digital deverá garantir a proteção do sigilo relativamente à identidade da criança vítima e outra informação pessoal pertinente.

Os Estados devem garantir que as crianças que recorrem à justiça são protegidas contra manobras de retaliação ou intimidação, quer por parte dos alegados infratores, quer por agentes estaduais, agentes do setor privado, sociedade civil ou familiares. Na instauração do processo, pode haver opacidade das estruturas empresariais e suscitarem-se dúvidas quanto à instância junto da qual devem ser apresentadas as queixas e de que forma. Existe pouca jurisprudência e o apoio jurídico pode não estar disponível. Os Estados devem garantir que a privacidade das vítimas é protegida ao longo do processo, que está disponível apoio jurídico e que as vias de recurso incluem a cooperação transnacional. As empresas devem ser encorajadas a assegurar a existência, no seu próprio seio, de mecanismos de recurso eficazes. Se necessário, o Estado deve também estabelecer e financiar um mecanismo adaptado a crianças para a receção de petições anónimas co vista à instauração de inquérito com base em procedimentos pré-estabelecidos e validados.

45. As ferramentas ou produtos técnicos que identifiquem as vítimas e sobreviventes ou os delinquentes devem ser complementadas com estratégias que ofereçam vias de apoio às crianças. Os Estados devem integrar o apoio às vítimas e sobreviventes nos quadros de proteção das crianças e reconhecer que a difusão de imagens representa uma ameaça contínua de revitimização. Os Estados devem ir além dos crimes mais graves e assegurar-se de que a reparação e o apoio estão à disposição das crianças para todos os tipos de abuso de direitos e que a natureza e escala do apoio são compatíveis com a violação. Por exemplo, o apoio e reparação de que necessitam as crianças vítimas de burlões ou discriminadas devido à inclusão abusiva numa base de dados serão diferentes dos que necessita uma criança que tenha, por exemplo, sido coagida a entrar num gangue ou sofrido abuso sexual.

Existem muitos indícios de que os programas de reeducação para o tratamento de delinquentes, por exemplo os avaliados pela *EU Rehab Children*[65], constituem um fator importante para interromper o alastramento dos abusos. Estes programas podem ser impopulares junto dos políticos e do público visto que parecem desviar recursos para os autores de crimes repugnantes, mas os peritos lembram que um

[65] A *EU Rehab Children* publicou diretrizes de boas práticas em toda a Europa - http://www.famylias.org/wp-content/uploads/2015/05/Handbook-of-Best-Practices-in-Juvenile-Rehabilitation-Programs-in-Europe-LD.pdf.

único agressor pode ter muitas vítimas, pelo que a retirada de cada um do sistema pode vir a beneficiar muitas crianças. Além disso, existe a necessidade de compreender como funcionam os agressores. Estes estudos são muito importantes para aperfeiçoar os programas de prevenção e proteção.

46. Para além dos esquemas de recurso e reparação legais e patrocinados pelos governos, existem muitos casos em que a resposta pode ter que vir das empresas. Será necessário que os Estados adotem normas obrigatórias em matéria de desenho e funcionamento das tecnologias digitais, mas também normas sobre moderação, resposta, reparação e indemnização. É também necessário que os mecanismos de queixa das empresas tenham em conta a idade e etapa de desenvolvimento das crianças, devendo ser transparentes, suscetíveis de responsabilização independente e executáveis.

Os Estados devem proporcionar oportunidades para que as crianças e jovens recorram das reparações concedidas se estas forem desproporcionais ao dano sofrido.

Deve ser dada atenção específica ao desenvolvimento de um quadro e à disponibilização de recursos eficazes para apoiar as crianças que tenham, elas próprias, comportamentos nocivos em meio digital. As respostas a estes comportamentos devem ser educativas e não punitivas, reconhecendo os fatores sociais e contextuais que possam ter contribuído para a situação, incluindo a experiência na apresentação de queixa.

47. É necessária a cooperação internacional no caso de muitas violações, incluindo, mas não só, o abuso sexual de crianças, o aliciamento por organizações extremistas, as burlas, fraudes e roubo de identidades – e as violações de dados. Barreiras como diferenças na tipificação dos crimes, diferentes normas em matéria de proteção de dados, diferentes proteções para os vários grupos etários – e falta de compreensão dos direitos da criança e do funcionamento da tecnologia digital, ou de ambas as questões – podem impedir uma cooperação eficaz.

Os Estados devem tentar partilhar conhecimentos, harmonizar definições e trabalhar para cumprir as exigências de iniciativas internacionais como o Painel de Alto Nível do Secretário-Geral da ONU sobre Cooperação Digital[66], o Eixo Digital para o Desenvolvimento da União Europeia (D4D)[67] e a sua primeira colaboração regional com a União Africana.

48. Os Estados devem garantir que a legislação e regulamentação nacional estabelecem medidas de proteção e direitos de participação das crianças

---

66 https://www.un.org/en/pdfs/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ENG.pdf.

67 https://d4dlaunch.eu/#about.

relativamente a todos os produtos e serviços digitais que operem no seu território. Devem também juntar forças com as organizações regionais e internacionais com vista à definição de normas universais a fim de que as crianças em jurisdições com ambientes de regulação menos amadurecidos beneficiem das mesmas proteções que as que se encontram em sociedades mais conectadas.

49. As crianças devem conseguir compreender os seus direitos e vias para obter justiça, pelo que a informação deve ser fornecida em formatos e línguas que compreendam. Devido à natureza transnacional dos abusos em ambiente digital, a cooperação transfronteiriça entre os Estados é fundamental para assegurar a eficácia das vias de recurso, uma vez que agressores e vítimas se podem encontrar em países diferentes. O fornecimento de informação, por si só, não é suficiente, devendo ser asseguradas vias apoiadas para acesso à justiça e à ação coletiva.

VI. Direitos e liberdades civis

A. Acesso à informação

50. As crianças querem, necessitam e têm direito de acesso à informação. O ambiente digital constitui uma fonte de informação fundamental para todas as áreas de interesse das crianças e os Estados têm a obrigação de facilitar este acesso a todas as crianças. As únicas limitações ao exercício do direito à informação colocam-se quando é necessário respeitar os direitos de reputação de terceiros ou para proteger a segurança nacional, a ordem pública ou a saúde pública.

> "À medida que o tempo passa e a tecnologia se desenvolve, podemos aceder facilmente e obter informação. Mas é difícil saber se a informação é válida ou não."
>
> Indonésia, rapariga, 14[68]

O ambiente digital está desenhado de uma forma singular que significa que muita da informação que a criança vê é gerada automaticamente[69]. Isto cria uma tensão entre o direito de acesso da criança e o desejo (em grande parte comercialmente determinado) de uma empresa, organização ou pessoa de colocar informação à frente da criança ou da criança enquanto parte de um grupo mais alargado. A este respeito, o direito de acesso da criança não deve ser confundido com o desejo do terceiro de aceder à criança ou de a influenciar. As crianças não devem ser forçadas a ouvir nem bombardeadas com informação não solicitada.

---

[68] *Our Rights in a Digital World*, p. 14.

[69] Por exemplo, o algoritmo de recomendação do YouTube é responsável por 70% dos conteúdos a que as pessoas assistem. https://www.cnet.com/news/youtube-ces-2018-neal-mohan/

A legislação deve prever expressamente mecanismos que incluam a literacia para os media e a informação enquanto ferramentas nacionais, para promover a utilização do ambiente digital tendo em vista o acesso a uma ampla variedade de informação de qualidade, reconhecendo a possibilidade única do ambiente digital de fornecer informação em múltiplos formatos e de formas que sejam apelativas e excitantes para crianças de todas as idades.

51. Os Estados devem usar todas as alavancas políticas à sua disposição para garantir que as crianças têm acesso nas redes a informação diversificada e de qualidade que dê prioridade aos benefícios sociais e culturais e aos materiais destinados a promover o bem-estar e a saúde, em detrimento da maximização dos lucros.

52. Os Estados devem assegurar-se de que as crianças conseguem aceder a uma variedade muito ampla de informação proveniente de diversos meios de comunicação e outras fontes, incluindo informação detida por organismos públicos. Esta capacidade de acesso a informação pertinente pode ter um significativo impacto positivo sobre a igualdade.

Além disso, as questões de interesse específico para as crianças devem estar à sua disposição na sua própria língua ou em formatos que compreendam. Por exemplo, as crianças com deficiência visual necessitam que a informação seja disponibilizada em formatos áudio[70] e o Relator Especial sobre tráfico de crianças recomendou a criação, em ambiente digital, de conteúdos adaptados a crianças e respetivas idades, incluindo a disponibilização de informação sobre o risco de tráfico para todas as formas de exploração, aliciamento e abuso.

53. Os Estados devem apoiar o acesso das crianças a informação de boa qualidade que seja independente de interesses comerciais ou políticos. A desinformação e informação enganosa interferem nestes objetivos[71]. As crianças não têm a capacidade de processar grandes quantidades de informação falsa, por exemplo páginas de negação do Holocausto, desinformação sobre questões de saúde ou falsidades a respeito de figuras públicas ou grupos sociais, nem se deve esperar que o façam[72]. Os Estados devem assegurar-se de que a informatização e os sistemas de filtragem, incluindo os utilizados pelas empresas para recomendar ou ordenar conteúdos, são de alta qualidade e não priorizam conteúdos por razões de lucro ou interesse político.

54. O ambiente digital é um sistema complexo, mas isto não o isenta das responsabilidades de defesa dos direitos da criança. A informação pode vir de indivíduos, nomeadamente outras crianças, de grupos, incluindo grupos de

---

[70] *Two clicks forward and one click back*, Relatório sobre crianças com deficiência em ambiente digital, CoE, 2019.
[71] https://rm.coe.int/information-disorder-report-november-2017/1680764666.
[72] https://www.bbc.co.uk/news/blogs-trending-38156985.

crianças, ou de organizações, empresas ou através de meios automatizados. Todos os sistemas digitais deverão, com regularidade, identificar, prevenir e tomar providências para mitigar os riscos da informação nociva e tendenciosa para as crianças. Muitos destes riscos podem ser identificados e mitigados com a introdução de um processo de devida diligência, por exemplo avaliando o impacto nas crianças e informando das respetivas conclusões e medidas tomadas. Estes riscos incluem concretamente os *feeds* e algoritmos das redes sociais. O Comentário Geral n.º 16 (2013) sobre as obrigações do Estado relativamente ao impacto do setor empresarial nos direitos da criança tem mais informação sobre tais processos[73].

A mitigação não deve excluir automaticamente as crianças, mas antes procurar soluções tecnológicas e administrativas. Por exemplo, a introdução de legislação no Reino Unido[74] teve como resultado a desativação, pelas empresas, das funcionalidades de mensagem direta[75] (quando a informação pode ser partilhada em privado com crianças), a introdução de definições de privacidade mais exigentes por defeito[76], a retirada de publicidade a atividades ou conteúdos impróprios para crianças, como produtos dietéticos e para perda de peso[77], o investimento em tecnologia mais sofisticada para classificar a adequação dos conteúdos aos diferentes grupos etários[78] e que só o acesso a conteúdos claramente impróprios, como pornografia extrema ou páginas de encontros, é restringido em função da idade. Muitos destes riscos são automatizados e amplificados. Os Estados deverão exigir que os fornecedores de sistemas digitais garantam a não amplificação dos riscos.

O *ciberstalking* e o *ciberbullying* são fenómenos que estão a aumentar e as crianças são as vítimas mais fáceis e mais comuns destes fenómenos[79]. Contudo, são também, por vezes, as autoras de tais comportamentos. Ao aplicarem políticas e leis para dar resposta ao *ciberbullying* e *ciberstalking* cometidos por crianças, os Estados devem, na máxima medida possível, evitar criminalizar as crianças e focar-se em soluções de reparação e educação. A posição dos pais e tutores legais deve também ser considerada, devendo os mesmos receber apoio para resolver tais situações de forma construtiva.

---

[73] https://undocs.org/CRC/C/GC/16.
[74] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.
[75] https://www.bbc.com/news/technology-52310529
[76] https://newsroom.tiktok.com/en-us/strengthening-privacy-and-safety-for-youth.
[77] https://newsroom.tiktok.com/en-us/coming-together-to-support-body-positivity-on-tiktok.
[78] https://www.theverge.com/2020/9/22/21449717/youtube-age-restriction-machine-learning-rollout-kids-content-monetization-creators.
[79] https://violenceagainstchildren.un.org/news/ending-torment-tackling-bullying-schoolyard-cyberspace.

55. A classificação dos conteúdos constitui uma forma não intrusiva de indicar a adequação dos conteúdos digitais a crianças, de acordo com as respetivas capacidades em evolução. Para além disso, deve estar facilmente acessível e ser difícil de ignorar informação concisa e adaptada à idade acerca dos serviços, tipos de conteúdo e moderação de conteúdos. A apresentação de queixa deve ser fácil e clara para uma criança utilizadora.

Todos os sistemas de controlo de conteúdos devem ser compatíveis com padrões exigentes de minimização de dados, por exemplo os enunciados no RGPD, estabelecidos na Lei de Proteção dos Jovens da Alemanha[80] e resumidos pelo Gabinete do Comissário para a Informação do Reino Unido[81].

56. Nenhum ambiente está isento de riscos para as crianças e muitas crianças desejam aceder ao ambiente digital, pelo que as medidas de proteção devem ser proporcionais e respeitar todos os direitos. Com demasiada frequência, os direitos e necessidades das crianças são ignorados na criação e funcionamento do ambiente digital. Os Estados devem garantir que estão em vigor leis e regulamentos para proteger as crianças e que os fornecedores de serviços digitais cumprem as exigências legais e os códigos de conduta voluntários aos quais se tenham comprometido.

São frequentemente utilizados controlos técnicos para proteger as crianças. Estes são apenas uma ferramenta e não devem ser usados de formas que restrinjam os direitos à informação, à expressão e à privacidade das crianças e adolescentes. Devem ser acrescentados mecanismos reguladores e não reguladores para os avaliar, modificar e eliminar (se necessário).

57. Os Estados deverão assegurar-se de que as crianças têm a possibilidade de denunciar e apresentar queixa sem comprometer a sua privacidade ou revelar publicamente a respetiva identidade.

B. Liberdade de expressão

58. A liberdade de expressão não depende de qualquer forma de tecnologia ou meio digital em particular. O ambiente digital está a emergir como uma arena cada vez mais dominante para que as crianças exprimam as respetivas ideias, identidade, opiniões ou posições políticas. Isto pode ser particularmente importante para as crianças que estão isoladas, seja pelas suas circunstâncias específicas, como crianças refugiadas ou em instituições de acolhimento, seja pela

[80] http://dipbt.bundestag.de/extrakt/ba/WP19/2685/268540.html.
[81] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

geografia, pertença a comunidades rurais ou cujas vozes sejam menos ouvidas, por exemplo devido ao seu género ou pertença a uma minoria indígena[82].

59. Quaisquer restrições à liberdade de expressão das crianças em ambiente digital devem ser excecionais, não discriminatórias e claramente articuladas numa língua e formato que a criança possa compreender. Deverão também ser legais, transparentes e proporcionais. Por exemplo, não devem ser usados filtros para restringir desproporcionalmente o acesso de certas crianças ou de grupos ou comunidades de crianças com determinadas características ou em determinados contextos, por exemplo com base no respetivo género ou orientação sexual[83].

As crianças são participantes e criadoras no mundo digital e embora não possam ser responsabilizadas pelas ações de empresas ou terceiros, necessitam de ter acesso a uma informação e educação que as ajude a compreender os seus direitos e a respeitar os direitos dos demais.

60. A experiência de assédio ou abuso tem um impacto significativo na confiança e bem-estar das crianças e pode ter consequências tanto dentro como fora das redes. Isto é especialmente verdade para aquelas cujas identidades se intersetam, nomeadamente com base na raça, classe, identidade de género e orientação sexual. Os Estados devem desenvolver e implementar iniciativas que apoiem um ambiente digital seguro. Isto inclui programas educativos e de sensibilização sobre cidadania digital, uma ampla variedade de serviços de apoio como linhas telefónicas de atendimento às vítimas, formação de funcionários em matéria de proteção das crianças defensoras de direitos humanos e a recolha e publicação de dados desagregados por idade, género e outras características sobre assédio nas redes.

Os Estados devem garantir que as crianças não sofrem abusos cometidos através das redes e que a liberdade de expressão é equilibrada com a proteção contra a violência.

Aquilo que pode ser considerado um debate robusto e saudável no mundo dos adultos pode nem sempre se traduzir diretamente no mundo das crianças, pelo que é necessário estabelecer diretrizes claras para definir os limites do comportamento aceitável. Tais diretrizes devem ser exemplificativas e não procurar ser exaustivas, reconhecendo que o conteúdo é fundamentalmente importante. Os Estados devem também garantir que as empresas respeitam o direito das crianças à proteção contra a violência, que está subjacente às exigências de um processo justo e aos enquadramentos de monitorização e reparação.

---

[82] Veja, por exemplo, estudos sobre o Extremo Oriente: https://www.unicef-irc.org/publications/pdf/16.EAP.pdf.

[83] https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads

61. Existe a necessidade de uma supervisão ética e responsabilizadora dos processos decisórios baseados em algoritmos, que garanta que os Estados protegem as crianças de sistemas automatizados suscetíveis de interferir na respetiva liberdade de pensamento ou de ter impacto negativo no seu desenvolvimento, por exemplo algoritmos de recomendação que possam exacerbar ansiedades ou direcionar as crianças para perfilharem uma determinada visão do mundo.

C. Liberdade de pensamento, consciência e religião

62. O direito das crianças à liberdade de pensamento, consciência e religião necessita de ser protegido no ambiente digital contra manobras de manipulação ou interferência. As inferências sobre o estado íntimo das crianças retiradas a partir de dados pessoais podem ser nocivas e conduzir a resultados negativos ou discriminação contra as crianças. A definição de crianças-alvo e de perfis com base em dados pessoais pode levar à manipulação do estado íntimo das crianças. Assim, é necessário que os Estados introduzam regulamentação em matéria de proteção de dados para garantir a adequada proteção do "foro interno" das crianças[84].

As proteções de dados não se podem limitar à informação fornecida pelas crianças, mas sim incluir todos os dados recolhidos, inferidos, processados e transferidos acerca da criança. Como tal, constituem também uma oportunidade para definir normas e supervisionar os algoritmos e sistemas automatizados. Não devem ser feitas inferências acerca do estado mental das crianças que possam ser usadas contra elas.

63. Os Estados devem respeitar e proteger diferentes formas de convicção e expressão, não devendo as crianças ser penalizadas por partilharem dessas convicções. No ambiente digital, não devem ser feitas inferências acerca das convicções das crianças.

D. Liberdade de associação e de reunião pacífica

64. As crianças têm o direito, e manifestam largamente o interesse, de se envolverem em atividades políticas e sociais com outras pessoas, incluindo manifestações políticas, e em associações como grupos de jovens, clubes desportivos, grupos liderados por crianças e partidos políticos, bem como em trabalhar com organizações e movimentos de crianças e em associar-se e reunir-se informalmente através da família, amigos e redes sociais, dentro e fora do ambiente digital.

---

[84] https://undocs.org/A/HRC/28/66.

> "A era digital contemporânea proporciona uma plataforma e dá voz às minorias de um país…Através da tec[nologia] digital, podes manter viva a tua religião e a tua cultura."
>
> Paquistão, rapaz, 15[85]

65. Muitas atividades e organizações sociais, cívicas, políticas, religiosas e culturais funcionam parcial ou exclusivamente em ambiente digital e os Estados devem considerar a possibilidade de garantir o direito das crianças a participar nestas atividades, assegurando que a legislação se encontra igualmente alinhada com os meios digitais. Muitas crianças usam os meios digitais para organizar e coordenar as suas atividades cívicas, por exemplo a *Fridays for Future*[86], campanha mundial para protestar contra as alterações climáticas às sextas-feiras. Estas atividades, e todas as levadas a cabo pelas crianças defensoras de direitos humanos[87], deverão estar isentas de vigilância e castigo[88].

66. Os Estados devem reconhecer o potencial das tecnologias digitais para criar redes de crianças e dar a estas a possibilidade de fazer ouvir as suas vozes. As crianças têm vindo a utilizar esta tecnologia para apoiar os seus interesses e comunicar entre si sobre questões que consideram importantes. Por exemplo, o governo de Taiwan pediu aos jovens que indicassem as suas reivindicações prioritárias antes de um ato eleitoral[89]. Os Estados devem encorajar e, se possível, criar ambientes digitais seguros nos quais as crianças possam ser ouvidas.

E. Direito à privacidade

67. O direito das crianças à privacidade abrange a privacidade face ao Estado, às empresas, às organizações e a outras pessoas, incluindo pais e outras crianças.

O ambiente digital encoraja e sistematiza a revelação e partilha de informação. Esta informação pode ser fornecida pela criança, sua família ou pares e pode também ser fornecida por instituições e organizações com as quais a criança interaja, por exemplo a escola ou uma organização de jovens. Pode ainda ser recolhida e inferida (presumida) a partir da respetiva utilização digital, por

---

[85] *Our Rights in a Digital World*, p. 20.
[86] https://fridaysforfuture.org/.
[87] https://www.childrightsconnect.org/children-human-rights-defenders-2/.
[88] Por exemplo, uma jovem ativista Indiana foi acusada do crime de sedição pelo seu alegado papel na criação de um conjunto de ferramentas digitais para organizar protestos contra as novas leis agrícolas do país. https://www.aljazeera.com/news/2021/2/24/indian-climate-activist-gets-bail-in-sedition-case-over-farm-stir#:~:text=Disha%20Ravi%20was%20arrested%20in,violence%20during%20the%20farmers'%20protest.
[89] https://freedomreport.5rightsfoundation.com/a-young-democracy-is-a-strong-democracy-civil-rights-of-taiwans-children.

exemplo resultados de buscas, utilização de ferramentas para exercício físico, serviços de apoio ou redes sociais. No seu conjunto, esta informação oferece uma imagem muito poderosa dos interesses da criança, estado emocional e outras circunstâncias, o que pode comprometer o respetivo direito à privacidade. Muitas crianças quase não têm ideia até que ponto terceiros conhecem informação a seu respeito ou as formas como a mesma pode ser utilizada para tomar decisões sobre si.

68. Os dados recolhidos e processados em ambiente digital são muito abrangentes e, muito importante, a combinação de múltiplas fontes e tipos de dados pode revelar coisas acerca da criança que ela própria (e os seus pais) desconhecem, por exemplo a respetiva sexualidade, deficiência ou propensão para uma utilização excessiva. As consequências não intencionais da definição de perfis e recomendação de conteúdos podem revelar detalhes muito íntimos acerca das vidas das crianças. Ao longo dos anos, tem havido múltiplos relatos de "saída do armário através do algoritmo"[90]. Por exemplo, o destaque de conteúdos LGBTQ pela Netflix[91] ou a exibição de publicidade no Facebook sobre os serviços de pessoas que apoiam os jovens na sua "saída do armário"[92] em contas partilhadas ou ecrãs localizados em salas comuns.

A proteção de dados é amplamente reconhecida como uma ferramenta para proteger a autonomia e privacidade das crianças e salvaguardá-las contra a exploração. O primeiro instrumento autónomo com diretrizes para a proteção dos dados de crianças é o Código de Desenho Apropriado à Idade[93], do Reino Unido, que parte da exigência do RGPD de que as crianças beneficiem de medidas de proteção específicas. O Comissário para a Informação da Irlanda definiu também diretrizes fundamentais sobre a proteção dos dados das crianças[94] e outras jurisdições anunciaram a intenção de fazer algo semelhante.

Os Estados deverão assegurar-se de que a forma como os dados são recolhidos, processados e partilhados não tem um impacto negativo sobre as crianças nem viola os seus direitos à privacidade e à liberdade de pensamento.

69. No contexto do ambiente digital, a criança é extremamente vulnerável a violações da sua privacidade. Os Estados deverão enunciar e aplicar os princípios

---

[90] https://5rightsfoundation.com/in-action/lgbtq-children-online-why-digital-platforms-must-design-with-them-in-mind.html.
[91] https://www.menshealth.com/sex-women/a29712873/netflix-algorithm-nearly-outed-gay-teenager/
[92] https://www.intomore.com/you/facebook-ads-outed-me/.
[93] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.
[94] https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf.

da proteção de dados, minimização de dados e direito da criança à privacidade em ambiente digital. O direito à privacidade compreende a privacidade relativamente aos governos, às empresas e a outros utilizadores do ambiente digital, incluindo pais.

70. Os Estados têm a obrigação de estabelecer enquadramentos legislativos e industriais para proteger a privacidade das crianças no mundo digital. Tais enquadramentos devem ser sistémicos por natureza e transparentes, responsabilizadores e realistas. Devem também ser sujeitos a revisão e atualizados regularmente.

Tem havido consideráveis tensões entre aqueles que protegem a privacidade dos adultos, em particular relativamente ao Estado[95], e o abuso dessa privacidade pelos que difundem e/ou consomem materiais configurando abuso sexual de crianças[96]. Contudo, a privacidade oferecida aos utilizadores, incluindo crianças, pelas empresas privadas não pode proteger aqueles que consomem ou cometem abusos sexuais de crianças nem interferir nos sistemas de deteção de materiais que configurem tais abusos. Os Estados deverão, não só investir em medidas para detetar e eliminar materiais abusivos, mas também fazer mais para acabar com o carregamento e a difusão de materiais que configurem abuso sexual de crianças[97] ou com as oportunidades para que predadores sexuais entrem em contacto com crianças.

Mais concretamente, os aspetos do desenho dos sistemas que encorajem a criação ou difusão de materiais que configurem abuso sexual de crianças devem ser identificados através da avaliação do risco de impacto nas crianças; por exemplo, a apresentação de adultos estranhos a crianças, a permissão de serviços de mensagens diretas de estranhos a crianças ou a exibição pública dos perfis de crianças a todos os utilizadores, devem ser entendidos pelos Estados como aspetos que colocam riscos desnecessários às crianças[98]. De igual modo, embora muitos sistemas de deteção sejam atualmente desadequados, não devem ser desmantelados até que as empresas consigam proporcionar sistemas de igual ou melhor qualidade sob o ponto de vista de observadores independentes. As empresas que comprovadamente difundam ou fomentem continuamente o abuso sexual de crianças devem ser sujeitas a vigilância e controlos legais rigorosos.

71. Embora o consentimento da criança ou seus pais seja e continue a ser uma consideração no domínio da proteção de dados, não deve ser usado para prejudicar mecanismos de proteção de dados justos e respeitadores dos direitos. Qualquer consentimento deverá ser informado, significativo e prestado pela

---

[95] https://www.openrightsgroup.org/blog/online-harms-encryption-under-attack/.
[96] https://www.theguardian.com/society/2020/dec/08/encrypted-messaging-putting-children-at-risk-of-abuse-says-watchdog.
[97] http://luxembourgguidelines.org/.
[98] http://dipbt.bundestag.de/extrakt/ba/WP19/2685/268540.html.

pessoa cujos dados estejam a ser processados, com implicações específicas para utilizações por terceiros dos dados das crianças. Não é adequado utilizar dados fornecidos para determinada finalidade para uma série de outros fins que podem ser pouco claros, indesejados ou desconhecidos pela criança. Os Estados devem supervisionar a aplicação de políticas de utilização de dados que sejam claras, concisas, acessíveis e fáceis de compreender e que não possam ser modificadas arbitrariamente sem notificar ativamente os utilizadores.

72. Os Estados devem legislar para garantir que as crianças têm o direito de retirar, corrigir e eliminar os seus dados pessoais de formas que sejam fáceis de aceder e de compreender, e que o processamento de dados não vai além das utilizações para as quais as crianças (ou respetivos pais em seu nome) possam ter consentido. Em todos os casos, a criança deve ter a possibilidade de retirar o consentimento a todo o tempo, com a mesma facilidade com que o mesmo foi inicialmente prestado, nomeadamente não tendo de provar a respetiva idade para eliminar uma imagem, caso não lhe tenha sido pedida prova dessa idade e exigido o mesmo nível de garantia no momento em que foi criada.

73. Os Estados devem limitar o período durante o qual os dados podem ser conservados pelas autoridades públicas ou sujeitos privados e devem também exigir a eliminação dos dados logo que estes deixem de ser necessários. Os organismos públicos e empresas privadas devem ser sujeitos a quadros normativos transparentes, responsabilizadores e regularmente revistos de limitação dos objetivos.

As disposições relativas à transferência de dados de um local para outro deverão abranger divergências de consentimento entre pais/cuidadores e crianças e prosseguir o interesse superior da criança. O consentimento dos pais/cuidadores não deve sobrepor-se automaticamente ao das crianças, em particular adolescentes, ou vice-versa.

74. A proteção dos dados existe para benefício das crianças e da sua privacidade. Deverá ser concebida em observância de todos os seus direitos, por exemplo o direito à informação.

Os dados são, cada vez mais, recolhidos em todos os tipos de ambientes e a partir de muitos dispositivos conectados, incluindo espaços públicos e equipamentos domésticos, brinquedos ou dispositivos de uso pessoal. Espera-se que o mercado global de dispositivos conectados cresça de 14.3 mil milhões de dólares em 2020 para 40.3 mil milhões em 2025[99]. A vigilância (especialmente se possível na ausência de consentimento) constitui uma violação da privacidade e dos direitos

[99] https://www.marketsandmarkets.com/Market-Reports/connected-device-analytics-market-249243332.html#:~:text=%5B345%20Pages%20Report%5D%20The%20global,23.0%25%20during%20the%20forecast%20period.

da criança. As crianças podem não ter consciência de que estão a ser vigiadas enquanto se encontram em espaços públicos, usam vestuário detetável remotamente ou brincam com determinados brinquedos. Assim, os Estados necessitam de garantir que estão em vigor medidas robustas de proteção de dados para salvaguardar as crianças de tal recolha intrusiva dos seus dados sem o respetivo conhecimento ou consentimento.

75. A vigilância digital de crianças pode resultar no controlo constante das mesmas dentro e fora das redes, por exemplo em ambientes educativos e assistenciais. Por exemplo, a pandemia Covid-19 fez aumentar o número de estabelecimentos de ensino que recorrem a *software* de monitorização remota dos testes para detetar se os alunos estão a copiar ou envolvidos em outros tipos de conduta imprópria. Muitos destes serviços usam formas de vigilância altamente invasivas, como o armazenamento dos *templates* biométricos dos traços distintivos das crianças[100], o seguimento e monitorização dos movimentos dos olhos e das cabeças dos estudantes e o armazenamento dos registos áudio dos ambientes das crianças. A vigilância de crianças, juntamente com qualquer processamento automatizado de dados pessoais que lhe esteja associado, particularmente se forem feitas inferências acerca do estado emocional ou mental da criança, deve respeitar o direito da mesma à privacidade. Tais invasões da privacidade da criança não devem ser levadas a cabo de forma rotineira, indiscriminada ou sem o conhecimento da criança ou, no caso de crianças muito jovens, sem o conhecimento dos respetivos pais ou cuidadores, devendo tais pessoas ter, sempre que possível, o direito de se opor a tal vigilância.

76. As preocupações em torno dos perigos do mundo digital resultaram num mercado cada vez maior de ferramentas de vigilância que monitorizam os dispositivos das crianças, detetam a sua localização ou revelam a terceiros, sobretudo pais ou educadores, as suas atividades nas redes. Estas ferramentas devem ser usadas com moderação e unicamente para finalidades bem definidas, já que podem dar uma falsa sensação de segurança, interferir no desenvolvimento da criança ao dar-lhe a sensação de que nunca está sozinha e inibir o desenvolvimento de competências sociais e críticas que apoiem a sua própria segurança e autonomia. Podem também criar tensões entre os pais e as crianças mais velhas, que formam opiniões e adquirem experiências por si mesmas.

77. O anonimato é uma característica muito contestada do ambiente digital. Pode oferecer privacidade às crianças que, de outro modo, seriam impedidas de falar ou punidas por fazê-lo, mas pode também proteger aqueles que as atacam, maltratam, promovem o ódio ou difundem falsas informações. Os Estados devem encorajar uma abordagem de segurança e privacidade desde a fase de desenho. Ao considerar o anonimato como parte de um equilíbrio entre a segurança e a

[100] https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education.

privacidade, é possível desenvolver abordagens mais matizadas e adaptadas ao ambiente de cada um. Por exemplo, a identidade dos titulares das contas pode ser verificada junto dos serviços mesmo que a identidade do utilizador não seja tornada pública, permitindo que as empresas contactem ou bloqueiem os que violam as regras da comunidade.

Algumas crianças usam *avatars* ou nomes de utilizador na Internet para proteger a sua identidade e tais práticas podem ser importantes para proteger a respetiva privacidade. Para as crianças que sejam atraídas por pessoas do mesmo sexo, intersexo ou com diversidade de géneros, a privacidade e o anonimato nas redes podem também proporcionar proteção contra a perseguição enquanto exploram as suas identidades.

78. Os Estados deverão assegurar-se de que as crianças que acedem a aconselhamento e outro apoio em matéria de saúde o podem fazer independentemente da respetiva idade e sem que seja necessário o consentimento ou a autorização de um adulto, incluindo os respetivos pais. Os Estados devem garantir que os serviços de saúde e aconselhamento aos quais as crianças têm acesso cumprem requisitos exigentes em matéria de privacidade, confidencialidade e proteção das crianças. Uma criança não pode sofrer uma violação dos seus restantes direitos em resultado da procura de aconselhamento ou ajuda.

F. Registo dos nascimentos e direito à identidade

79. Para muitas crianças, o acesso a documentos de identidade é necessário para lhes permitir o acesso a serviços públicos. As tecnologias digitais oferecem importantes oportunidades para aperfeiçoar o registo dos nascimentos e, assim, ampliar o acesso aos serviços, particularmente para as crianças que possam viver em comunidades isoladas, em itinerância ou separadas da família.

Os Estados devem promover mecanismos de registo dos nascimentos e garantir a ampla difusão de informação sobre a forma de acesso aos mesmos. Tais mecanismos deverão ser respeitadores da privacidade e não utilizados para discriminar, punir ou violar de qualquer forma os demais direitos das crianças.

VII. Violência contra crianças

80. O aumento do tempo passado em plataformas virtuais pode deixar as crianças mais vulneráveis à exploração e ao aliciamento sexual nas redes. Tem havido um aumento constante do tempo passado à frente dos ecrãs o que, juntamente com a falta de contactos cara a cara com amigos e parceiros, pode levar a que a criança se exponha a mais riscos, por exemplo com o envio de imagens sexualizadas. A

diminuição das oportunidades para encontros cara a cara e uma maior dependência do tempo passado nas redes a usar produtos e serviços desenhados sobretudo a pensar nos adultos podem expor as crianças a conteúdos potencialmente nocivos e violentos, bem como a um maior risco de ciberbullying.

> "A internet permite discussões mais alargadas sobre a violência existente, mas aumenta a possibilidade de violência, como o ciberbullying."
>
> Brasil, rapariga, 15[101]

Além disso, o ambiente digital oferece novas vias para que os agressores sexuais aliciem crianças para fins sexuais, participem em abusos sexuais de crianças na Internet através de transmissões ao vivo, distribuam materiais configurando abuso sexual de crianças e cometam extorsão sexual contra crianças, nomeadamente acedendo ilegal e secretamente a câmaras, microfones ou ficheiros pessoais em computadores ou dispositivos móveis.

81. O crescimento do abuso e exploração sexual de crianças na Internet é uma questão que preocupa consideravelmente todas as agências que trabalham com crianças. Existe já um número importante de documentos que fornecem orientações sobre as medidas necessárias para responder a tal abuso e exploração, nomeadamente:

- Comentário Geral n.º 16 (2013), sobre as obrigações do Estado relativamente ao impacto do setor empresarial nos direitos da criança[102]
- Comentário Geral n.º 13 (2011), sobre o direito da criança a não ser sujeita a qualquer forma de violência[103]
- Comentário Geral n.º 14 (2013), sobre o direito da criança a que o seu interesse superior seja primacialmente tido em conta (artigo 3.º, n.º 1)[104]
- Relatório do Representante Especial do Secretário-Geral sobre a Questão dos Direitos Humanos e as Multinacionais e Outras Empresas Comerciais (2008)[105]
- Princípios Orientadores sobre Empresas e Direitos Humanos: Implementando o Enquadramento das Nações Unidas em matéria de "Proteger, Respeitar e Reparar" (2011)[106]
- Relatório do Grupo de Trabalho da Revisão Periódica Universal – Ruanda (2011)[107]

---

[101] *Our Rights in a Digital World*, p. 36.
[102] https://undocs.org/CRC/C/GC/16.
[103] https://undocs.org/CRC/C/GC/13.
[104] https://undocs.org/CRC/C/GC/14.
[105] https://undocs.org/A/HRC/8/5.
[106] https://undocs.org/A/HRC/17/31.
[107] https://undocs.org/A/HRC/17/4.

- Relatório do Comité dos Direitos da Criança relativo ao Dia de Debate Geral sobre meios digitais e direitos da criança, de 2014[108]
- Diretrizes sobre a aplicação do Protocolo Facultativo à Convenção sobre os Direitos da Criança relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil (2019)[109]

A violência contra as crianças não se restringe à violência praticada por estranhos nem à violência sexual. Muitas crianças são violadas por pessoas que conhecem, incluindo familiares, e muitas crianças sofrem uma ou mais formas de violência, incluindo as que são promovidas por conteúdos presentes na Internet, como a automutilação, o suicídio ou os comportamentos alimentares extremos.

Devem ser introduzidas medidas robustas de prevenção de todas as formas de violência e as empresas digitais devem dispor de formas eficazes e transparentes de moderação de conteúdos, denúncia e resposta nos ambientes onde a violência tem lugar. É necessário que a vítima que procura ajuda seja protegida do confronto com imagens de abuso de crianças ou plataformas de agressores. A utilização de tecnologias de segurança deve ser encorajada de uma forma orientada que bloqueie os riscos e ilegalidades mais graves mas não comprometa a capacidade da criança de aceder a informação e apoio.

Nem todas as crianças reagem da mesma forma às mesmas circunstâncias e muitos atos de violência de pequena escala conduzem a atos mais extremos. Os Estados devem considerar todos os atos de violência contra crianças, incluindo o fomento dos atos de violência, como uma violação do direito da criança à proteção.

82. Os multifacetados e complexos desafios resultantes da violência contra crianças por meios digitais exigem que os Estados estabeleçam mecanismos legais, institucionais e práticos holísticos e atualizados de prevenção, tratamento, assistência, apoio e proteção, incluindo unidades policiais especiais, agentes do sistema de justiça especializados, bem equipados e treinados, juntamente com mecanismos de queixa e investigação adaptados a crianças e linhas de apoio acessíveis.

O sistema educativo, incluindo a educação não formal, tem um papel fundamental no combate à violência por meios digitais, violência entre pares, *bullying* e assédio nas escolas. Os Estados devem desenvolver programas de ensino específicos, formar e equipar os professores e outro pessoal docente com ferramentas pedagógicas, estabelecer pontos focais nas escolas para a denúncia de tais incidentes e mecanismos de investigação, em coordenação com o sistema social, a polícia e o sistema de justiça. Os professores não devem ficar sem recursos e os

[108] https://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf.
[109] https://undocs.org/CRC/C/156.

programas de formação devem ser abrangentes e isentos de interesses comerciais.

As empresas comerciais devem cumprir a sua responsabilidade de proteger efetivamente as crianças contra todas as formas de violência mediante a reforma das suas práticas empresariais, o desenvolvimento de ferramentas técnicas, o aproveitamento dos mais recentes conhecimentos e inovações disponíveis e a adoção de uma abordagem proactiva e preventiva ao desenho dos sistemas. Por exemplo, a ferramenta Photo DNA está disponível gratuitamente, mas muitas empresas ainda não a utilizam[110]. Na ausência de medidas rápidas de prevenção, foram utilizadas plataformas para difundir o ódio e a violência, por exemplo no Myanmar[111]. Os Estados devem desenvolver abordagens reguladoras que exijam que as empresas tomem todas as providências técnicas e processuais razoáveis e proporcionais para combater os comportamentos criminosos e nocivos dirigidos contra crianças e relacionados com o ambiente digital. Tais exigências devem ser sujeitas a salvaguardas jurídicas que protejam outros direitos fundamentais, como o direito à privacidade e a liberdade de expressão.

83. O ambiente digital abre novos caminhos que permitem que grupos criminosos, incluindo gangs, procurem e trafiquem crianças para finalidades criminosas, incluindo a distribuição de drogas. Os serviços das redes sociais, como o WhatsApp, têm vindo a ser massivamente utilizados como canal para o recrutamento de crianças[112]. Sistemas de geolocalização, como o "Find My Friends", oferecidos por diferentes smartphones, são utilizados para monitorizar e localizar os movimentos das crianças quando transportam e vendem drogas no Reino Unido, sendo as crianças por vezes forçadas a transmitir os seus movimentos ao vivo, 24 horas por dia[113].

Os Estados devem garantir que a legislação de combate ao tráfico proíbe o recrutamento de crianças por grupos criminosos e que as crianças delinquentes são tratadas como vítimas ou, se julgadas, o são em conformidade com sistemas de justiça adaptados a crianças. Os Estados são encorajados a incorporar plenamente o princípio da não punição, conforme desenvolvido pelo Grupo de Coordenação Interagências das Nações Unidas contra o Tráfico de Pessoas

---

[110] https://www.iicsa.org.uk/publications/investigation/internet/part-c-indecent-images-children/c2-detection-images.

[111] https://resourcecentre.savethechildren.net/node/16212/pdf/mobile_myanmar_2019_2019-11-06.pdf.

[112] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf.

[113] https://www.theguardian.com/global-development/2019/feb/05/county-lines-drug-gangs-blackmailing-tracking-children-social-media.

(ICAT)[114], a fim de assegurar uma aplicação consistente e baseada nos direitos humanos deste princípio, o qual estabelece que as pessoas traficadas não serão sujeitas a captura, imputação, detenção ou acusação, nem penalizadas ou punidas de outra forma, por condutas ilegais por si praticadas em consequência direta do tráfico.

VIII. Ambiente familiar e cuidados alternativos

84. Os pais e cuidadores necessitam de apoio para compreender de que formas as tecnologias e empresas digitais influenciam as crianças. Isto inclui as formas como as crianças podem realizar os respetivos direitos utilizando tecnologia digital, bem como as formas como podem ficar em risco ou sofrer danos.

Os sistemas digitais devem ser desenhados em reconhecimento do facto de que muitas crianças não têm o apoio de pais com empenho, literacia ou aptidões ao nível das tecnologias digitais, pelo que os sistemas devem ser respeitadores da privacidade, seguros, apropriados e capazes de apoiar as crianças desde a fase de desenho.

85. Os Estados devem prestar um apoio realista aos pais reconhecendo as pressões temporais, emocionais, cognitivas e de literacia nos contextos domésticos. Os pais têm frequentemente as suas próprias questões com a tecnologia e as tecnologias emocionais, empáticas e afetivas destinadas a crianças são também suscetíveis de afetar os pais. Isto pode, por vezes, ter um profundo impacto no seu papel enquanto pais e no seio das dinâmicas familiares. Por exemplo, as crianças reportam que os pais estão frequentemente distraídos com os seus *smartphones* ou que encontram materiais que as perturbam nos equipamentos que partilham com os pais.

É necessário que os Estados prestem particular atenção à regulamentação dos produtos e serviços sobre os quais seja pouco provável que os pais estejam bem informados, por exemplo de recolha de dados e utilização de tecnologias de persuasão em cascata.

As crianças utilizam os produtos e serviços digitais desde idades cada vez mais precoces. Os pais podem desconhecer a natureza e o impacto de muitos serviços e abordar a utilização pelas crianças tendo unicamente em conta o tempo passado nas redes, em vez de adotar uma abordagem que responda à natureza do produto e serviço e às capacidades em evolução e circunstâncias da criança.

Se as crianças forem excessivamente limitadas, tal influenciará a sua disponibilidade para reportar experiências negativas, encorajando-as mesmo a

[114] https://www.unodc.org/documents/human-trafficking/ICAT/19-10800_ICAT_Issue_Brief_8_Ebook.pdf

evadir-se ao controlo ou a enganar os pais. Os Estados devem apoiar os pais fornecendo-lhes informação sofisticada, isenta de influências comerciais, que os ajude a compreender os múltiplos riscos e oportunidades que as crianças enfrentam. Técnicas de parentalidade positiva, incluindo as que possibilitam e apoiam uma utilização responsável da tecnologia pelas crianças, são fundamentais[115]. A informação e educação complementam, não substituindo, uma avaliação sistémica do risco e estratégias de mitigação destinadas a garantir a segurança do ambiente digital desde a fase de desenho.

86. Pais e crianças manifestam o desejo de que os primeiros compreendam melhor o ambiente digital e disponham das aptidões necessárias para interagir com ele. O aconselhamento deve ser prestado de uma forma que reconheça que as famílias têm posições culturais e pessoais muito diferentes e que, à medida que crescem, as crianças terão as suas próprias opiniões independentes.

Os Estados devem prestar um aconselhamento que encoraje o acesso das crianças e a utilização segura do ambiente digital para muitas atividades diferentes. Os pais devem ser apoiados para que consigam desenvolver aptidões e conhecimentos em matéria de tecnologias digitais, incluindo a forma de apoiar a utilização positiva, pelos seus filhos, de uma ampla variedade de produtos e serviços respeitadores dos direitos.

87. Os Estados podem ter de fazer intervenções específicas para garantir que as crianças separadas das suas famílias dispõem de acesso a tecnologias digitais para se manterem em contacto com as mesmas. Isto pode incluir crianças cujos pais ou cuidadores trabalhem no estrangeiro ou em outras partes do país, cujos pais estejam presos, que vivam com outros familiares ou que estejam elas próprias sob cuidados alternativos.

Tal acesso pode exigir que sejam considerados muitos fatores diferentes, como o investimento em infraestruturas, eletricidade, acesso a equipamentos, dados ou as circunstâncias e permissões necessárias para estabelecer contacto.

88. O contacto deverá ser feito no interesse superior da criança. Por exemplo, não pode ser um meio que permita a pais abusadores retomar o contacto com os filhos de quem tenham sido separados. Pode ser necessária a supervisão de tais comunicações pelos serviços de segurança social, pelo que os respetivos profissionais deverão receber uma formação que lhes permita compreender os riscos. Por exemplo, as tecnologias digitais têm funcionalidades que permitem detetar a localização da criança ou transmitir informação pessoal que torna os seus interesses ou hábitos visíveis para muitos milhões de utilizadores. Os princípios[116] de segurança desde a fase de desenho devem ter em conta a

[115] https://www.unicef.org/parenting/.
[116] https://www.esafety.gov.au/about-us/safety-by-design.

vulnerabilidade das crianças face aos adultos, incluindo familiares, que representem um perigo.

IX. Crianças com deficiência

89. O ambiente digital oferece um mundo de oportunidades para as crianças com deficiência. Por exemplo, para as crianças que necessitem de apoio na locomoção, os sistemas visuais de localização digital podem ajudá-las a descobrir se uma área é ou não acessível a cadeiras de rodas[117]. O Google Maps, por exemplo, recolhe informação sobre a acessibilidade de cadeiras de rodas a mais de 15 milhões de locais em todo o mundo[118]. Contudo, para que as crianças com deficiência beneficiem destas oportunidades, é importante que os Estados identifiquem quaisquer barreiras que possam enfrentar no acesso à tecnologia digital, por exemplo devido ao desenho do *software*, inacessibilidade de páginas, serviços e aplicações, inexistência de adaptações, ou dificuldades financeiras, e tomem todas as providências necessárias para responder a essas barreiras e eliminá-las.

90. Os Estados deverão considerar e agir com base nos direitos das crianças com deficiência em matéria de acesso ao ambiente digital. As estratégias de acessibilidade, a disponibilidade de tecnologias de assistência e a padronização de um ambiente digital acessível oferecem importantes oportunidades para melhorar o acesso. Os Estados devem garantir o acesso a uma ampla variedade de tecnologias de assistência economicamente acessíveis e assegurar-se de que a disponibilização de serviços digitais não restringe o acesso das crianças com deficiência, especialmente das que vivem em situação de pobreza, a interações físicas e virtuais.

Os Estados devem proporcionar orientações e recursos ao pessoal das escolas e outras instituições competentes a fim de que o mesmo disponha de formação suficiente para conseguir repensar as dinâmicas e metodologias escolares sempre que as necessidades das crianças com deficiência não estejam a ser satisfeitas. Além disso, os Estados devem garantir a disponibilização dos conteúdos da educação formal obrigatória em formato virtual, através de materiais e tecnologias adequados às necessidades especiais das crianças com deficiência.

91. Ao criarem sistemas digitais que sejam acessíveis a crianças com diferentes necessidades, os Estados devem interagir com as próprias crianças e encorajar as empresas a fazer o mesmo. As crianças têm opiniões acerca da forma como o mundo digital poderia estar mais bem concebido para ser por si utilizado.

---

117 https://publications.parliament.uk/pa/cm201719/cmselect/cmpetitions/759/75905.htm#footnote-117.

118 https://blog.google/products/maps/wheelchair-accessible-places-google-maps/.

> "[Necessitamos de] termos e condições adaptados aos jovens com um resumo dos pontos mais relevantes."
>
> Alemanha, rapaz, 17[119]

92. Embora o ambiente digital ofereça oportunidades específicas para as crianças com deficiência, estas mesmas crianças enfrentam frequentemente maiores riscos[120], incluindo um risco acrescido de abuso sexual de crianças. Os Estados devem garantir que os riscos acrescidos enfrentados pelas crianças com deficiência são abrangidos pelas avaliações de risco infantil e programas de segurança, desde a fase de desenho. A informação destinada a crianças deve ser fornecida em formatos acessíveis.

Os Estados devem apoiar o desenvolvimento de organizações lideradas por crianças e iniciativas de crianças com deficiência e a sua participação ativa através do ambiente digital, bem como ajudar os adultos a facilitar tais iniciativas. Por exemplo, o *Council for Disabled Children*[121] apoia a participação dos respetivos membros em iniciativas de defesa por meios digitais[122].

X. Saúde e bem-estar

93. Devem ser desenvolvidos produtos e serviços digitais para melhorar o acesso das crianças a serviços de saúde e bem-estar, nomeadamente em tempos de emergência pública ou de crise. Por exemplo, em 2019-2020, muitas organizações desenvolveram recursos informativos sobre a Covid-19 para as crianças[123] e para que os adultos falassem com as crianças[124].

94. As crianças utilizam serviços digitais para aceder a informação sobre saúde, incluindo informação sobre saúde sexual e reprodutiva. Os Estados devem garantir que os serviços que fornecem tal informação o fazem de uma forma que seja de alta qualidade e não comprometa a privacidade ou confidencialidade da criança. Em particular, devem estar em vigor sistemas de proteção de dados para os serviços que oferecem aconselhamento a crianças em matéria de saúde. Por exemplo, ao abrigo do Regulamento Geral sobre a Proteção de Dados (RGPD) da UE, a ONG *Privacy International* pediu a cinco aplicações diferentes sobre

---

[119] *Our Rights in a Digital World*, p. 15.
[120] https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.
[121] https://councilfordisabledchildren.org.uk/our-work/participation.
[122] https://www.un.org/development/desa/disabilities/.
[123] https://www.unicef.org/romania/covid-19-information-children-adolescents-parents-and-professionals.
[124] https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/talking-with-children.html.

menstruação que partilhassem a informação detida sobre certas utilizadoras[125]. Estas aplicações tinham a sua base na Alemanha, Índia, Ilhas Virgens Britânicas e EUA. As investigações concluíram que, das cinco aplicações inquiridas, só duas responderam aos pedidos de informação ao abrigo do Direito de Acesso do Titular dos Dados (DATD). Ambas alojavam nos seus servidores múltiplas páginas com dados sensíveis, incluindo dados sobre a vida e hábitos sexuais das utilizadoras e medicação tomada. Alguns destes dados foram também partilhados com terceiros.

Os profissionais que trabalham nos serviços de saúde e bem-estar (por exemplo, profissionais de clínicas de ginecologia e obstetrícia) desempenham um papel fundamental para ajudar as crianças, incluindo jovens, e suas famílias a cuidar do seu bem-estar em meio digital.

95. As tecnologias digitais devem melhorar o acesso da criança a disposições em matéria de saúde. Uma criança não deve sofrer violações dos seus outros direitos, por exemplo do seu direito à privacidade ou a que as suas opiniões sobre questões que a afetem sejam ouvidas.

> "Pesquisei sobre doença mental, depressão e ansiedade, por curiosidade, já que ninguém falava sobre isso e eu queria saber mais."
>
> Brasil, rapaz jovem, idade desconhecida[126]

Os Estados devem assegurar-se de que a introdução de produtos e serviços digitais no setor da saúde não discrimina certos grupos de crianças ao negar-lhes acesso a cuidados de saúde presenciais ou ao prestar um serviço de mais baixa qualidade por ser prestado através da Internet.

96. Existem riscos de saúde associados à utilização de certos produtos e serviços e o risco de difusão de informação nociva sobre questões de saúde pelos serviços digitais, por exemplo o aumento dos comportamentos autodestrutivos em resultado da sua cobertura generalizada pelas redes sociais[127] ou a prevalência de informação enganosa e desinformação sobre as vacinas[128].

Os Estados devem antecipar as necessidades das crianças encorajando a que os regimes de segurança desde a fase de desenho constituam a regra e pondo em prática enquadramentos jurídicos e de regulação suficientes para garantir a participação segura das crianças no ambiente digital. Por exemplo, como parte

---

[125] https://privacyinternational.org/long-read/4316/we-asked-five-menstruation-apps-our-data-and-here-what-we-found.
[126] *Our Rights in a Digital World*, p. 38.
[127] Arendt, F., Scherr, S., & Romer, D. (2019) *Effects of exposure to self-harm on social media: Evidence from a two-wave panel study among young adults*. https://doi.org/10.1177/1461444819850106.
[128] Buri, T. (2019) Vaccine Misinformation and social media. https://doi.org/10.1016/S2589-7500(19)30136-0.

integrante da próxima Lei sobre Segurança na Internet, o governo do Reino Unido estabelecerá um novo dever legal de cuidado, exigindo aos serviços que tenham antecipadamente em conta a segurança dos seus utilizadores[129].

97. Os serviços e produtos digitais podem ser utilizados para encorajar comportamentos saudáveis, exercício, contacto com outras pessoas, ativismo cívico e aprendizagem. Estes fatores devem ser encorajados, mas não à custa dos demais direitos da criança. Os Estados devem adotar regulamentação que impeça que as crianças se tornem alvos de produtos pouco saudáveis ou impróprios para a idade e as crianças devem beneficiar das mesmas proteções dentro e fora do mundo digital. Por exemplo, incorporando em disposições regulamentares as Diretrizes da Organização Mundial de Saúde sobre a Publicidade a Alimentos[130].

98. As orientações dadas a pais, crianças e educadores devem encorajar uma utilização produtiva e prazenteira das tecnologias digitais, reconhecendo simultaneamente que o desenvolvimento infantil exige um equilíbrio entre as várias atividades. O mundo digital está concebido para conseguir a máxima atenção, interação e empenho constante – as crianças precisam de tempo dentro e fora das redes e os Estados devem deixar claro, nas suas orientações, que as crianças têm o direito de descansar, que é fundamental para o respetivo desenvolvimento.

XI. Educação, lazer e atividades culturais

A. Direito à educação

99. A educação tradicional ministrada por meios digitais oferece perspetivas de maior acesso a uma educação de qualidade e atividades pedagógicas associadas. Cada vez mais, a literacia digital constitui uma aptidão essencial e representa uma extensão fundamental do direito à educação no mundo contemporâneo, exigindo que os Estados e as instituições educativas e culturais tomem medidas adequadas para o desenvolvimento de competências digitais a fim de melhorar a educação e a participação das crianças e adolescentes no ambiente digital[131].

Para a realização dos direitos das crianças relacionados com a informação, é necessário acesso a recursos digitais de qualidade que apoiem a aprendizagem, juntamente com a aquisição das competências digitais necessárias para

---

[129] https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.
[130] https://www.who.int/dietphysicalactivity/marketing-food-to-children/en/.
[131] https://en.unesco.org/themes/media-and-information-literacy , https://www.unicef.org/globalinsight/media/1271/file/%20UNICEF-Global-Insight-digital-literacy-scoping-paper-2020.pdf.

desenvolver a “personalidade, os talentos e as capacidades mentais e físicas” das crianças e adolescentes em prol de uma vida responsável numa sociedade livre.

100. As instituições educativas e culturais, como arquivos, bibliotecas e museus, podem usar tecnologias digitais para ajudar as crianças a interagir com as suas próprias práticas criativas e culturais e a aprender com as dos demais, através dos meios da educação global.

101. Todas as escolas necessitam de dispor de uma infraestrutura tecnológica adequada que permita a cada criança beneficiar plenamente do ambiente digital e para tal é necessário o apoio de pessoal docente com a devida formação e programas de qualidade.

Os Estados devem fazer esforços deliberados para combater as disparidades digitais sempre que trabalham em prol da realização do direito à educação. À medida que o ensino à distância vai sendo incluído na educação, é necessário que os Estados tenham em conta as crianças em diferentes ambientes e situações. As atividades à distância ou outras realizadas por meios informáticos não devem criar ónus ou desigualdades acrescidas às crianças que não disponham de acesso aos meios digitais, aptidões e apoio para o efeito. Os Estados devem garantir a introdução de adaptações para as crianças com deficiência, nomeadamente tornando acessíveis conteúdos prontos com recurso a legendagem e descrição verbal de conteúdos visuais, permitindo adaptações adicionais como a utilização de linguagem gestual e simplificação linguística, tornando acessível a aprendizagem digital, em conformidade com as necessidades do aluno, e adotando princípios de adaptação universal.

Para fomentar um ambiente educativo rico, os Estados devem assegurar-se de que as garantias em matéria de propriedade intelectual preveem exceções adequadas para os materiais utilizados para fins pedagógicos.

102. Para as crianças que frequentam a escola (ou o jardim de infância, a universidade ou outras instituições educativas), as tecnologias pedagógicas digitais podem ajudar as interações entre professor e aluno e dos alunos entre si. Para as crianças que não se encontrem fisicamente presentes na escola, vivam em áreas remotas ou estejam em situações de desvantagem ou vulnerabilidade, as tecnologias pedagógicas digitais podem permitir a implementação de programas de ensino à distância ou em mobilidade.

Os Estados devem criar um ambiente digital suscetível de garantir que as crianças continuam a ter acesso à educação sem interrupção em situações de emergência, desastre natural e epidemia (como a pandemia de Covid-19 que o mundo enfrenta atualmente); e respeitar as necessidades das crianças e suas famílias neste contexto. Por exemplo, durante a pandemia de Covid-19, a emissora pública do Bangladesh emitiu aulas gravadas através dos seus canais. A decisão de utilizar a televisão e a rádio para as crianças sem dispositivos ligados à internet ou acesso a

banda larga demonstrou ser capaz de chegar a uma maior percentagem de crianças.[132]

Os Estados devem garantir e proporcionar às crianças que não possam frequentar presencialmente a escola acesso a recursos de conectividade (por exemplo, internet, computador e *tablets*) que lhes permitam receber educação em ambiente digital. Além disso, os Estados devem implementar um plano, na máxima medida dos seus recursos disponíveis, para garantir um acesso justo a estes recursos (tanto dentro como fora da escola) de todas as crianças que frequentem a escola presencialmente.

As responsabilidades dos Estados deverão garantir que as escolas dispõem de recursos suficientes para proporcionar aos pais orientações sobre aprendizagem em casa e ambientes educativos através de meios digitais. Tal deverá também incluir orientações sobre proteção contra os riscos associados à utilização das tecnologias digitais.

103. As normas aplicáveis à tecnologia digital para fins pedagógicos devem garantir que as utilizações destas tecnologias salvaguardam os direitos da criança e não expõem as crianças a violência, discriminação, utilização abusiva de dados pessoais, exploração comercial ou outros atentados aos seus direitos, incluindo a utilização de tecnologia digital para rastrear a atividade da criança e revelá-la aos seus pais sem o conhecimento ou consentimento da criança.[133]

104. É fundamental que a educação em matéria de literacia digital eduque as crianças acerca do desenho e finalidade do mundo digital e as faça compreender os direitos da criança, incluindo a respetiva aplicação no ambiente digital. Uma educação que aborde estas áreas fundamentais deve ser desenhada em conjunto com as crianças e peritos e disponibilizada formalmente às crianças através dos ambientes educativos.

A introdução da educação em matéria de literacia digital deve começar na primeira infância ou logo que as crianças comecem a utilizar a tecnologia. Os Estados devem apoiar as creches e jardins-de-infância para que habilitem as crianças com as aptidões e os conhecimentos necessários para se manterem seguras nas redes e interagirem de forma proveitosa com o ambiente digital.

---

[132] https://www.bbc.co.uk/news/world-south-asia-54009306

[133] Por exemplo, a polícia poderá aceder aos dados recolhidos pela aplicação de localização de contactos *Trace Together*, de Singapura (que é utilizada por quase 80% dos 5.7 milhões de residentes no país), para utilização em inquéritos criminais. Isto contraria a política de privacidade inicialmente definida quando o governo lançou esta aplicação em março de 2020, depois de dizer que a participação na localização de contactos é obrigatória. https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid/

A educação deve incluir uma componente crítica e de literacia informativa, para apoiar a busca e avaliação de informação fidedigna, incluindo informação em matéria de saúde e informação sensível procurada pelas crianças numa base de confidencialidade conforme necessário, para fomentar o bem-estar e um estilo de vida saudável. O governo australiano fornece um ótimo exemplo disto na sua página sobre parentalidade.[134]

Os programas de literacia digital devem dotar os alunos dos conhecimentos e aptidões necessários para lidar em segurança com uma ampla variedade de ferramentas e recursos digitais e relacionados com os conteúdos, criação, colaboração, participação e empenhamento cívico. As crianças necessitam também de ser educadas para conseguirem avaliar criticamente as fontes de informação de forma a poderem distinguir entre as fontes de informação confiáveis ou fidedignas e a desinformação e outras formas de conteúdos tendenciosos ou falsos, e a participarem como agentes empenhados nas suas comunidades.

Os curricula em matéria de literacia digital devem abranger um amplo conjunto de temas, incluindo a forma como os serviços digitais podem ajudar a aceder a serviços de apoio e aconselhamento confidenciais sobre várias questões, nomeadamente saúde sexual e saúde mental. Os curricula em matéria de segurança devem também dar destaque à participação positiva no mundo digital, particularmente a forma como as crianças se podem reunir e trabalhar de forma segura com outras crianças sobre questões relativas à sua segurança dentro e fora das redes. Por exemplo, muitos jovens em todo o mundo têm utilizado o ambiente digital para se organizarem coletivamente a fim de manifestar as suas opiniões e os seus receios acerca das alterações climáticas.

Os objetivos de desenvolvimento sustentável proporcionam uma visão do mundo segundo a qual aptidões, valores e atitudes são necessários para a transição para uma relação mais sustentável e equitativa com os recursos do mundo, devendo as crianças ser ensinadas acerca do papel que as tecnologias digitais podem desempenhar na promoção e, por vezes, no afastamento, deste caminho. Os Estados devem promover a implementação da educação para um desenvolvimento sustentável (EDS) a fim de possibilitar que se lide com as tecnologias, as práticas e os conteúdos digitais de uma forma crítica, resiliente e responsável.

Os curricula em matéria de segurança digital devem apoiar a participação das crianças através dos meios digitais, encorajando o debate e os conhecimentos acerca de comportamentos respeitadores; as crianças devem ser capazes de identificar abordagens abusivas, da sua parte e de terceiros. Todos os programas devem procurar dotar os alunos de conhecimentos em matéria de direitos

[134] https://raisingchildren.net.au/

humanos, incluindo direitos da criança e outros em ambiente digital, e formas disponíveis de apoio e recurso.

Os Estados devem investir na formação para garantirem que os professores ficam habilitados a ministrar cursos abrangentes de literacia digital.

105. Os alunos devem aprender, pelo menos, os rudimentos da cibersegurança e segurança digital, a partir da idade em que comecem a utilizar as tecnologias digitais. Devem também compreender as implicações sociais, económicas, culturais, políticas e ambientais da digitalização e vigilância.

Os professores devem receber formação para ministrar esta educação e devem dispor de amplos conhecimentos da prática em matéria de gestão de dados e disposições empresariais do setor, bem como de um rico acervo de recursos para orientar a utilização proveitosa de diversos produtos e serviços digitais.

> "Queremos que o governo, as empresas tecnológicas e os professores nos ajudem a lidar com a informação não fidedigna disponível nas redes"
>
> Gana, grupo de crianças[135]

B. Direito à cultura, ao lazer e a brincar

106. Os jogos de computador e outros constituem uma dimensão fundamental da alegria da infância e um aspeto essencial do desenvolvimento das crianças. As crianças de todo o mundo destacam o valor que atribuem ao interesse, diversão e estímulo obtidos a partir das atividades na Internet. Contudo, as brincadeiras são frequentemente vistas pelos pais como atividades "não produtivas", que simplesmente fazem as crianças perder tempo. Os Estados devem fomentar a utilização proveitosa dos produtos e serviços digitais e encorajar os pais a compreender a importância de brincar em ambiente digital. Para muitas crianças, as brincadeiras na Internet dão-lhes oportunidades para colaborar, experimentar, criar e explorar de que muito gostam e das quais beneficiam, e que de outra forma lhes poderiam faltar. Especialmente se desenhado de formas respeitadoras dos direitos da criança, o ambiente digital pode proporcionar espaços e recursos estimulantes em apoio das brincadeiras livres de formas que as crianças considerem emocional e culturalmente significativas.

107. O ambiente digital tem um papel cada vez mais importante na definição das identidades individuais e coletivas das crianças. Estas utilizam os espaços digitais para a construção, exploração e expressão das respetivas identidades. Há o risco de que os conteúdos disponíveis no ambiente digital sejam predominantemente em língua inglesa e concentrados na experiência cultural dos que os construíram e os detêm, primeiramente os EUA. Os Estados devem encorajar e investir em

[135] *Our Rights in a Digital World*, p. 14.

conteúdos locais nas línguas faladas pelas crianças[136], reconhecendo que estas beneficiarão e formarão a sua identidade em resultado da respetiva participação em atividades culturais e cívicas muito diversas na Internet.

108. O mundo digital é, na sua vasta maioria, feito por adultos e para adultos, com a consequência de que as crianças são frequentemente deixadas num mundo que não foi concebido para si. Os Estados devem encorajar os produtos e serviços digitais desenhados especificamente para crianças e, sempre que estas acedam a produtos para adultos, os fornecedores deverão considerar as respetivas necessidades. O ambiente digital representa uma oportunidade sem paralelo de lazer e aprendizagem, mas deverá ser concebido de forma a respeitar os direitos das crianças e satisfazer as suas necessidades de desenvolvimento.

109. As crianças necessitam de equilíbrio entre jogos e lazer nos espaços dentro e fora das redes, sendo a interação cara a cara essencial para todos os aspetos do seu desenvolvimento. Por muito que as crianças gostem da vida digital e nela participem, é igualmente importante que se reúnam com os seus amigos e famílias e acedam aos serviços nos locais onde moram. Em particular, as atividades recreativas como jogos, a socialização e a participação em atividades de grupo e desportivas em ambiente físico são importantes para a respetiva saúde, bem-estar e felicidade.

110. As crianças podem sofrer danos em ambiente digital se, para conseguirem participar num jogo ou atividade, forem visadas por publicidade (por exemplo, a comida pouco saudável), pressionadas por técnicas de desenho persuasivo ou encorajadas a fornecer os seus dados pessoais. A influência e o impacto dessas técnicas são tais que a Organização Mundial de Saúde fixou a redução da exposição das crianças ao *marketing* de alimentos pouco saudáveis como uma das principais recomendações da sua Comissão para a Erradicação da Obesidade Infantil.[137] Os Estados devem introduzir regulamentação para garantir que as crianças beneficiam de medidas de proteção contra a comercialização agressiva da infância.

111. Ao introduzir disposições regulamentares, é importante encontrar um equilíbrio entre a garantia de uma adequada proteção das crianças contra

---

[136] Os investigadores concluíram que os conteúdos em língua espanhola são com menor frequência e menor rapidez moderados para detetar casos de desinformação do que os conteúdos em língua inglesa. Enquanto que 70% da desinformação em inglês acaba por ser assinalada com advertências para os utilizadores, apenas 30% da desinformação comparável em língua espanhola é assinalada. https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation/

[137] https://www.who.int/end-childhood-obesity/en/ https://www.euro.who.int/__data/assets/pdf_file/0017/322226/Tackling-food-marketing-children-digital-world-trans-disciplinary-perspectives-en.pdf.

conteúdos nocivos e a liberdade para explorar oportunidades para brincar e desenvolver atividades recreativas e de lazer nas redes.

XII. Medidas especiais de proteção

A. Proteção contra a exploração económica, sexual e outras formas de exploração

112. Os Estados deverão proteger as crianças vítimas de exploração e abuso sexual nas redes garantindo que os materiais nocivos como os que configurem situações de abuso sexual de crianças são ativamente investigados, identificados e removidos. Isto para assegurar que as crianças vítimas de abuso sexual nas redes são identificadas, tiradas das situações de abuso e dispõem de acesso à justiça, a vias de recurso e ao apoio social e psicológico de que necessitam. Para que isto aconteça, é necessária coordenação a nível nacional e formação especializada dos agentes responsáveis pela aplicação da lei, bem como a afetação dos fundos adequados, devendo ainda os Estados cooperar a nível internacional.

113. Os Estados devem regulamentar e fazer aplicar as leis em vigor relativas ao trabalho infantil artístico, caracterizado pelo envolvimento habitual, monetizado ou recompensado de crianças em produções artísticas ou de entretenimento, orientado para o espetáculo e com expectativas externas, com a estipulação de medidas adequadas de proteção, como autorização judicial, acompanhamento educativo e psicológico e limitações do horário de trabalho diário, conforme estabelecido pela Convenção n.º 138 e Recomendação n.º 146 da Organização Internacional do Trabalho, reconhecendo a sua relevância para as crianças influenciadoras digitais. Por exemplo, a França adotou uma lei sobre a utilização comercial das imagens de crianças influenciadoras digitais em plataformas digitais de partilha de vídeos no caso de crianças menores de 16 anos[138]. Estas novas medidas de proteção tornarão aplicáveis às crianças influenciadoras digitais os códigos laborais franceses, considerando-se a compensação obtida pelas crianças influenciadoras digitais como um salário[139].

Os Estados devem também rever as leis e políticas pertinentes para garantir que as crianças são protegidas contra a exploração económica e outras formas de exploração, e que os respetivos direitos em relação ao trabalho em ambiente digital e oportunidades conexas de remuneração ficam salvaguardados. Os Estados devem igualmente informar os pais e as crianças acerca das medidas de

---

[138] https://www.bbc.co.uk/news/world-europe-54447491.

[139] https://marketinglaw.osborneclarke.com/data-and-privacy/french-parliament-adopts-law-commercial-use-child-influencers-image-video-sharing-platforms/#:~:text=The%20French%20Parliament%20adopted%20an,Youtubers%20count%20millions%20of%20subscribers.

proteção aplicáveis e garantir a existência de mecanismos de aplicação adequados.

Os Estados deverão ainda trabalhar para dar resposta ao papel que a exploração infantil desempenha na produção de dispositivos digitais como *smartphones*, *laptops* e carros elétricos. Por exemplo, as investigações revelaram a presença de crianças trabalhando em condições não reguladas na República Democrática do Congo (RDC)[140].

114. Os Estados deverão assegurar-se de que estão em vigor leis e regulamentos para proteger eficazmente as crianças contra bens ou serviços nocivos que estas possam encontrar em ambiente digital. Estas leis deverão ser apoiadas com os recursos e o compromisso necessários para fazê-las cumprir.

As empresas que vendem ou disponibilizam bens e serviços com restrições etárias necessitam de utilizar mecanismos de verificação da idade que proporcionem níveis apropriados de salvaguarda, privacidade e proteção de dados.

115. As leis que abrangem o tráfico de crianças deverão ser atualizadas de forma a abranger o ambiente digital, por exemplo o projeto da Câmara dos Representantes dos EUA, *Fight Online Sex Trafficking Act* (FOSTA) e o projeto do senado norte americano, *Stop Enabling Sex Traffickers Act* (SESTA), assinadas pelo Presidente Donald Trump[141]. O pacote FOSTA-SESTA proíbe a comparticipação, cumplicidade ou instigação conscientes do tráfico para fins sexuais, incluindo exploração sexual de crianças. Os Estados devem garantir que os serviços e produtos digitais não fomentam nem ocultam, intencionalmente ou não, o tráfico de crianças.

116. Cada jurisdição ou região pode ter as suas próprias leis e o comentário geral n.º 25 reflete a expectativa de que as mesmas sejam atualizadas de forma a abranger o mundo digital. No Reino Unido, por exemplo, foi introduzido um código legal ao abrigo do *Data Protection Act 2018* a fim de estabelecer normas reguladoras dos serviços digitais tendo em vista a proteção das crianças na Internet – o *Age Appropriate Design Code*[142]. No Gana, as crianças são expressamente mencionadas no *Data Protection Act* de 2012[143].

---

[140] https://www.oecd-ilibrary.org/docserver/5d3abe03-en.pdf?expires=1615902487&id=id&accname=guest&checksum=60206F84B1815E701A64A522AE238C79.

[141] https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom

[142] https://ico.org.uk/for-organisations/age-appropriate-design/additional-resources/what-is-the-children-s-code/#:~:text=The%20Children's%20Code%20(or%20Age,comes%20to%20their%20personal%20data.

[143] https://iclg.com/practice-areas/data-protection-laws-and-regulations/ghana

B. Administração da justiça para crianças

117. As crianças que são presas e acusadas de cribercrimes devem beneficiar de todas as salvaguardas dos sistemas de justiça para crianças enunciadas no comentário geral n.º 24 (2019) sobre os direitos das crianças no sistema de justiça para crianças[144]. Aqui se incluem os crimes de terrorismo alegadamente praticados em meios digitais, estando as crianças, por exemplo, cada vez mais em risco da prática do crime de "glorificação do terrorismo"[145]. É muitas vezes possível dar resposta à cibercriminalidade através da utilização de mecanismos de justiça reparadora. Se necessário, deverão estar disponíveis mecanismos alternativos ao processo judicial para as crianças delinquentes, com supervisão e formação reabilitadora sobre a utilização responsável das tecnologias digitais.

Os Estados devem tentar utilizar as tecnologias digitais de formas que promovam o acesso das crianças à justiça.

118. O aumento dos conteúdos auto gerados está associado a uma série de normas do mundo digital – por exemplo, métricas de popularidade que encorajam os jovens a difundir imagens geradoras de interações desproporcionais ou de comercialização de conteúdos de cariz sexual pelos influenciadores[146].

As crianças não têm a capacidade nem a responsabilidade dos adultos e não devem ser punidas criminalmente pela criação de tais conteúdos, devendo antes os Estados responder a estes comportamentos, alguns dos quais gerados sob coação, proporcionando às crianças a educação e o apoio emocional necessários à respetiva reabilitação. Quadros de segurança desde a fase de desenho devem garantir que os serviços digitais não permitem nem encorajam a criação de conteúdos sexuais gerados pelo próprio.

119. A vigilância em locais públicos não deve ser usada para perseguir criminalmente as crianças ou privá-las de outros direitos – por exemplo o direito de associação. Nos meses de verão de 2020, decorreram manifestações em todo o

---

144 https://undocs.org/CRC/C/GC/24

145 https://www.trtworld.com/magazine/french-police-interrogate-muslim-children-for-disliking-insulting-cartoons-41233

146 Por exemplo, a OnlyFans, um serviço por subscrição que permite a compra e venda de conteúdos sexualmente explícitos, tornou-se mais comum para celebridades e influenciadores das redes sociais. Devido a este estatuto de celebridade, as crianças são simultaneamente expostas a conteúdos oriundos do OnlyFans (por exemplo, porque os criadores promovem conteúdos do OnlyFans em serviços como o Twitter, que permite a nudez na sua plataforma) e à ideia de que se pode atingir sucesso financeiro a partir do serviço. Desta forma, as crianças ficam em risco, não só de acederem a conteúdos pornográficos, mas também de participarem de forma não intencional na procura e produção de imagens que configurem abuso sexual de crianças, quando os conteúdos de cariz sexual são comercializados e publicitados no mundo digital.

mundo em solidariedade com o movimento *Black Lives Matter*. Há preocupações de que a vigilância digital, com base na utilização pela polícia de *software* de reconhecimento facial e de vídeos públicos ou imagens carregadas pelos manifestantes, possa deixar muitas pessoas, sem o saberem, em bases de dados de reconhecimento facial.[147]

120. Sempre que a digitalização dos processos judiciais resulte na ausência de contacto pessoal com as crianças, tal poderá prejudicar a capacidade destas para interagir com os tribunais de forma significativa e, no âmbito do sistema de justiça penal, frustrar as medidas de justiça reabilitativa e reparadora assentes no desenvolvimento de relações com a criança. Diligências judiciais realizadas remotamente podem desorientar as crianças e privá-las do apoio pessoal de que necessitam.

A introdução de inteligência artificial no sistema de justiça pode ter efeitos discriminatórios ou violar os demais direitos da criança, devendo ser seguido um princípio de precaução a fim de prevenir a violação dos direitos à não discriminação e à privacidade no contexto da inteligência artificial.[148]

Os Estados devem garantir que o funcionamento dos serviços digitais em contextos judiciais não prejudica os direitos da criança nem as aliena do processo judicial. Sempre que as crianças estejam privadas de liberdade, o contacto pessoal é igualmente necessário para garantir o bem-estar e a reabilitação da criança.

C. Proteção das crianças em conflitos armados, crianças migrantes e crianças em outras situações de vulnerabilidade

121. O ambiente digital pode dar poder às crianças e a outras pessoas, fornecendo-lhes informação valiosa acerca de certas situações em tempos de conflito armado, busca de asilo e desastres naturais, que pode fazer a diferença entre a vida e a morte. Pode permitir-lhes manter contacto com as respetivas famílias, procurar informação fundamental, obter ajuda, prosseguir a educação e sentir-se em ligação com o mundo exterior. Em alguns casos, o ambiente digital pode até ser um escape das realidades dos conflitos armados, como demonstra a popularidade dos videojogos para jovens no Afeganistão.[149] Questões como a exploração comercial (ou não comercial) de crianças vulneráveis em tais ambientes deverão ser consideradas pelos governos – nomeadamente fotografia,

---

147 https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database

148 https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf

149 https://www.nytimes.com/2020/11/23/world/asia/afghanistan-video-games-pubg-playerunknown-battlegrounds.html

videografia, vigilância por *drones* e outros modos análogos no contexto de atividades como a realização de documentários; especialmente se não forem consentidas, constituem graves violações dos direitos destas crianças vulneráveis.

Devem ser considerados e concebidos programas intergovernamentais de coesão social para o ambiente digital a fim de ultrapassar os problemas enfrentados pelas crianças em conflitos armados, contextos migratórios e outras situações de vulnerabilidade (para melhorar competências de vida, minimizar problemas de adaptação social, aumentar a consciencialização para os riscos e recursos existentes na sociedade e garantir que vivem a vida de acordo com os seus direitos e, simultaneamente, que desenvolvem a compreensão recíproca e a tolerância entre culturas).

122. O ambiente digital tem vindo a permitir o aliciamento de crianças por grupos extremistas com vista à sua radicalização e envolvimento em conflitos armados ou violentos a nível interno ou internacional. Por exemplo, a cidadã alemã Linda Wenzel é apenas uma de dezenas de crianças aliciadas e recrutadas através de meios de comunicação digitais aos 15 anos de idade para ir da Alemanha para a Síria a fim de se juntar ao Estado Islâmico[150]. Os Estados devem garantir que tal atividade é criminalizada e efetivamente investigada e objeto de ação penal.

XIII. Cooperação internacional e regional

123. A natureza internacional das empresas que fornecem serviços e produtos digitais cria a necessidade de cooperação bilateral e multilateral. Embora cada Estado individualmente seja responsável pela proteção das crianças dentro dos limites da legislação do país onde vivem, os Estados devem colaborar para efeitos de aplicação da lei, tendo em vista a partilha de informações e a definição de regras coerentes. Se tais medidas forem adotadas a nível internacional ou regional, serão mais capazes de proteger toda a panóplia de direitos, como a liberdade de expressão ou o direito à informação, ao mesmo tempo que combatem a desinformação e o discurso de apelo ao ódio.

124. O mundo digital é internacional por natureza, pelo que se encoraja a cooperação entre Estados. Muitos Estados começaram o processo de criação de normas e regimes de regulação em uma ou mais áreas abrangidas pelo Comentário Geral. A partilha de conhecimentos e a adoção de abordagens comuns podem acelerar e apoiar mais prestações e medidas de proteção para as crianças de todo o mundo. A cooperação pode ser efetuada numa base regional, internacional e bilateral. Em particular, a adoção de linguagem e definições comuns garantirá uma ágil cooperação transfronteiriça. Por exemplo, a

[150] https://www.independent.co.uk/news/world/german-isis-bride-death-penalty-hanging-iraq-groomed-teenager-linda-wenzel-a7984171.html.

Terminologia Universal da Resposta Nacional Modelo sobre abuso sexual de crianças.[151]

XIV. Difusão

125. O conteúdo e recomendações do Comentário Geral terão mais valor se forem amplamente conhecidos e compreendidos. É necessário que os Estados façam esforços significativos para garantir que todas as pessoas para as quais o Comentário Geral for relevante têm acesso ao mesmo e beneficiam de apoio para compreender o que significa e que providências haverá que tomar para lhe dar seguimento. Versões adaptadas ou acessíveis a crianças devem também ser disponibilizadas e distribuídas muito amplamente por toda a sociedade.

[151] https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf.

Anexo 1: Glossário

Termo	Definição
Tecnologia de assistência	Tecnologia desenvolvida para apoiar ou melhorar a independência de uma pessoa, incluindo sistemas e dispositivos de adaptação e reabilitação para pessoas com deficiência como um leitor de ecrãs ou mecanismo de reconhecimento de fala.
Processamento automatizado	Processo de tomada de decisão por meios automáticos, isto é, usando *software* configurado para analisar os dados fornecidos e seguir regras estabelecidas a fim de chegar a decisões com base em algoritmos, sem envolvimento humano.
Busca automatizada	Processo de análise dos dados dos utilizadores para filtrar o conteúdo a que estes têm acesso nas redes, sobretudo com interesses comerciais. O conteúdo é geralmente escolhido com base nas perceções da reação do utilizador a outros conteúdos, ou com base nos conteúdos procurados por outros utilizadores que tenham agido de forma semelhante.
Sistemas automatizados	*Software* e *hardware* programados para desempenharem automaticamente uma função sem necessidade de intervenção humana que dê ordens ou instruções para cada operação.
Orientação para os comportamentos	Análise da atividade dos utilizadores nas redes a fim de lhes dirigir publicidade, mensagens, sugestões de novos conteúdos ou contactos com outros utilizadores com base nas suas anteriores preferências, frequentemente com a intenção de manipular os seus comportamentos futuros.
Riscos de conteúdo, contacto, conduta e contratação	*Riscos de conteúdo:* potencial dano para os utilizadores baseado na natureza do conteúdo digital, incluindo desadequação etária (eg. pornografia), não fidedigna (eg. informação enganosa ou desinformação) ou determinadas outras categorias de conteúdo (eg. promoção de comportamentos de risco ou métodos de automutilação ou suicídio). *Riscos de contacto:* potencial dano criado pela oportunidade dada aos utilizadores para contactarem entre si através da utilização de serviços digitais, por exemplo permitindo que estranhos ou pessoas que ocultem a sua identidade contactem crianças. *Riscos de conduta:* potencial dano baseado no comportamento ou conduta do utilizador ou seus pares, como a utilização deliberada de plataformas digitais para

	ameaçar ou assediar outros utilizadores, incluindo o *ciberbullying*, o envio de mensagens de cariz sexual e os comentários de ódio, por vezes também de forma não intencional através da revelação de informação confidencial relativa a outros utilizadores. *Riscos de contratação:* potencial dano quando um utilizador é exposto a relações ou pressões indevidas de contratação comercial, como utilização compulsiva, jogo, publicidade dirigida, custos ocultos, termos e condições injustos e perda de controlo sobre os respetivos dados pessoais.
Moderação de conteúdos	Prática de monitorizar e verificar se os conteúdos gerados pelos utilizadores estão conformes a regras pré definidas tendo em vista a eliminação de conteúdos considerados proibidos, automaticamente ou utilizando moderação humana. A moderação de conteúdos pode ser levada a cabo em simultâneo com a criação de conteúdos, como nos serviços de chat, ou com dilação temporal, como nos fóruns.
Ciberagressão	Atos nocivos infligidos a indivíduos ou grupos, nas redes ou através da utilização das tecnologias digitais, frequentemente com a intenção de ofender ou magoar outro indivíduo ou grupo.
Minimização de dados	Princípio de recolher o mínimo número possível de dados pessoais pertinentes que sejam necessários para o objetivo prosseguido com o processamento de dados e de conservar tais dados unicamente até que seja necessário para o mesmo fim.
Processamento de dados	Inclui processos de recolha, gravação, conservação, análise, difusão e utilização de dados.
Literacia digital	Capacidade de utilizar as tecnologias da informação e comunicação para encontrar, avaliar, criar e comunicar. Termos conexos são, nomeadamente, "literacia para os media", "literacia para a informação" ou "literacia para os media e a informação".
Digitalização	Adaptação de ambientes, práticas, empresas e vida quotidiana a fim de incluir os serviços e infraestruturas digitais e beneficiar dos mesmos. Refere-se também à conversão da informação em formato digital.
Informação enganosa e desinformação	*Informação enganosa:* partilha consciente de informação falsa. *Desinformação*: partilha de informação falsa, sem intenção de provocar dano.

Análise emocional	Recolha de dados tendo em vista determinar ou inferir o estado de espírito de uma pessoa, frequentemente levada a cabo mediante a análise de vídeos, comunicações de voz e texto, ou dados pessoais, para identificar marcadores, como a expressão facial e o tom, que estão correlacionados com emoções concretas, utilizando técnicas de aprendizagem mecanizadas, incluindo algoritmos.
Roubo de identidade	Personificação fraudulenta de outra pessoa, por exemplo tendo em vista aceder ao seu património, prejudicar a sua reputação, conseguir acesso aos seus contactos nas redes ou lucrar de outra forma.
Publicidade imersiva	Integração subliminar de publicidade em conteúdos ou serviços digitais, fazendo com que os utilizadores fiquem imersos nas funcionalidades dos conteúdos e serviços e simultaneamente expostos a *marketing* e mensagens comerciais.
Tecnologia de implante	Microship que pode ser implantado numa pessoa para armazenar, localizar ou obter informação contida numa base de dados externa, nomeadamente de identificação pessoal e/ou questões médicas, aplicação da lei ou contactos.
Filtragem de informação	Utilização de um programa para monitorizar os conteúdos digitais e identificar ou ocultar conteúdos que preencham determinados requisitos. Utilizações comuns da filtragem de informação são, por exemplo, a ocultação de conteúdos ofensivos dos resultados dos motores de busca ou a ordenação destes resultados.
Interoperabilidade	Capacidade dos diferentes sistemas para comunicar entre si, partilhar dados e utilizar a informação recebida.
Marketing neurológico	Estudo da forma como os cérebros das pessoas reagem a conteúdos de marketing e aplicação deste conhecimento no desenvolvimento de campanhas de marketing mais eficazes. As reações podem ser medidas de muitas formas diferentes, da digitalização da atividade cerebral ao tempo de interação, número de clics e tempo despendido numa página.
Privacidade desde a fase de desenho	Prática de conceber serviços digitais tendo em vista proteger ao máximo a privacidade dos utilizadores, por exemplo estabelecendo que as contas dos utilizadores menores de idade serão privadas por defeito ou minimizando o número de dados recolhidos.
Definição de perfis	Prática de utilizar os dados pessoais de um indivíduo para inferir, prever ou analisar características relativas a essa pessoa, por exemplo o que gosta, o que não gosta, preferências, posições, opiniões ou comportamento,

	tendo em vista recomendar conteúdos, produtos ou serviços com base no perfil de dados da pessoa.
Segurança desde a fase de desenho	Prática de conceber serviços digitais tendo em vista garantir ao máximo a segurança dos utilizadores, por exemplo estabelecendo definições de segurança por defeito para as contas dos utilizadores menores de idade ou impedindo que os adultos os contactem.
Publicidade dirigida	Prática de exibir determinados anúncios a certos utilizadores com base nos dados recolhidos acerca destes, nomeadamente a sua atividade nas redes, compras, localização, género, idade e preferências.
Realidade virtual e aumentada	*Realidade virtual:* simulação, gerada por computador, de uma imagem ou ambiente tridimensional com o qual uma pessoa, utilizando equipamento digital especial como um capacete com ecrã incorporado ou luvas equipadas com sensores, possa interagir de uma forma aparentemente real. *Realidade aumentada:* simulação do mundo físico com características alteradas ou itens suplementares, geralmente experimentada através de um ecrã que permite a sobreposição de objetos virtuais a uma imagem ou vídeo ao vivo da realidade.

Acerca da Fundação 5Rights

A Fundação 5Rights desenvolve novas políticas, cria enquadramentos inovadores, desenvolve normas técnicas, publica estudos, discute narrativas recebidas e garante que os direitos e necessidades das crianças são reconhecidos e beneficiam de prioridade no mundo digital. Embora a 5Rights trabalhe exclusivamente em prol e com as crianças e jovens menores de 18 anos, as nossas soluções e estratégias são relevantes para muitas outras comunidades.

O nosso foco está na mudança realista e o nosso trabalho é citado e amplamente utilizado em todo o mundo. Trabalhamos com governos, instituições intergovernamentais, associações profissionais, instituições de ensino superior, empresas e crianças, para que os produtos e serviços digitais possam ter um impacto positivo nas experiências vividas pelos jovens.

Saiba mais

Visite ww.5Rightsfoundation.com ou contacte info@5rightsfoundation.com

Construindo o mundo digital que os jovens merecem