PODER LEGISLATIVO
Câmara dos Deputados
Comissão Especial sobre Inteligência Artificial (PL 2338/2023)

Evento: Audiência Pública – Sistemas de IA, IA no serviço público e em infraestruturas críticas

Nesta terça-feira (30), a Comissão Especial destinada a proferir parecer ao PL 2338/2023 realizou audiência pública para debater o tema "**Sistemas de IA, IA no serviço público e em infraestruturas críticas**".

A audiência foi convocada a partir dos Requerimentos nºs 23, 35, 95, 101, 114, 116, 149 e 150/2025, de autoria dos(as) deputados(as) **Fernanda Melchionna** (PSOL/RS), R**eginaldo Lopes** (PT/MG), **Camila Jara** (PT/MS), **Jandira Feghali** (PCdoB/RJ), **Aureo Ribeiro** (SD/RJ), **Luizianne Lins** (PT/CE), **David Soares** (UNIÃO/SP) e **Adriana Ventura** (NOVO/SP).

Estiveram presentes na audiência:

- **Carlos Bruno Ferreira da Silva**, procurador da República e Coordenador da Comissão de Tecnologia da Informação e Comunicação da 3ª Câmara de Coordenação e Revisão do Ministério Público Federal (MPF);
- **Rodrigo Henrique Luiz Corrêa**, secretário Municipal de Integridade da Prefeitura do Rio de Janeiro, associado ao Fórum de Proteção de Dados Pessoais dos Municípios;
- **Pablo Nunes**, pesquisador em segurança pública, tecnologia e dados abertos;
- **Hugo Melo Giallanza**, presidente da Brasil Startups;
- **Raúl Echeberría**, diretor Executivo da Associação Latino-Americana de Internet (ALAI);
- **Jacqueline Alves Torres**, gerente da Agência Nacional de Saúde Suplementar (ANS); e
- **Sandra Ávila**, professora e cientista da computação do Instituto de Computação da Universidade Estadual de Campinas (Unicamp).

Carlos Ferreira do MPF, informou que em 2024 foi emitida uma nota técnica sobre o projeto de lei em debate e, embora reconheça avanços no texto, ressaltou que alguns pontos seguem merecendo atenção.

Em primeiro lugar, apontou que ainda falta previsão de uma avaliação contínua do impacto algorítmico. O artigo 23 menciona a avaliação prévia, mas não contempla a necessidade de acompanhamento permanente, sobretudo diante do risco de vieses discriminatórios. A ausência de monitoramento constante pode trazer graves prejuízos a minorias raciais, sexuais e outros grupos vulneráveis.

Mencionou também a limitação do artigo 13, que não prevê a possibilidade de inclusão de novas atividades vedadas pela autoridade administrativa. Considerando que não é possível antecipar todas as aplicações futuras da inteligência artificial, seria fundamental admitir que a autoridade pudesse atualizar a lista de forma transparente e com participação social. Entre os avanços, destacou o inciso IV do artigo 13, que, com suas novas alíneas, fortalece a atuação das entidades de segurança pública, permitindo monitoramento em tempo real e prevenindo ações criminosas ou terroristas.

Ao tratar das obrigações dos desenvolvedores de sistemas de alto risco, previstas no artigo 18, observou que a referência à robustez carece de exigência quanto ao volume mínimo de

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

dados. Essa previsão daria consistência técnica ao conceito e contribuiria para evitar vieses discriminatórios. Outro ponto de preocupação é a ausência de menção expressa à cooperação com autoridades de controle, como o Ministério Público. Muitas empresas se escoram no sigilo industrial e comercial para não fornecer informações necessárias à fiscalização, dificultando a atuação dos órgãos competentes.

Referiu-se também aos sistemas generativos, observando que o artigo 29 não impõe a obrigação de etiquetamento para conteúdos produzidos por inteligência artificial. Essa medida já é adotada em legislações internacionais e seria essencial para evitar manipulação eleitoral, danos à honra e desinformação.

Defendeu ainda que o artigo 11, em especial o inciso II, deveria incluir expressamente a legislação de direitos coletivos, como a Lei da Ação Civil Pública e o Código de Defesa do Consumidor, uma vez que os danos causados por sistemas de IA tendem a ser difusos e coletivos. Sobre a avaliação de conformidade, ressaltou que o artigo 16 menciona essa obrigação, mas não garante que seja feita por entes externos independentes, algo que já se mostrou essencial em outros setores regulados, como o de mineração.

Por fim, defendeu o aperfeiçoamento do capítulo V, de responsabilidade, com a inclusão da responsabilidade objetiva e da inversão do ônus da prova nos casos de IA de alto risco. Considerou que o Congresso já alcançou maturidade para reconhecer a gravidade desses sistemas e estabelecer parâmetros jurídicos mais rigorosos.

O secretário **Rodrigo Corrêa** ressaltou que alguns estados e cidades, como o Rio de Janeiro, já implementam legislações próprias sobre inteligência artificial, o que demonstra a urgência do tema no âmbito subnacional. Defendeu que, por serem os municípios os entes mais próximos do cidadão e aqueles que concentram a maior parte da prestação de serviços públicos, é indispensável que sejam contemplados pela legislação em construção.

Ao comentar o texto do PL 2338/2023, abordou o artigo 23, apontando que a vedação ao tratamento de dados de raça, cor ou etnia, salvo previsão expressa em lei, pode engessar a atuação dos municípios, uma vez que a formulação de políticas públicas baseadas em evidências exige o tratamento desses dados. Sugeriu substituir a exigência de previsão legal por justificativa expressamente fundamentada, conferindo maior flexibilidade e efetividade.

Destacou ainda o artigo 70, que atribui aos entes públicos responsabilidades ligadas à educação, informação, letramento digital e conscientização sobre tecnologias. Considerou tais atribuições necessárias e salutares, mas alertou que, sem previsão de custeio, sua execução se tornará inviável, diante das limitações orçamentárias de estados e municípios. Defendeu, portanto, que o projeto preveja a criação de um fundo pela União ou a destinação de recursos oriundos das multas aplicadas.

Em seguida, abordou o artigo 45, que institui o Sistema Nacional de Regulação e Governança em Inteligência Artificial. Sugeriu que esse sistema assegure a participação de entidades representativas de estados e municípios, de modo a tornar a governança mais democrática. Propôs, também, que a Agência Nacional de Proteção de Dados (ANPD) seja obrigada a consultar tais entidades antes de editar normas específicas sobre temas de interesse regional ou local, permitindo ainda que consórcios ou entes individuais apresentem propostas adaptadas às suas realidades.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Na mesma linha, recomendou que o Conselho Permanente de Cooperação Regulatória de Inteligência Artificial, previsto no artigo 53, contemple representantes de estados e municípios, garantindo voz ativa aos entes subnacionais na definição das diretrizes nacionais.

Defendeu, ainda, que os municípios sejam incluídos no regime de *sandbox* regulatório simplificado, previsto no artigo 56, atualmente restrito a startups e pequenas empresas. Argumentou que muitas prefeituras possuem estrutura administrativa inferior à de microempresas e, sem um regime adaptado, dificilmente conseguirão implementar programas de inteligência artificial.

Por fim, ao comentar o artigo 73, alertou para a redação que prevê regime simplificado apenas em casos de fomento nacional. Ressaltou que a expressão poderia restringir iniciativas locais e regionais e sugeriu a alteração para "fomento de caráter nacional, regional e local".

O pesquisador **Pablo Nunes** informou que atualmente existem 442 projetos de reconhecimento facial em andamento no país, com potencial de vigiar 87 milhões de pessoas. Esse crescimento ocorreu sem debate público, regulação ou avaliação de impacto, resultando de escolhas políticas e de contratos milionários celebrados por estados e municípios com empresas privadas, muitas vezes em processos pouco transparentes. Ressaltou que a pressão pelo uso da tecnologia não vem da sociedade, mas dos fornecedores que buscam expandir seus negócios no Brasil.

Ao abordar os riscos do reconhecimento facial, destacou, em primeiro lugar, os vieses discriminatórios. Estudos nacionais e internacionais demonstram que os erros recaem principalmente sobre pessoas negras e periféricas, realidade que persiste mesmo após avanços técnicos recentes. O segundo risco apontado foi a invasão de privacidade, já que a tecnologia permite o monitoramento biométrico em massa, sem transparência, com dados armazenados em bancos sem controle social. Em terceiro lugar, alertou para os impactos negativos no policiamento, uma vez que os falsos positivos aumentam a carga de trabalho das forças de segurança, sem contribuir efetivamente para a prevenção de crimes. Como quarto ponto, citou a ameaça aos direitos democráticos, pois o reconhecimento facial pode ser usado para identificar e intimidar manifestantes ou opositores políticos. Por fim, mencionou o risco de vazamento de dados sensíveis, já verificado no Brasil, com informações biométricas sendo comercializadas na *deep web*.

Trouxe exemplos de estudos de caso em Goiás e na Bahia, onde recursos foram destinados à instalação de câmeras de reconhecimento facial em municípios que careciam de serviços básicos, como internet para estudantes ou saneamento adequado, revelando um dilema de prioridades. Em São Paulo, relatou o caso do programa *Smart* Sampa, avaliado segundo metodologia do Banco Mundial, cujo resultado demonstrou ausência de impacto positivo na redução da criminalidade, apesar do alto custo mensal de R$ 10 milhões.

Ressaltou ainda os riscos à segurança nacional, considerando que muitas empresas fornecedoras são estrangeiras e mantêm os dados da população em data centers fora do país. Nesse contexto, analisou o PL 2338/2023, reconhecendo que o texto classifica o uso do reconhecimento facial como de risco excessivo, mas alerta que as exceções previstas, com termos vagos como "estritamente necessário" ou "crime grave", criam um vácuo regulatório que legitima seu uso sem garantias adequadas de proteção.

Defendeu, assim, a revisão do inciso IV do artigo 13, propondo a proibição geral do uso de reconhecimento facial em espaços públicos. Caso a retirada das exceções não seja viável, sugeriu que estas sejam submetidas às mesmas exigências dos sistemas de alto risco, incluindo avaliação de impacto, auditoria independente, supervisão humana e mecanismos de

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

contestação. Defendeu também que qualquer uso excepcional seja condicionado a legislação específica com salvaguardas robustas de direitos humanos, e que haja controle multissetorial envolvendo a ANPD, o CNJ, ouvidorias e conselhos de direitos humanos. Reforçou, ainda, a importância de cláusulas de revisão periódica com publicação de métricas e relatórios técnicos.

Concluiu afirmando que, se o objetivo for proteger direitos e fortalecer a democracia, o Congresso deve enfrentar o debate com coragem. O reconhecimento facial deve ser compreendido como uma tecnologia de vigilância que amplia desigualdades, compromete a soberania e fragiliza a democracia, sem evidências de ganhos concretos de segurança pública. Defendeu que a segurança da população será alcançada não com mais vigilância, mas com mais direitos, políticas públicas e democracia.

Hugo Giallanza da Brasil Startups, iniciou sua intervenção comparando o cenário brasileiro ao internacional, destacou que o país enfrenta uma baixa cultura de investimento. Enquanto o Brasil conta com cerca de 6 milhões de investidores na bolsa de valores, a China possui aproximadamente 80 milhões e os Estados Unidos 150 milhões. Essa diferença reflete a dificuldade nacional em alavancar recursos para competir em áreas estratégicas como a inteligência artificial, especialmente diante de um ambiente de juros altos e perfil conservador de investimentos.

Apresentou um panorama dos principais *players* globais em inteligência artificial. Os Estados Unidos investem cerca de US$ 67 bilhões no setor, equivalentes a 3,5% do PIB, com mais de 5 mil empresas estabelecidas e forte capital humano, além de uma política governamental flexível voltada à inovação. A China investe US$ 38 bilhões, 2,4% do PIB, com cerca de 3 mil empresas e 20% dos empreendedores reconhecidos internacionalmente. A Europa, por sua vez, aplica US$ 10 bilhões, 2,1% do PIB, com aproximadamente 1.500 empresas, mas adota uma política mais rígida. O Brasil investe apenas US$ 1,8 bilhão, 1,2% do PIB em P&D, com cerca de 140 a 150 empresas consolidadas, baixo capital humano e um Plano Nacional de Inteligência Artificial ainda em construção.

Segundo dados levantados pela Brasil Startups junto ao ecossistema de inovação, os principais obstáculos enfrentados pelas empresas são a insegurança jurídica, a falta de incentivos, as restrições ao uso de dados, a burocracia e os altos custos tributários. A insegurança jurídica aparece como o fator mais crítico, reforçando a necessidade de um marco regulatório que ofereça previsibilidade e confiança para investidores e empreendedores.

Alertou que mudanças abruptas em legislações ou regulamentos podem comprometer modelos de negócio já estabelecidos, trazendo instabilidade e risco de inviabilização. Defendeu, portanto, que a regulação deve buscar equilíbrio: rígida o suficiente para proteger direitos, mas sem sufocar a inovação e o desenvolvimento das empresas nacionais.

Apontou ainda que excesso de burocracia, restrições desmedidas ao uso de dados e alta carga tributária reduzem a competitividade internacional do Brasil, atrasam a inovação e limitam o *time to market* das soluções. Para ilustrar, comparou o ambiente regulatório europeu, mais restritivo, com o norte-americano, voltado à remoção de barreiras e estímulo à inovação. Na sua visão, o Brasil deve adotar uma posição intermediária, aproveitando a proteção proporcional da União Europeia, mas preservando a flexibilidade e o incentivo à inovação dos Estados Unidos.

Entre as propostas apresentadas, defendeu a adaptação do registro europeu com maior transparência na formação de bases de dados sem violar direitos autorais, a desburocratização e a manutenção de baixo custo regulatório, a criação de mecanismos de fomento à inovação capazes de oferecer segurança jurídica, o estabelecimento de *sandbox regulatórios* que permitam experimentação supervisionada por startups e a redução de barreiras desnecessárias

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

ao desenvolvimento tecnológico, de forma a preservar condições para que a inovação floresça no Brasil.

Raúl Echeberría da ALAI, informou que na América Latina existem cerca de 500 projetos de lei sobre o tema em discussão nos parlamentos nacionais da região, embora apenas dois tenham sido aprovados até o momento, em El Salvador e no Peru. Esse dado demonstra a complexidade do tema e a dificuldade de construir regulações equilibradas.

Afirmou que o Brasil tem a oportunidade de assumir protagonismo ao conciliar proteção de direitos, promoção da inovação e governança institucional eficiente. Citou experiências internacionais e regionais que demonstram o potencial da inteligência artificial na educação, na recuperação ambiental, em agências reguladoras, na justiça, na segurança pública e na gestão municipal. Ressaltou, contudo, que para esses avanços alcançarem escala é indispensável garantir interoperabilidade e segurança jurídica.

Apresentou preocupações centrais em relação ao texto do PL 2338/2023. Em primeiro lugar, destacou que os conceitos de risco são excessivamente amplos, com categorias como risco elevado ou excessivo sem critérios objetivos, o que pode levar ao enquadramento indevido de sistemas simples utilizados pelo próprio Estado, como triagens ou assistentes virtuais. Em segundo lugar, criticou a responsabilização genérica de toda a cadeia produtiva, sem distinção entre desenvolvedores, fornecedores, usuários e contratantes, o que gera insegurança jurídica e pode afastar empresas do setor público. Em terceiro lugar, apontou barreiras ao uso legítimo de dados públicos para treinamento de modelos, limitando o desenvolvimento de soluções adaptadas à realidade brasileira. Acrescentou ainda a burocratização excessiva, com exigências desproporcionais de relatórios, explicabilidade e transparência indistinta, e alertou para o poder normativo amplo da Agência Nacional de Proteção de Dados sem salvaguardas como consultas públicas e análises de impacto regulatório. Por fim, ressaltou problemas graves no capítulo de direitos autorais, que, da forma como está, exigiria licenciamento individualizado de obras para treinamento, algo tecnicamente inviável e economicamente insustentável, sem precedentes internacionais.

Defendeu ajustes no projeto com base em boas práticas internacionais, como a adoção de regras proporcionais ao risco, critérios objetivos para a classificação de sistemas de alto risco, uso legítimo de dados públicos com salvaguardas, estímulo ao ecossistema acadêmico e de pesquisa, fortalecimento do código aberto, maior exigência de motivação técnica e consulta pública nas decisões da ANPD e revisão do capítulo de direitos autorais, com foco no resultado dos modelos e na previsão de exceções para pesquisa, startups e usos não comerciais.

Mencionou, ainda, iniciativas em andamento na região voltadas ao desenvolvimento de modelos de linguagem que reflitam a realidade linguística e cultural latino-americana, como o LATAM-GPT, e defendeu que tais projetos só terão sucesso se houver políticas públicas adequadas e regras de propriedade intelectual flexíveis. Concluiu recomendando que o Brasil evite requisitos técnicos prescritivos e adote padrões e boas práticas atualizados em colaboração entre indústria, academia e reguladores, para que a regulação seja efetiva e adaptável à evolução da tecnologia.

Jacqueline Torres da ANS, destacou que o princípio central do projeto de lei deve ser a dignidade da pessoa humana. A tecnologia deve fortalecer a autonomia do paciente, apoiar os profissionais de saúde e garantir acesso e qualidade na assistência, nunca os fragilizar.

Recordou que a Constituição define a saúde como serviço de relevância pública, o que implica que, mesmo quando prestada por entes privados, permanece sob titularidade do Estado e sujeita à regulamentação, fiscalização e controle social. Sublinhou que a saúde não pode ser

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

tratada como mera mercadoria subordinada exclusivamente à lógica de mercado. Nesse sentido, defendeu que o projeto de lei inclua uma seção específica dedicada à saúde, à semelhança do que já existe para áreas como segurança pública e direitos autorais, estabelecendo disciplina normativa própria, limites claros e centralidade do interesse público.

Apresentou fundamentos essenciais para orientar o uso da inteligência artificial em saúde. O primeiro é a qualidade, segurança e eficácia, uma vez que, assim como medicamentos precisam de validação clínica, sistemas de IA destinados a diagnósticos e tratamentos devem comprovar eficácia, sensibilidade e confiabilidade, com monitoramento contínuo de falhas e distorções. O segundo fundamento é a governança de dados e a mitigação de vieses, destacando que a IA só é tão boa quanto os dados que a alimentam e que esses precisam refletir a diversidade brasileira, sob pena de falhas graves em diagnósticos, como no caso do câncer de pele em populações não representadas. O terceiro fundamento é a revisão ética, a partir da experiência brasileira consolidada no sistema CEP-Conep, que poderia inspirar a criação de comitês de bioética digital para avaliação independente e contínua dos riscos e benefícios das aplicações de IA em saúde. O quarto fundamento é a transparência e explicabilidade, garantindo que pacientes e profissionais sejam informados sempre que decisões clínicas ou administrativas forem influenciadas por IA, com direito à revisão humana e compreensão sobre a forma como a decisão foi tomada. O quinto fundamento é a centralidade do interesse público também na saúde suplementar, já que o uso da IA em rotinas administrativas de operadoras, como glosas e pagamentos, pode comprometer o acesso e a continuidade do cuidado.

A partir desses fundamentos, apresentou sugestões para o texto legislativo. No artigo 2º, propôs incluir explicitamente a promoção da saúde, da segurança e da integridade física e mental como princípio central da lei. No artigo 6º, recomendou três garantias específicas: informação prévia e destacada ao paciente quando uma decisão clínica for influenciada por IA, direito de revisão por profissional humano qualificado e consentimento informado claro para uso de dados de saúde, com possibilidade de retirada sem prejuízo ao cuidado. No artigo 7º, sugeriu a inclusão de um parágrafo que diferencie níveis de explicação: em linguagem acessível para pacientes e em maior profundidade técnica para profissionais de saúde, com documentação disponível às autoridades reguladoras. No artigo 8º, defendeu o reforço da supervisão humana, com a criação de comitês de bioética para aplicações de alto risco. No artigo 14, propôs classificar expressamente como de alto risco as aplicações de IA em diagnósticos, prognósticos, recomendações terapêuticas e decisões administrativas que impactem o acesso e a continuidade do cuidado, sobretudo em populações vulneráveis.

Sugeriu ainda a criação de um artigo específico sobre qualidade, segurança e eficácia clínica, de forma que sistemas de IA em saúde só sejam utilizados após comprovação formal de eficácia, com regulamentação técnica detalhada pela autoridade setorial. Defendeu também a inclusão de um artigo sobre governança de dados, exigindo padrões de qualidade, integridade, representatividade e mecanismos de mitigação de vieses.

Concluiu afirmando que o Brasil tem a oportunidade de ser referência mundial não apenas em legislação, mas também no desenvolvimento ético e seguro da inteligência artificial. Destacou que as proposições apresentadas não limitam a inovação, mas criam condições para que ela se desenvolva de maneira responsável, alinhando tecnologia, ética, evidência científica e governança. Enfatizou que a saúde, como bem de relevância constitucional, exige proteção especial, e que cabe ao Estado garantir que a inteligência artificial seja aplicada sempre em favor da vida, da equidade e da dignidade humana.

Sandra Ávila da Unicamp, iniciou sua exposição ressaltando a importância de refletir sobre os fundamentos da inteligência artificial e de como o tema deve ser tratado no projeto de lei em discussão. Explicou que, embora se fale em “aprendizado” de máquina, trata-se, na

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

realidade, de correlações matemáticas definidas por pessoas. São os profissionais que escolhem as tarefas, as métricas e as formas de avaliação do desempenho dos sistemas, o que torna essencial questionar sempre quem está desenvolvendo a tecnologia, para quem ela está sendo feita e de acordo com os interesses de quem.

Com base nesse raciocínio, destacou que o artigo 2º do projeto de lei, ao prever que o desenvolvimento, a implementação e o uso de sistemas de inteligência artificial devem ser centrados na pessoa humana, precisa ser melhor qualificado. Defendeu que esse princípio seja verificado em todas as etapas do ciclo de vida da tecnologia, desde a concepção até a implantação e o monitoramento dos sistemas.

Ao tratar do capítulo 3, fez críticas à redação que prevê que os agentes "poderão" realizar avaliação preliminar antes da introdução de sistemas no mercado. Em sua visão, essa avaliação não pode ser facultativa, devendo ser obrigatória, à semelhança do que ocorre na indústria farmacêutica, em que nenhum medicamento é disponibilizado sem testes rigorosos. Defendeu também que a aferição do risco deve considerar o contexto de aplicação. Um sistema de reconhecimento facial para autorizar entrada em um ambiente restrito, exemplificou, não pode ser tratado da mesma forma que um sistema de vigilância em massa, que deveria ser banido.

Apontou problemas no uso recorrente de expressões como "significativamente" ou "impacto significativo" em diversos dispositivos do projeto, por se tratarem de termos vagos que podem gerar interpretações diversas. Argumentou que, quando se trata de vidas humanas, não se deve aceitar que pequenos impactos sejam tolerados como irrelevantes. O mesmo raciocínio aplicou aos artigos que tratam de explicabilidade, transparência e riscos para grupos vulneráveis, defendendo maior precisão conceitual.

Ressaltou também a necessidade de qualificar a previsão do artigo 30, que exige a publicação de um resumo do conjunto de dados. Segundo ela, resumos excessivamente genéricos podem comprometer a compreensão da base de dados utilizada. Defendeu, portanto, que o conceito de resumo seja detalhado e que ferramentas adequadas sejam previstas para garantir a devida compreensão da composição e representatividade desses dados.

Outro ponto levantado foi a questão dos data centers. Considerou importante que o país desenvolva suas próprias infraestruturas de armazenamento, como forma de garantir soberania e territorialidade sobre os dados, mas criticou a referência a "data centers sustentáveis", avaliando que a expressão não reflete a realidade atual, já que tais infraestruturas ainda apresentam elevado impacto ambiental.

Concluiu ressaltando que o projeto de lei, ao afirmar em seu artigo 2º a centralidade da pessoa humana, precisa garantir que essa diretriz seja efetivamente observada em todos os dispositivos. Defendeu que o texto seja qualificado de forma a assegurar que a inteligência artificial beneficie toda a sociedade, sem exclusões e sem a reprodução de desigualdades.

DEBATES E CONSIDERAÇÕES FINAIS

A deputada **Soraya Santos** (PL/RJ) destacou a importância de integrar o debate sobre inteligência artificial à pauta educacional. Lembrou que 29% da população brasileira enfrenta o analfabetismo digital e alertou que essa realidade pode aprofundar desigualdades no acesso às oportunidades de trabalho e de cidadania. Defendeu, por isso, a realização de uma audiência pública conjunta com a Comissão de Educação, em razão da revisão em curso do Plano Nacional de Educação, para os próximos dez anos.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Ressaltou que a discussão precisa levar em conta não apenas o setor público, mas também o setor privado, questionando que mão de obra o país pode perder e que tipo de capacitação será necessária. Manifestou preocupação com a chamada "geração Google", que, segundo ela, perdeu a capacidade de análise de médio e longo prazo ao se apoiar em respostas imediatas. Defendeu a necessidade de direcionar de forma mais clara os investimentos em pesquisa, de modo que respondam às demandas estratégicas do país e fortaleçam os arranjos produtivos setoriais.

Destacou ainda a relevância de incluir no debate entidades representativas do comércio, da indústria e do agronegócio, de forma a alinhar a preparação da mão de obra aos setores que serão mais impactados. Ressaltou que a inteligência artificial deve ser compreendida não apenas como fornecedora de informação, mas como tecnologia que faz correções próprias, o que exige cuidado especial em áreas como a saúde, onde a aplicação envolve vidas humanas.

Reforçou a necessidade de que o projeto de lei inclua um capítulo específico sobre saúde, acompanhando a sugestão já apresentada por outros expositores. Argumentou que a saúde foi uma das primeiras áreas em que a inteligência artificial passou a ser aplicada de forma acelerada e que a regulação deve dar respostas claras sobre limites éticos e de segurança.

Por fim, chamou atenção para o impacto social da inteligência artificial sobre as mulheres. Lembrou que atualmente 51% das famílias brasileiras são chefiadas por mulheres, que ainda ocupam as posições mais vulneráveis no mercado de trabalho e, portanto, estão mais sujeitas aos impactos negativos da automação. Ressaltou que esse recorte social deve ser considerado de forma central na discussão do projeto, pois o desafio é garantir que a inovação tecnológica caminhe junto com a proteção da vida, da dignidade e da equidade.

O deputado **Aguinaldo Ribeiro** (PP/PB), observou que o debate trouxe pontos fundamentais para o aprimoramento do texto, desde as propostas do Ministério Público até as colocações sobre a participação dos entes federados, reafirmando que o processo tem sido produtivo e plural. Ressaltou que, após a conclusão das audiências públicas e a realização dos seminários regionais, terá início a etapa de redação do texto do projeto de lei, momento em que será possível consolidar e aperfeiçoar o material à luz de todas as contribuições recebidas.

Enfatizou que a centralidade da pessoa humana deve ser o princípio norteador de todo o processo, ainda que os avanços tecnológicos imponham desafios e incertezas, especialmente com a expansão da inteligência artificial generativa e seus impactos no emprego, na educação e na saúde. Destacou que o desafio do Parlamento é elaborar uma regulação que, ao mesmo tempo, assegure um ambiente favorável à inovação e imponha os limites necessários para a proteção dos direitos fundamentais.

Ressaltou que a Comissão terá de se debruçar sobre a questão dos data centers, mencionou a Medida Provisória do Redata e reforçou que a ideia é que esse debate seja incorporado ao texto no âmbito da Comissão Especial. Acrescentou que o tema da soberania nacional e da proteção dos dados é fundamental e dialoga diretamente com as observações feitas anteriormente pela professora da Unicamp.

Assinalou que a próxima fase consistirá em refinar os 80 artigos que compõem o projeto até aqui, com o objetivo de entregar um texto moderno e de vanguarda, capaz de equilibrar proteção aos cidadãos e estímulo ao desenvolvimento tecnológico.

A deputada **Adriana Ventura** (NOVO/SP) citou o caso do programa *Smart* Sampa, em São Paulo, afirmando que, embora haja vigilância, os resultados ainda não são efetivos, o que, em sua visão, não significa que a tecnologia não possa contribuir. Ressaltou que a inteligência

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

artificial, quando bem utilizada, pode apoiar o enfrentamento à criminalidade e à impunidade, devendo ser pensada como ferramenta complementar às demais políticas públicas.

Recordou que a Lei Geral de Proteção de Dados já previu uma exceção para a segurança pública, considerando que essa área não pode ser regulada nos mesmos termos que o uso comercial de tecnologia. Defendeu que o mesmo princípio deveria orientar o marco legal da inteligência artificial, de forma a não restringir demasiadamente a atuação do Estado em um cenário de crise de segurança, enquanto organizações criminosas continuam a utilizar tecnologias avançadas.

Defendeu que a Comissão avalie formas de flexibilizar as restrições do texto ou, ao menos, reservar a regulação da aplicação da inteligência artificial em segurança pública a uma legislação específica, a exemplo do que ocorreu com a LGPD Penal. Questionou os convidados, em especial ao Carlos Bruno e ao pesquisador Pablo Nunes, sobre como conciliar o uso da inteligência artificial com as demandas de segurança pública, reconhecendo que toda escolha envolve ônus e bônus. Indagou se, em alguns casos, a sensação de segurança poderia justificar uma flexibilização em relação a determinadas liberdades individuais e quais ganhos concretos poderiam ser alcançados com esse equilíbrio.

O deputado **Orlando Silva** (PCdoB/SP) comentou a intervenção da deputada Adriana Ventura e recordou que, quando da aprovação da Lei Geral de Proteção de Dados, a Câmara dos Deputados decidiu torná-la inaplicável à persecução penal e aos temas de defesa, em razão das particularidades que envolvem a proteção da privacidade e dos dados pessoais nesses contextos.

Sobre reconhecimento facial, relatou que, em audiências anteriores da comissão, foi informado por representante de empresa de inteligência artificial que os falsos positivos incidentes sobre pessoas negras decorriam da ausência desses dados nos processos de treinamento, já que informações étnico-raciais são consideradas sensíveis e protegidas. Observou que isso poderia suscitar alterações na LGPD, mas manifestou preocupação com os vieses algorítmicos já constatados, que resultam em danos graves à população negra. Afirmou que o reconhecimento facial exige maior critério e cuidado quando utilizado em políticas públicas.

Destacou sua preocupação com a grande quantidade de dados públicos coletados e tratados no país sob domínio de poucas empresas multinacionais, sem garantias de segurança. Ressaltou que é impossível falar em soberania digital sem autonomia tecnológica, o que demanda capacidade nacional de coleta, guarda e tratamento de dados. Considerou que a infraestrutura de dados é a mais crítica do debate sobre inteligência artificial e que o Brasil ainda não possui autonomia nesse campo.

Nesse contexto, mencionou a Medida Provisória do Redata, enviada pelo governo ao Congresso, que estabelece regime especial para infraestrutura de dados. Lamentou, no entanto, que a proposta tenha como foco a instalação de data centers voltados à exportação de serviços, quando o país deveria priorizar a criação de data centers com capacidade nacional instalada para atender às próprias demandas. Defendeu tratamento fiscal diferenciado para empresas que ofereçam serviços ao Brasil e incentivo ao desenvolvimento de companhias nacionais de tecnologia, de modo a garantir autonomia tecnológica e, a partir dela, verdadeira soberania digital.

O deputado **Aguinaldo Ribeiro** (PP/PB) aproveitou a intervenção do deputado Orlando Silva para registrar que, na edição da medida provisória que trata do Redata, foi reafirmado o compromisso de que o tema também seja tratado no texto do PL 2338/2023. Ressaltou que esse alinhamento é fundamental para que se garanta a construção de uma infraestrutura de dados

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

dentro de um desenho adequado, compatível com os objetivos da legislação em debate. Afirmou que há compromisso nesse sentido tanto do governo quanto do Parlamento, em especial da Comissão Especial, de modo a assegurar que a regulação contemple as demandas estratégicas relacionadas à soberania digital e ao fortalecimento da capacidade nacional no setor.

O secretário **Rodrigo Corrêa** destacou, em suas considerações finais, a necessidade de avançar na regulamentação de uma lei geral de proteção de dados na área penal. Ressaltou que o PL 2338/2023 dialoga com esse tema ao estabelecer salvaguardas no artigo 23, parágrafo primeiro, que impõe garantias para o exercício dos direitos da pessoa afetada no uso de sistemas biométricos. Reconheceu as preocupações levantadas por Pablo Nunes e por outros participantes em relação aos erros decorrentes do reconhecimento facial, salientando que é fundamental avaliar o grau de precisão desses sistemas. Lembrou, contudo, que as cidades e municípios são cada vez mais demandados a participar de esforços em segurança pública por meio do uso de câmeras e sistemas de reconhecimento facial, de modo que não se trata de uma discussão encerrada entre ser contra ou a favor da tecnologia, mas sim de fortalecer as condições de segurança e governança no seu uso.

O pesquisador **Pablo Nunes** reforçou que, embora exista a percepção de que o PL 2338/2023 possa ser excessivamente restritivo, o texto atual contém tantas exceções que, na prática, permite praticamente todos os usos de reconhecimento facial monitorados no Brasil. Alertou que a minuta é, inclusive, mais permissiva do que o AI Act europeu, legislação que inspirou parte do texto brasileiro, o que evidencia a necessidade de salvaguardas adicionais para as exceções. Reiterou que se trata de tecnologias classificadas como de risco excessivo e que, portanto, devem estar sujeitas a mecanismos robustos de governança, incluindo avaliação de impacto e auditoria. Concordou com o deputado Orlando sobre a urgência de retomar o debate da LGPD Penal, lembrando que, embora o artigo 4º da LGPD tenha previsto exceção para segurança pública, ainda falta regulação específica para o tratamento de dados nesse campo. Concluiu defendendo que, em vez de ampliar usos de alto risco, seja priorizado o investimento em tecnologias capazes de qualificar investigações, como bancos de dados voltados à identificação de armas utilizadas em homicídios, o que contribuiria para aumentar os baixos índices de resolução desses crimes.

Raúl Echeberría da ALAI, voltou ao tema do reconhecimento facial para enfatizar que o risco não está na tecnologia em si, mas nas suas aplicações. Reiterou que não é possível tratar como equivalentes, por exemplo, o uso da tecnologia para autorizar ingresso em ambientes restritos e sua utilização para vigilância de cidadãos, pois os riscos são completamente distintos. Observou que o mesmo vale para algoritmos de recomendação, que podem tanto sugerir um produto a um consumidor quanto definir critérios para filas de transplantes de órgãos, situações em que o impacto é incomparável. Defendeu, portanto, que a lei associe riscos às aplicações e não às tecnologias de maneira genérica.

Destacou que o Brasil precisa adotar uma política transversal, coordenada e com diretrizes claras para a inteligência artificial. Essa política, segundo ele, deve incluir o desenvolvimento de capacidades e talentos, apoio a startups, orientação para que órgãos públicos adotem a IA no aperfeiçoamento de serviços e políticas, além de exigir que a ação regulatória promova a inovação em vez de inibi-la.

Concluiu afirmando que a inteligência artificial deve ser tratada como ativo estratégico de desenvolvimento, justiça social e eficiência pública. Advertiu que o marco legal a ser adotado pelo Brasil será decisivo para posicionar o país como líder regional ou como mero espectador no cenário internacional. Alertou que, sem ajustes, o PL 2338/2023 poderá criar insegurança jurídica, afastar investimentos e desperdiçar a janela histórica de oportunidades.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

PODER LEGISLATIVO
Câmara dos Deputados
Grupo de Trabalho sobre Proteção de Crianças e Adolescentes em Ambiente Digital

Evento: Audiência Pública – Verificação etária, publicidade, jogos e proteção da infância

Nesta quarta-feira (24), o Grupo de Trabalho sobre Proteção de Crianças e Adolescentes em Ambiente Digital realizou audiência pública para debater o tema "**Verificação etária, publicidade, jogos e proteção da infância**".

A audiência foi convocada a partir dos Requerimentos nºs 1, 2, 3, 4 e 5/2025, de autoria da deputada **Rogéria Santos** (REP/BA), nº 8/2025, da deputada **Amanda Gentil** (PP/MA), nºs 13, 18 e 21/2025, da deputada **Laura Carneiro** (PSD/RJ), nº 19/2025, da deputada **Tabata Amaral** (PSB/SP), nºs 23, 26, 28, 30, 31 e 33/2025, da deputada **Sâmia Bomfim** (PSOL/SP), nº 35/2025, do deputado **Dr. Zacharias Calil** (UNIÃO/GO) e nº 41/2025, do deputado **Pompeo de Mattos** (PDT/RS).

Estiveram presentes na audiência:

- **Ricardo de Lins e Horta**, diretor de Segurança e Prevenção de Riscos no Ambiente Digital da Secretaria de Direitos Digitais do Ministério da Justiça e Segurança Pública (MJSP);
- **Cristiana Camarate**, superintendente de Relações com Consumidores da Anatel;
- **Dênis Rodrigues da Silva**, coordenador-geral da Secretaria de Comunicação Social;
- **Hugo Silva**, presidente da União Brasileira dos Estudantes Secundaristas (UBES);
- **Roberta Rios**, gerente de Relações Governamentais e Políticas Públicas do Google;
- **Tais Niffinegger**, gerente de Segurança e Bem-estar da Meta na América Latina;
- **Gustavo Rodrigues**, gerente de Políticas Públicas do TikTok;
- **Marilia Monteiro**, representante do Discord;
- **Luis Felipe Monteiro**, vice-presidente Global de Relações Institucionais da Unico IDTech;
- **Ergon Cugler**, membro do Conselho de Desenvolvimento Econômico Social Sustentável (CDESS);
- **Thiago Tavares**, diretor da Safernet;
- **Kelli Angelini**, representante da Ong Criança em Jogo e assessora do NIC.br;
- **Alexandre A. Gonzales**, representante da DiraCom;
- **Igor Britto**, secretário-executivo do Instituto de Defesa dos Consumidores (IDEC); e
- **Ana Potyara**, representante da ANDI – Comunicação e Direitos.

Ricardo Horta do MJSP, observou que, antes mesmo da aprovação da chamada Lei do ECA Digital, o Ministério da Justiça e Segurança Pública já vinha se preparando para o desafio de sua implementação. Recordou a participação da delegação brasileira, em dezembro de 2024, na primeira conferência ministerial global sobre a eliminação da violência contra crianças e adolescentes, realizada em Bogotá, ocasião em que o país assumiu compromissos prioritários: a construção de um protocolo nacional unificado para atendimento a crianças e adolescentes

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

vítimas de violências, inclusive as ocorridas no ambiente digital, e o desenvolvimento de soluções voltadas ao aperfeiçoamento da verificação etária em plataformas digitais.

Destacou que o ministério estruturou uma estratégia específica de prevenção à violência em ambientes digitais, com a criação de dois comitês de especialistas: um para tratar do recebimento de denúncias e outro para definir requisitos mínimos para soluções de aferição de idade. Nesse contexto, anunciou que, em 14 de outubro, na Semana da Criança, será aberta consulta pública de 30 dias, construída em parceria com a Agência Nacional de Proteção de Dados (ANPD), para apresentar proposta de sistemática de verificação de idade no Brasil.

Ressaltou que a verificação etária é uma medida fundamental, uma vez que crianças e adolescentes brasileiros acessam plataformas digitais de forma precoce, já a partir de 8 ou 9 anos, em contrariedade às próprias políticas das empresas, que estabelecem idade mínima de 13 anos. Lembrou que o Ministério da Justiça é responsável pela classificação indicativa oficial no país, que aponta restrições de acesso a plataformas digitais para menores de 14, 16 ou 18 anos.

Apontou ainda que, em função da pandemia, houve intensificação do uso precoce da internet por crianças de todas as classes sociais, o que reforça a necessidade de um ambiente digital seguro e adequado. Utilizou a metáfora do "queijo suíço", explicando que a internet precisa ser estruturada em camadas de proteção, de forma semelhante às salvaguardas aplicadas em ambientes físicos desenhados para crianças.

Elencou medidas já previstas ou em implementação, como: políticas públicas de educação midiática para conscientização sobre riscos digitais; responsabilidade empresarial e segurança por design, exigindo que produtos digitais sejam concebidos levando em conta o uso por crianças; atualização da classificação indicativa para monitorar aplicativos digitais; políticas de aferição etária; fiscalização da ANPD; e, por último, quando todas as camadas falham, a atuação da lei penal e da Polícia Federal, que já é referência no combate a crimes de abuso e exploração sexual infantil na internet.

Enfatizou que o ECA Digital estabelece que todos os usuários da internet, inclusive adultos, deverão passar pela aferição etária, constituindo camada essencial de proteção. Explicou que existem metodologias mais ou menos invasivas para essa verificação, e que o governo busca incentivar soluções que não comprometam a privacidade. Lembrou, entretanto, que o prazo de implementação no Brasil é curto, apenas seis meses, enquanto países como a União Europeia e a Austrália tiveram até três anos, mas ressaltou que a experiência internacional pode servir de referência.

Destacou a necessidade de avançar na regulamentação dos influenciadores mirins. Relatou que existem perfis de crianças de apenas 4, 5 ou 6 anos com milhões de seguidores, sem a devida fiscalização, em desacordo com as regras aplicadas ao trabalho infantil em outras áreas, como na televisão. Mencionou situações graves de publicidade ilegal voltada a crianças, inclusive em jogos de apostas, e defendeu a criação de um banco ou cadastro nacional de alvarás judiciais para permitir que plataformas digitais verifiquem a legalidade dessas atividades.

Cristiana Camarate da ANATEL, destacou a internet como uma janela de possibilidades educacionais, sociais e positivas, mas observou que seu uso requer o desenvolvimento de habilidades digitais, inclusive entre crianças e adolescentes, que cada vez mais têm acesso precoce ao mundo digital. Ressaltou a necessidade de questionar se famílias, sociedade civil, governo e indústria estão devidamente preparados para acolher esse público em um ambiente que, embora ofereça oportunidades, também traz riscos.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Entre os riscos, mencionou o bullying, que no ambiente digital ocorre de forma contínua, sem restrição de tempo, muitas vezes sem o conhecimento dos pais, que acreditam que seus filhos estão protegidos em casa. Enfatizou a importância de orientar famílias, educadores e crianças sobre como lidar com esse problema.

Nesse sentido, apresentou um projeto piloto da Anatel realizado em 2023, intitulado "Vida de Influencer", que levou 600 crianças de escolas públicas ao auditório da agência para assistir a uma peça teatral abordando, de forma lúdica, temas como bullying e a relevância do diálogo entre família e escola. O projeto recebeu prêmio internacional da Cúpula Mundial da Sociedade da Informação, concedido pela União Internacional de Telecomunicações (UIT), Unesco e outras agências da ONU.

Lembrou que a Anatel, como representante do Brasil na UIT, desenvolveu em 2020, em conjunto com governos, indústria, academia e entidades de segurança pública, um material de referência internacional sobre proteção digital, traduzido para o português em parceria com a Embaixada do Reino Unido e o CETIC.

Defendeu que o trabalho do grupo deva manter um enfoque principiológico, capaz de garantir perenidade e permitir a atuação coordenada das diversas entidades envolvidas, e alertou para a importância da harmonização internacional de medidas, de modo a evitar burlas na implementação e acompanhar a natureza global da internet e das empresas de tecnologia.

Ao tratar especificamente da verificação etária, apresentou exemplos de medidas adotadas no Reino Unido pela Ofcom, como verificação por meio de bancos, biometria, reconhecimento facial, checagem via redes de telecomunicações, uso de cartões de crédito e integração com cadastros públicos, como o Gov.br no caso brasileiro. Lembrou que, em alguns sites de jogos online, já existem práticas mais responsáveis, restringindo o acesso apenas a usuários logados. Citou ainda a atuação da ANACOM, reguladora portuguesa, que também implementa medidas nesse campo.

Finalizou destacando que a Anatel tem desenvolvido ações adicionais, como a expansão do projeto teatral para outros estados e uma parceria com a Unesco para diagnosticar as melhores formas de promover habilidades digitais tanto entre crianças quanto entre idosos, reafirmando o compromisso da agência em atuar dentro de suas competências para apoiar a construção de um ambiente digital saudável e seguro para todos.

Dênis Rodrigues da Silva, coordenador-geral da Secretaria de Comunicação Social da Presidência da República, ressaltou a aprovação da Lei nº 15.21/2025 (antigo PL 2628), destacando-a como uma das legislações mais avançadas na proteção de crianças e adolescentes no ambiente digital, mas observou que ainda há muito a ser feito, sobretudo no processo de regulamentação. Relatou a mobilização conduzida pela Secretaria de Comunicação Social desde 2023, a partir de denúncias de sociedades científicas e associações profissionais sobre o crescimento de casos de ansiedade, depressão, autolesões, suicídios, problemas de saúde física e cognitiva entre jovens, além da exposição a conteúdos nocivos e da vitimização sexual.

Apontou que o Brasil figura entre os países com maior número de crianças e adolescentes conectados, sendo que a maioria acessa a internet por meio de celulares, o que amplia riscos e dificulta o acompanhamento pelas famílias.

Descreveu a formação de um grupo de trabalho interministerial com a participação de órgãos como Justiça, Saúde, Educação e Desenvolvimento Social, além de representantes da sociedade civil, especialistas, o Conselho Nacional de Justiça e a Defensoria Pública. Em 2023,

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

além da instituição do grupo, foi aberta uma consulta pública que recebeu centenas de contribuições, e iniciou-se, com apoio da Embaixada do Reino Unido, um projeto de escuta de crianças, adolescentes, familiares e educadores.

Esse processo resultou na elaboração do guia "Crianças, Adolescentes e Telas", lançado em março de 2025, documento baseado em evidências científicas e práticas internacionais, que reúne orientações para famílias, profissionais de saúde, educadores e gestores públicos. O guia aborda desde o uso precoce de dispositivos digitais até recomendações sobre jogos, tempo de exposição, canais de denúncia, cyberbullying e mediação familiar. Também incorpora falas e recomendações das próprias crianças e adolescentes, que indicaram preocupações tanto com o comportamento dos pares quanto com o excesso de tempo de tela dos próprios adultos.

O material trata ainda do modelo de negócios das plataformas digitais, apontando a lógica da chamada "economia da atenção", em que dados e comportamentos são explorados comercialmente por meio de algoritmos e designs manipulativos, como notificações incessantes e rolagens infinitas. Segundo o expositor, essa dinâmica exige um olhar crítico sobre o papel das grandes empresas de tecnologia e seus impactos sobre a sociedade.

Explicou que o guia reúne recomendações voltadas a governos, sistemas de ensino, saúde e assistência social, além de orientações para empresas. Ressaltou que já está disponível online e será compartilhado com o grupo de trabalho.

O expositor informou que, paralelamente, o governo tem investido em políticas públicas estruturantes. Citou a criação de uma comissão específica no Ministério da Justiça para tratar da verificação etária e de um comitê intersetorial para a formulação da Política Nacional de Proteção das Crianças e Adolescentes no Ambiente Digital, coordenado pelo CONANDA em conjunto com a Secretaria Nacional dos Direitos da Criança e do Adolescente, o Ministério da Justiça e a SECOM, com a participação de outros ministérios da Esplanada.

Hugo Silva, presidente da UBES, ressaltou que a internet ocupa para a atual geração o papel de uma "praça pública", espaço central de convivência, aprendizado, construção de identidade e expressão, mas também de vulnerabilidade e exposição a riscos.

Um dos principais problemas apontados foi a ineficácia da verificação etária nas plataformas digitais. Segundo ele, o controle de idade é meramente formal, permitindo que crianças e adolescentes acessem, com um simples clique, conteúdos violentos, sexualizados ou vinculados a discursos de ódio, com reflexos negativos nas escolas e na convivência social.

Destacou ainda a publicidade disfarçada e a lógica algorítmica que mantém usuários constantemente conectados, comparando esse funcionamento a um "cassino digital", em que o engajamento excessivo gera lucros crescentes para as plataformas enquanto alimenta vícios e dependência. Ressaltou que essa dinâmica tem agravado problemas de saúde mental entre jovens, como distúrbios do sono, ansiedade e depressão, sem que haja, por parte das empresas, compromisso efetivo com a mitigação desses efeitos.

Observou que o impacto da internet insegura recai de forma mais intensa sobre crianças e adolescentes em situação de vulnerabilidade social, especialmente moradores de periferias, que têm menos acesso a bibliotecas, recursos pedagógicos e oportunidades de aprendizagem fora do ambiente digital. Para ele, a ausência de políticas públicas estruturadas amplia desigualdades, enquanto as big techs seguem lucrando com esse cenário.

Defendeu a efetiva implementação da legislação que prevê psicólogos e psicopedagogos nas escolas, de forma a garantir suporte à saúde mental dos estudantes. Propôs

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

que o Parlamento avance em três frentes centrais: assegurar a verificação etária eficaz, regulamentar a publicidade e a propaganda nas redes sociais com transparência algorítmica, e implementar a educação digital e midiática como disciplina obrigatória nas escolas brasileiras. Ressaltou que não basta proibir o uso de celulares em sala de aula sem oferecer formação adequada para que os estudantes aprendam a lidar de forma crítica e responsável com as tecnologias.

Finalizou afirmando que nenhuma empresa pode estar acima do direito de crianças e adolescentes a um desenvolvimento saudável e seguro.

Roberta Rios, do Google, ressaltou que a proteção de crianças e adolescentes online é uma prioridade para o Google há muitos anos e que avanços só são possíveis com a atuação conjunta de famílias, governos, especialistas e empresas de tecnologia. Informou que a empresa consolidou princípios orientadores para criação de políticas públicas, que serão disponibilizados ao grupo de trabalho, com foco em três dimensões: respeito às diferentes etapas de desenvolvimento, redução da exposição a riscos e responsabilização por meio da avaliação de impactos.

Destacou que a aferição etária é um dos maiores desafios do ambiente digital e deve ser tratada de forma equilibrada, respeitando a privacidade e evitando coleta excessiva de dados, preservando o acesso legítimo dos adultos e aplicando verificações proporcionais e mais intrusivas apenas em serviços de alto risco. Explicou que, nos serviços do Google, a criação de contas exige inserção da data de nascimento, que só pode ser alterada mediante verificação. Acrescentou que pais e responsáveis podem criar contas supervisionadas por meio da ferramenta Family Link, desenvolvida com participação de engenheiros brasileiros.

Relatou que, recentemente, a empresa implementou uma segunda camada de proteção com um modelo de estimativa de idade baseado em inteligência artificial e aprendizado de máquina. Esse sistema, já em uso na Europa e em fase de expansão para o Brasil, utiliza sinais associados às contas, como histórico de pesquisas ou tempo de existência da conta, para estimar se o usuário é menor de idade e, nesse caso, aplicar proteções adicionais em produtos como YouTube, Google Play, buscas e anúncios. Se houver erro de classificação, o usuário adulto pode comprovar sua identidade por verificação.

Abordou o combate ao abuso e à exploração sexual infantil, informando que o Google utiliza tecnologias de detecção automatizada, revisão humana e comparação de conteúdo com repositórios internacionais. Todo material identificado é denunciado ao National Center for Missing and Exploited Children (NCMEC), que encaminha os casos às autoridades competentes, sendo a Polícia Federal a destinatária no Brasil. Segundo dados apresentados, apenas no segundo semestre de 2024 foram realizadas mais de 2,2 milhões de denúncias ao NCMEC e enviados quase 3 milhões de registros digitais (hashes) para facilitar a detecção em outras plataformas.

Afirmou que a empresa tem compromisso com a privacidade de crianças e adolescentes, não permitindo a personalização de anúncios para menores de 18 anos com base em idade, sexo ou interesses, nem a coleta de dados pessoais ou uso de rastreadores externos em conteúdos infantis. Ressaltou que anúncios contextuais continuam possíveis, desde que não exploratórios ou inadequados.

Mencionou que o Family Link é a principal ferramenta para supervisão parental, permitindo que famílias definam limites de tempo de tela, aprovem ou bloqueiem aplicativos e acompanhem hábitos digitais, inclusive com relatórios e lembretes de pausas. Além disso, a Play Store possibilita controle parental protegido por senha, e dispositivos Android podem restringir

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

funcionalidades em horários escolares, permitindo apenas ligações ou mensagens de contatos autorizados.

Destacou ainda que a empresa produziu um guia de privacidade voltado para crianças e adolescentes, em linguagem acessível, para explicar regras de uso dos serviços. Assinalou também que foram adotadas medidas para reduzir a exposição a conteúdos de baixa qualidade, tema que será detalhado em próxima audiência por representantes do YouTube.

Deputada **Amanda Gentil** (PP/MA) apresentou emendas modificativas ao texto aprovado com três eixos prioritários: padronizar, fortalecer e suprir lacunas da verificação etária, estabelecer mecanismos que impeçam novas inscrições irregulares e garantir a eficácia dos cadastros de novos perfis.

Dirigiu questionamentos à representante do Google sobre o modelo de estimativa de idade com base em inteligência artificial, sua implementação inicial na Europa e nos Estados Unidos e a inclusão do Brasil na próxima etapa, bem como sobre o cumprimento das regras de publicidade para o público infantojuvenil, prevenindo estratégias de marketing disfarçadas em jogos e vídeos. Estendeu as perguntas a demais plataformas sobre a existência de mecanismos que impeçam o ingresso de pessoas com histórico de crimes sexuais, tanto com nome verdadeiro quanto com perfis falsos. Indagou, ainda, se há iniciativas voltadas ao enfrentamento da adultização precoce, com ações educativas em escolas públicas e privadas para apoiar crianças já afetadas.

Solicitou esclarecimentos sobre o “horário escolar” citado no Android e por que recurso semelhante não está disponível em outros sistemas operacionais. Perguntou, de forma ampla, em que medida a crescente celeridade de consumo em aplicativos como WhatsApp, Instagram e TikTok beneficia crianças e adolescentes, considerando o aumento de ansiedade e depressão, e pediu à equipe do TIC Kids Online Brasil que indique, a partir das pesquisas, quais são as principais preocupações e impactos do uso de internet na infância e adolescência. À Sociedade Brasileira de Pediatria, questionou os efeitos clínicos observados da adultização precoce. Ao presidente da UBES, solicitou a percepção dos próprios estudantes sobre riscos e soluções eficazes, reconhecendo que parte dos adolescentes ainda não percebe os impactos, enquanto outros já relatam ansiedade e aceleração.

Reforçou que o objetivo é construir, por meio do diálogo, um texto mais eficaz para o país, capaz de proteger crianças e adolescentes sem soluções que recaiam apenas sobre as famílias e sem prejuízo do debate técnico com as plataformas. Colocou-se à disposição para seguir acompanhando o tema e encaminhar contribuições para o aperfeiçoamento legislativo.

Tais Niffinegger da Meta na América Latina, apresentou as iniciativas da empresa voltadas à proteção de adolescentes no ambiente digital, ressaltando o compromisso em oferecer ferramentas que apoiem os pais na supervisão e proporcionem experiências seguras e positivas. Informou que, no início de 2025, foi lançada no Brasil a modalidade de conta de adolescente no Instagram, que integra proteções automáticas quanto a contatos, conteúdos exibidos e tempo de uso, além de permitir que os pais configurem limites diários ou horários específicos, como momentos de estudo ou refeições.

Explicou que adolescentes menores de 16 anos necessitam de permissão dos responsáveis para modificar as configurações, e que 97% dos usuários permanecem nas definições restritivas após sua ativação. Mencionou também a adoção de medidas adicionais, como a proibição de transmissões ao vivo por menores de 16 anos, salvo autorização parental, e a ampliação das regras para contas de menores de 13 anos gerenciadas por adultos, restringindo visibilidade, recomendações e interações de potenciais usuários suspeitos.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Destacou que a empresa atualizou suas políticas em 2024 para proibir contas que exibam predominantemente conteúdo de menores, além de impedir a monetização dessas contas. Apontou ainda que essas iniciativas estão em sintonia com as inovações trazidas pelo ECA Digital, que tratam de aferição etária, supervisão parental, privacidade por padrão, publicidade, monitoramento infantil, jogos, moderação de conteúdo, relatórios de transparência e governança.

Enfatizou que a Meta adota uma abordagem em múltiplas camadas para identificar a idade dos usuários, lembrando que adolescentes utilizam em média 40 aplicativos por semana, segundo estudo da Universidade de Michigan, o que torna o acompanhamento parental mais complexo. Nesse cenário, ressaltou que a nova legislação traz avanços importantes ao exigir que as lojas de aplicativos obtenham a aprovação dos pais para download, compartilhando esse sinal com os desenvolvedores. Isso permite que adolescentes sejam automaticamente direcionados à experiência adequada à idade, reduzindo a necessidade de múltiplas verificações e garantindo maior privacidade.

Concluiu destacando que o objetivo da empresa é facilitar a vida das famílias, centralizando mecanismos de controle e promovendo um ecossistema mais seguro para adolescentes, ao mesmo tempo em que reconhece a necessidade de complementaridade entre a atuação das plataformas, das escolas, das famílias e das políticas públicas.

Gustavo Rodrigues do TikTok, destacou que, embora a plataforma seja comumente associada ao público jovem, a maioria dos usuários do TikTok no Brasil tem mais de 30 anos, o que demonstra sua ampla difusão social. Ressaltou, contudo, que a prioridade absoluta da empresa é a segurança dos usuários mais jovens e apresentou as principais políticas, ferramentas e campanhas educativas adotadas nesse sentido.

Informou que a plataforma é destinada a pessoas com 13 anos ou mais, sendo a verificação etária realizada por autodeclaração no momento do cadastro, método de eficácia questionada, razão pela qual o TikTok tem buscado dialogar com especialistas, academia, sociedade civil, pares da indústria e reguladores para identificar soluções equilibradas que conciliem segurança, privacidade, inclusão digital e acesso à informação. Acrescentou que, além da autodeclaração, são utilizados sistemas automatizados de inteligência artificial capazes de identificar, a partir de sinais comportamentais, se uma conta pertence a alguém com menos de 13 anos. Nesses casos, a conta é removida.

Para adolescentes entre 13 e 18 anos, explicou que a experiência é parametrizada conforme a idade. Contas de 13 a 15 anos são privadas por padrão, não possuem acesso a mensagens diretas, não permitem download de vídeos e restringem interações como comentários apenas a amigos. Também não têm acesso a funções como dueto e costura, que ampliam a exposição a outros usuários. Todos os adolescentes têm tempo de tela limitado a 60 minutos por dia, não podem realizar transmissões ao vivo nem utilizar a função de gifts virtuais, e não recebem anúncios personalizados.

Apresentou ainda o conjunto de ferramentas de supervisão parental denominado “sincronização familiar”, que permite aos responsáveis acompanhar a experiência digital dos filhos, definindo limites de tempo de uso, intervalos de descanso e recebendo relatórios semanais sobre o tempo de tela.

Sobre as diretrizes de segurança, explicou que estas são elaboradas a partir de dois pilares: consultas a especialistas de áreas como medicina, psicologia, pedagogia e direito, e diálogos com comunidades diretamente afetadas, como adolescentes e grupos alvo de discurso

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

de ódio. Mencionou a existência de um conselho multidisciplinar no Brasil que assessora a empresa e destacou como inovação global o Conselho de Jovens do TikTok, formado por adolescentes de 15 a 18 anos de diferentes países, inclusive do Brasil, que participam regularmente da formulação de políticas e ferramentas.

Apresentou os esforços educativos desenvolvidos pela empresa, ressaltando a necessidade de capacitar as famílias para utilizar as ferramentas disponíveis. Citou a parceria com o Cartoon Network, por meio de episódios do desenho *Irmão do Jorel* que abordaram, de forma lúdica, o uso de mecanismos de supervisão parental, a campanha anual "Por uma Internet Segura", em fevereiro, que conta com a participação de organizações da sociedade civil e já alcançou 380 milhões de visualizações e mais de 26 milhões de usuários, e a capacitação realizada em parceria com o ICMEC para policiais das 27 unidades da federação no combate a crimes sexuais contra crianças na internet.

Por fim, relatou a colaboração com influenciadores e organizações como Exodus Road e Instituto Liberta em ações de conscientização sobre o tráfico humano e crimes sexuais online, reafirmando o compromisso do TikTok em atuar de forma contínua para oferecer um ambiente digital mais seguro para crianças e adolescentes.

Marília Monteiro do Discord, apresentou uma breve introdução sobre o Discord, explicando que se trata de um serviço de comunicação, e não de uma rede social tradicional. Destinada a maiores de 13 anos, a plataforma conecta pessoas em tempo real por voz, vídeo ou texto, sendo utilizada principalmente por quem joga online — mais de 90% dos usuários estão no Discord jogando juntos. Diferencia-se das redes sociais por não possuir algoritmos de recomendação, feeds infinitos, contagem de curtidas ou estímulos à viralização de conteúdo. A interação é baseada em conversas espontâneas, seja em mensagens privadas, em grupos restritos de até 10 pessoas, ou em espaços comunitários denominados servidores, que funcionam como salas digitais organizadas em canais temáticos.

Destacou que o modelo de monetização é distinto, baseado em parcerias relacionadas ao universo dos jogos e em assinaturas pagas, como o serviço Nitro, sem depender de publicidade direcionada. Ao abordar a segurança de adolescentes, informou que a plataforma adota controles em três camadas: aqueles oferecidos diretamente ao usuário, as diretrizes de comunidade e a moderação da plataforma, além da moderação feita pela própria comunidade e por parceiros de segurança.

Entre os recursos voltados a adolescentes, citou o Assistente de Segurança, que aplica filtros automáticos para bloquear ou borrar conteúdos sensíveis, como imagens de teor sexual ou gráfico. Mencionou também alertas de segurança, que orientam os usuários a rejeitarem contatos potencialmente indesejados, e mecanismos como advertência e ignorar, que aumentam a transparência e permitem bloquear interações de outros usuários.

Apresentou a Central da Família, ferramenta que possibilita a integração da conta do adolescente com a de um responsável, permitindo o monitoramento da experiência, do tempo de uso, das interações e dos servidores acessados. O responsável recebe relatórios semanais por e-mail e pode consultar o Guia do Guardião, que explica como utilizar os recursos da plataforma e orienta sobre diálogos com adolescentes em situações sensíveis.

Enfatizou que o Discord possui diretrizes próprias de comunidade, faz moderação ativa e coopera com autoridades em diferentes níveis no Brasil. Reafirmou que a segurança dos usuários é um processo contínuo, que envolve aprimoramentos internos, parcerias com redes de segurança e a adoção das tecnologias mais avançadas, colocando a plataforma à disposição

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

para colaborar com o grupo de trabalho e com o governo brasileiro na implementação e regulamentação do ECA Digital.

Luis Felipe Monteiro da Unico IDTech, enfatizou que a Unico não é uma plataforma de conteúdo, mas um provedor de soluções de segurança e confiabilidade digital, com forte compromisso com a privacidade, em conformidade com a Lei Geral de Proteção de Dados e legislações equivalentes em outros países. Ressaltou que, apesar da existência de diversas ferramentas de controle parental, muitas famílias não as utilizam ou desconhecem seu funcionamento, o que reforça a necessidade de ação do Estado para garantir clareza e eficácia.

Apresentou um panorama do ecossistema digital, composto por sistemas operacionais, lojas de aplicativos, plataformas e conteúdos, explicando que os riscos para crianças e adolescentes estão concentrados na camada do conteúdo, enquanto a complexidade de implementação de verificações é maior nos níveis mais estruturais. Defendeu que, por essa razão, soluções técnicas precisam ser pensadas de acordo com cada contexto.

Ao abordar as tecnologias disponíveis, diferenciou métodos de estimativa de idade e de verificação de idade. No primeiro grupo, citou soluções como análise biométrica, verificação por atributos em bases públicas, uso de cartões de crédito, comprovação social e análise comportamental, reconhecendo que podem ser úteis em situações de baixo a médio risco, mas com margens de erro que comprometem a precisão quando se trata de adolescentes próximos da idade mínima. Já as tecnologias de verificação de idade oferecem resultados exatos, comparáveis à checagem de documentos físicos em estabelecimentos comerciais, e podem ser aplicadas digitalmente com recursos como biometria, identidade digital e mecanismos de *zero knowledge proof*, que confirmam se o usuário está acima ou abaixo de determinada idade sem expor dados pessoais adicionais.

Por fim, ressaltou que diferentes tipos de plataformas demandam soluções específicas, exemplificando com aplicativos de delivery que já exigem cadastros identificados, e redes sociais, que em geral não possuem tais informações.

Ergon Cugler do CDESS, apontou que os modelos de negócios das grandes plataformas priorizam conteúdos que geram maior engajamento, ainda que nocivos, citando como exemplo relatórios que mostram o direcionamento de conteúdos de automutilação a adolescentes e a existência de comunidades de ideologia nazista no Telegram, acessíveis sem filtros de idade. Reconheceu os avanços tecnológicos apresentados pelas empresas, mas alertou que eles surgem após anos de omissão.

Defendeu que a segurança online deve ser garantida sem comprometer a privacidade dos usuários e que a verificação etária não deve se transformar em verificação de identidade. Para isso, apresentou recomendações técnicas, destacando experiências internacionais que demonstraram ineficácia de diversos métodos: autodeclaração de idade, uso de cartão de crédito como prova de maioridade, upload de documentos de identidade em sites, biometria facial e análises comportamentais. Explicou que todos esses métodos são passíveis de fraude ou apresentam riscos de privacidade, além de falharem em situações de limiar, como distinguir adolescentes de 12 e 13 anos ou de 17 e 18 anos.

Propôs princípios para um sistema mais seguro: resistência contra fraudes, fornecimento apenas da informação essencial ("maior de 18 anos, sim ou não"), sem coleta excessiva de dados, dupla confidencialidade, de modo que nem o sistema público nem a plataforma conheçam informações além do necessário, auditoria dos processos e não dos usuários, possibilidade de revogação do consentimento, e verificação online sem armazenamento permanente de documentos, utilizando mecanismos temporários de autenticação.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Enfatizou que a verificação etária deve ser aplicada especialmente a ambientes nocivos, como sites de pornografia, jogos de azar e conteúdos violentos, evitando barreiras excessivas para acesso a conteúdos educativos ou informativos. Reforçou que a verificação de idade é apenas uma etapa, que precisa estar associada ao acompanhamento parental e, sobretudo, à moderação de conteúdo eficaz, pois de nada adiantará restringir a idade de acesso se adolescentes continuarem expostos a materiais nocivos já dentro das plataformas.

Thiago Tavares da Safernet, destacou que a instituição mantém um canal de denúncias, um canal de orientação a vítimas, realiza cursos de conscientização e opera, em parceria com o Ministério da Justiça, o canal Escola Segura. Ressaltou que a Safernet integra redes internacionais, como o InHope, o InSafe e o Child Helpline International, que conectam canais de ajuda em diversos países.

Destacou a colaboração com a Polícia Federal e o Ministério Público Federal, com quem mantém termos de cooperação, resultando em operações e prisões em todo o país. Apenas em 2024, mais de mil investigações foram instauradas a partir de denúncias compartilhadas pela organização. Citou também a parceria estratégica firmada recentemente com o Conselho Nacional do Ministério Público (CNMP), ampliando o compartilhamento de informações para todo o Ministério Público brasileiro.

Chamou atenção para a **necessidade de implementação adequada dos artigos 10 a 15 da Lei 15.211/2025**, referentes à verificação etária. Diferenciou os conceitos de autodeclaração, estimativa de idade e verificação efetiva, alertando que cada método tem vantagens e fragilidades. Ressaltou que a escolha de tecnologias precisa equilibrar segurança com proteção da privacidade, sob risco de gerar externalidades negativas, como falhas na identificação ou vazamentos de dados. Citou como exemplo as limitações do reconhecimento facial, que pode ser burlado por técnicas de inteligência artificial, além de apresentar riscos de exclusão de pessoas com deficiência.

Mencionou a experiência da lei que regulou as apostas online, que restringiu o cadastro de menores, mas previu exclusivamente o reconhecimento facial como método de verificação, o que demonstra riscos de obsolescência e ineficácia quando apenas uma técnica é adotada. Recomendou que a legislação brasileira evite amarrar-se a métodos únicos e preserve flexibilidade para acompanhar a evolução tecnológica.

Apresentou dados sobre a intensificação de problemas de saúde mental entre adolescentes, destacando relatório do TCU que aponta crescimento abrupto a partir de 2023, coincidindo com a popularização das plataformas de apostas. Defendeu que os recursos arrecadados com multas e sanções relacionadas a esse setor sejam melhor destinados a políticas de saúde e proteção infantojuvenil.

Por fim, reforçou a importância da prevenção e da educação. Relatou que a Safernet, em parceria com o MEC e o governo do Reino Unido, oferece disciplina de cidadania digital aplicada em mais de 800 escolas, alcançando 100 mil estudantes e mil professores. Reiterou que a efetividade da proteção depende não apenas de novas normas, mas também da implementação das leis já existentes, acompanhada de conscientização de famílias e responsáveis.

Kelly Angelini do NIC.br, recordou que, em 2010, o NIC.br começou a receber ofícios do Ministério Público relatando crimes graves contra crianças no ambiente digital, como casos de abuso sexual filmados e divulgados em redes sociais. A partir desses episódios, o NIC.br e o CGI.br decidiram desenvolver materiais educativos, como cartilhas e guias, voltados para

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

crianças, adolescentes, pais, educadores e pessoas idosas, com o objetivo de promover conscientização e capacitação.

Mencionou que, há dez anos, o NIC.br e o CGI.br realizam o simpósio "Crianças e Adolescentes na Internet", consolidado como principal espaço de debate sobre proteção infantojuvenil no ambiente digital. Ressaltou, ainda, que o CGI.br contribuiu com a elaboração técnica do ECA Digital, por meio de nota técnica que buscou garantir maior precisão conceitual à lei, assim como já havia atuado em marcos regulatórios anteriores, como o Marco Civil da Internet e a LGPD.

Destacou a relevância das pesquisas do CETIC.br, como a TIC Kids Online e a TIC Educação, que fornecem dados essenciais para formulação de políticas públicas. Citou como exemplo que 83% das crianças e adolescentes entre 9 e 17 anos possuem perfis em redes sociais, apesar da restrição etária de 13 anos presente nos termos de uso das plataformas. Apontou também que 70% dos jovens de 11 e 12 anos e 60% das crianças de 9 e 10 anos já estão nessas redes, muitas vezes expostas a conteúdos inadequados. Recordou episódios recentes de mortes de crianças no Brasil relacionadas a desafios perigosos difundidos em redes sociais, como o "desafio do aerossol".

Informou que a aprovação do ECA Digital (Lei 15.211/2024) representa um marco fundamental na atualização da proteção prioritária prevista na Constituição e no Estatuto da Criança e do Adolescente. Contudo, advertiu que a implementação da lei exigirá superar desafios técnicos, capacitar famílias, escolas e sociedade e promover campanhas de conscientização.

Por fim, em resposta a questionamento da deputada **Amanda Gentil** (PP/MA), destacou que as pesquisas do CETIC apontam dados positivos, como o uso educacional das tecnologias, mas também revelam riscos significativos, como exposição a violências, discriminação e discurso de ódio.

Alexandre Armes Gonzalez do Diracom, informou que a Coalizão Direitos na Rede está realizando ciclos de encontros sobre o tema, comprometendo-se a encaminhar contribuições formais escritas ao grupo de trabalho. Ressaltou que a discussão sobre verificação etária se insere em um contexto mais amplo da governança global da internet, que desde o início do século XXI vem sendo marcada pela ascensão de grandes plataformas digitais baseadas em modelos de negócio que naturalizam a vigilância e o monitoramento da vida cotidiana. Nesse sentido, a regulamentação voltada à proteção de crianças e adolescentes ajuda a desnaturalizar essas práticas e a estabelecer novos parâmetros de responsabilidade.

Observou que o ECA Digital traz dispositivos importantes, como o artigo 11, que prevê a atuação do poder público como regulador ou certificador de soluções técnicas de verificação de idade, assegurando a participação social por meio de consultas públicas, e o artigo 34, que veda a implementação de mecanismos de vigilância genérica e indiscriminada. Para ele, esses artigos desenham uma arquitetura de governança que deve evitar violações à privacidade e ao tratamento excessivo de dados pessoais.

Defendeu que a verificação etária não deve ser confundida com verificação de identidade, destacando a necessidade de métodos que permitam confirmar apenas a faixa etária sem que dados biográficos ou biométricos sejam coletados ou armazenados por diferentes serviços. Como alternativa, sugeriu a adoção de certificados criptografados que indiquem apenas se o usuário é maior ou menor de determinada idade, preservando o anonimato e reduzindo riscos de vazamentos.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Apontou ainda a possibilidade de o Brasil assumir protagonismo internacional nesse debate, assim como ocorreu em 2013 e 2014, ao estabelecer parâmetros de referência na governança da internet. Defendeu que soluções públicas, ou sem fins lucrativos, devem ser priorizadas, de forma a evitar que a verificação etária se torne mais um mecanismo de concentração de mercado nas mãos de grandes empresas. Para ele, universidades e institutos de pesquisa nacionais têm condições de contribuir significativamente nesse processo.

Igor Britto do IDEC, ressaltou a importância de somar esforços da sociedade civil para pressionar pela implementação efetiva do ECA Digital e de futuras normas voltadas à proteção de crianças e adolescentes no ambiente virtual. Apresentou a perspectiva do IDEC como maior associação de consumidores do país, com quase 40 anos de atuação em defesa do interesse público frente a poderes privados e públicos.

Destacou que crianças e adolescentes sempre foram o alvo mais estratégico do marketing, desde os primórdios da televisão, e que a internet apenas potencializou esse assédio, expondo-os de forma massiva a publicidades disfarçadas de conteúdo e entretenimento. Advertiu que qualquer estratégia tecnológica adotada para verificação etária deve considerar os riscos de coleta e vazamento de dados, especialmente em um país marcado por recorrentes falhas de segurança e escândalos envolvendo informações pessoais.

Manifestou preocupação com propostas que envolvem biometria facial ou coleta de dados sensíveis como requisito para a verificação de idade, avaliando-as como práticas invasivas, discriminatórias e perigosas, que podem ampliar a vulnerabilidade dos consumidores e gerar riscos de exclusão digital. Defendeu que a verificação etária não pode ser confundida com identificação pessoal, devendo assegurar anonimato e limitar a coleta de dados.

Também alertou para os riscos da chamada captura corporativa dos processos tecnológicos, quando grandes empresas tentam impor suas próprias soluções como padrão internacional, sem debate democrático. Afirmou que a proteção da infância deve prevalecer sobre interesses comerciais e estratégias de mercado.

Entre as reivindicações apresentadas, destacou: auditoria pública dos sistemas de verificação etária, preferência pelo uso de software livre, mecanismos transparentes de governança, respeito à proporcionalidade entre riscos dos serviços e robustez das medidas, e responsabilização direta das plataformas que utilizam algoritmos de segmentação comercial, para que garantam a moderação, a transparência e a proteção integral de crianças e adolescentes.

Concluiu afirmando que a proteção da infância e a preservação da privacidade não são objetivos conflitantes, mas complementares, que devem caminhar juntos na construção de soluções eficazes.

Ana Potiara da ANDI, observou que, por muito tempo, as empresas ficaram de fora do debate sobre direitos digitais e proteção da infância, recusando-se a assumir responsabilidades, mesmo quando seus próprios termos de uso já indicavam que crianças não deveriam acessar determinadas plataformas. Lembrou que experiências como a das casas de apostas online demonstram a fragilidade da autorregulação, já que adolescentes conseguem burlar sistemas de cadastro com CPFs falsos ou de terceiros.

Ressaltou que o ECA Digital trouxe avanços significativos, entre eles a regulamentação da verificação etária, a proibição do perfilamento e da análise emocional de crianças para fins publicitários, e medidas importantes em relação a jogos eletrônicos, como a vedação das

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

chamadas *loot boxes* e maior atenção a chats, espaços em que frequentemente ocorrem situações de exploração e aliciamento.

Defendeu que o Brasil precisa desenvolver um mecanismo nacional próprio de verificação de idade, adaptado às particularidades do país, e observou que o Ministério da Justiça já conduz iniciativas nesse sentido. Alertou que, apesar dos avanços, será necessário monitorar a aplicação da lei a partir de sua entrada em vigor, avaliando se os instrumentos adotados pelas empresas serão eficazes.

Enfatizou também a urgência de políticas de educação midiática voltadas não apenas a crianças e adolescentes, mas a toda a sociedade, em especial pais, mães e responsáveis, que muitas vezes não dominam as ferramentas de controle parental. Para ela, o grande desafio será alinhar a população nesse processo de conscientização e capacitação.

Por fim, apontou três pontos estratégicos que o grupo de trabalho deve enfrentar: a regulamentação do trabalho infantil em atividades digitais, incluindo influenciadores e youtubers mirins, a incorporação da proteção de crianças e adolescentes no debate legislativo sobre inteligência artificial, e o fortalecimento de medidas que consolidem a aplicação do ECA Digital.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

PODER LEGISLATIVO
CÂMARA DOS DEPUTADOS
Grupo de Trabalho sobre Proteção de Crianças e Adolescentes em Ambiente Digital

Audiência Pública: Prevenção de violências e combate aos riscos à vida no ambiente online

O Grupo de Trabalho sobre Proteção de Crianças e Adolescentes em Ambiente Digital da Câmara dos Deputados realizou, nesta terça (23), sua primeira audiência pública. Na sessão presidida pela deputada **Rogéria Santos** (REP/BA) estiveram presentes:

- **Mayara Silva de Souza**, chefe de gabinete da Secretaria Nacional dos Direitos da Criança e do Adolescente do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA);
- **Nahema Nascimento**, secretária-executiva do Comitê Nacional de Enfrentamento à Violência Sexual contra Crianças e Adolescentes;
- **Lucas Lopes**, secretário-executivo na Coalizão Brasileira pelo Fim da Violência contra Crianças e Adolescentes; e
- **Paula Alegria**, assessora de advocacy do Plan International Brasil.

Mayara de Souza iniciou sua intervenção esclarecendo que, embora seja suplente no Conanda, naquele momento falava em nome do Ministério dos Direitos Humanos e da Cidadania. Destacou a importância da sanção recente do chamado "ECA Digital" (Lei nº 15.211/2025), classificando-o como um marco histórico na proteção de crianças e adolescentes no ambiente digital. Reforçou que a realização da audiência era fundamental para consolidar esse novo cenário normativo e para aproximar o Parlamento, o Executivo e a sociedade civil em torno de medidas efetivas de proteção.

Em seguida, apresentou dados que revelam a alta exposição de crianças e adolescentes à internet no Brasil: 93% entre 9 e 17 anos acessam a rede regularmente, em todas as classes sociais. Destacou que o problema não é o uso em si, mas os riscos associados ao uso excessivo e inadequado, como impactos na saúde e no desenvolvimento. Enfatizou que a Constituição Federal, no art. 227, atribui corresponsabilidade à família, à sociedade e ao Estado, e lembrou que pesquisas indicam que a maioria da população acredita que as empresas de tecnologia fazem menos do que deveriam para proteger esse público.

Listou as principais estratégias governamentais em andamento, citando o Disque 100 como canal de denúncias que já abarca casos digitais; o Sistema de Informação para a Infância e Adolescência – Conselho Tutelar (SIPIA), com milhares de usuários ativos em conselhos tutelares; a Revisão do Plano Decenal Nacional de Enfrentamento da Violência Sexual e diagnósticos acadêmicos, como a pesquisa sobre violência sexual online em parceria com universidades brasileiras. Além disso, apontou a importância de formações continuadas para conselheiros tutelares e profissionais que atuam diretamente com crianças e adolescentes, e destacou resoluções recentes do Conanda que tratam de direitos digitais e da construção de uma política nacional para o ambiente digital.

Por fim, listou iniciativas interministeriais, como o Guia de Telas para Crianças e Adolescentes, a Estratégia Brasileira de Educação Midiática (SECOM), a estratégia Crescer em Paz (MJSP) e ações da Polícia Federal, além de leis recentes que criminalizam bullying e cyberbullying. Reforçou a necessidade de nomear violências específicas — *como racismo ou discriminação contra pessoas com deficiência* — em vez de tratá-las genericamente como "bullying". Encerrando, convidou todos a participarem da consulta pública que subsidiará a

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital, defendendo que o processo seja inclusivo e reflita a diversidade das infâncias e adolescências brasileiras.

Nahema Nascimento da Rede de Governança da Internet, enfatizou a relevância do debate sobre prevenção de violências no ambiente digital, situando sua fala no campo das tendências mais recentes em plataformas digitais, em especial os chatbots personalizados com inteligência artificial generativa (IA-G). Ela explicou que esses "companheiros de conversação" vêm crescendo em popularidade entre adolescentes, inclusive no Brasil, onde pesquisas já apontam seu uso por estudantes do ensino médio em atividades escolares. Chamou a atenção para relatórios de segurança digital que identificam aumento expressivo nas buscas relacionadas a IA por crianças e adolescentes, refletindo a rápida disseminação desses recursos.

Em seguida, ressaltou os riscos associados a esse fenômeno, citando exemplos internacionais como o caso do Character AI, adquirido pela Google via licenciamento, e que já foi alvo de processos judiciais após denúncias de exploração da vulnerabilidade de adolescentes que resultaram em suicídios. Relacionou tais ocorrências ao que chamou de **"**efeito ELIZA**"** — *tendência das pessoas a humanizarem programas de computador que simulam diálogos, atribuindo-lhes sentimentos ou intenções*. Para ela, esse processo de "ilusão digital" coloca em risco a saúde mental, em especial de crianças e adolescentes, dada sua maior ingenuidade e fragilidade cognitiva.

Avançando em sua análise, apontou que é fundamental regular a indústria da IA, responsabilizando startups e *big techs* pelo desenvolvimento e comercialização de chatbots inseguros. Defendeu a necessidade de uma **"**cultura do direito à realidade**"** em ambientes digitais, para que a fronteira entre fantasia e vida real seja clara, especialmente no contato de crianças com máquinas que simulam interações humanas. A seu ver, fundos de investimento e empresas não podem lucrar irresponsavelmente às custas do bem-estar infantil, devendo ser obrigados a demonstrar que seus produtos beneficiam crianças antes da implantação no mercado.

Por fim, propôs três mudanças para o debate público sobre IA e infância: (i) reconhecer que crianças interagem com IA mediadas por familiares e professores; (ii) priorizar a proteção da plasticidade cognitiva, assegurando que o desenvolvimento seja saudável; e (iii) exigir que empresas provem os benefícios de suas tecnologias antes da comercialização. Também reforçou a importância de avaliações de risco, classificação etária, design participativo com crianças e convergência entre ética da IA, psicologia do desenvolvimento e legislação. Encerrando, destacou que o Brasil, com seu modelo multissetorial de governança da internet, tem potencial de liderança global, mas precisa ajustar assimetrias e integrar o debate sobre IA de forma crítica e responsável.

Karina Figueiredo do Comitê Nacional de Enfrentamento à Violência Sexual contra Crianças e Adolescentes, observou que o grupo é responsável pela campanha "Faça Bonito, Proteja Nossas Crianças e Adolescentes", além de integrar a rede internacional Ecpat Brasil. Ressaltou que a pauta do enfrentamento à exploração sexual, incluindo a mediação por tecnologias, voltou à cena mundial após um período de relativa invisibilidade desde o 3º Congresso Mundial realizado no Brasil em 2008.

Destacou avanços conceituais, como a substituição do termo pornografia infantil por exploração sexual no contexto digital ou abuso e exploração sexual online, mudança que considera fundamental para consolidar o debate e dar precisão à linguagem. Essa atualização fortalece a luta contra as violências sexuais, sobretudo porque adequa a terminologia à gravidade

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

do problema e ao reconhecimento das crianças e adolescentes como sujeitos de direitos no ambiente digital.

Na sequência, chamou atenção para a dimensão internacional da problemática, lembrando que a exploração sexual mediada por tecnologias não é apenas uma questão nacional, mas global, exigindo cooperação entre países e fortalecimento das redes de proteção. Ressaltou que o Brasil tem papel de destaque nesse cenário por já ter sediado eventos de referência e por contar com uma rede articulada de enfrentamento, mas alertou para a necessidade de recolocar o tema no centro das agendas multilaterais.

Por fim, reforçou que a luta contra a exploração sexual digital precisa de articulação entre sociedade civil, órgãos governamentais e instâncias internacionais. Defendeu o fortalecimento de campanhas de conscientização, políticas públicas mais efetivas e a atualização constante da legislação frente aos avanços tecnológicos. Encerrando, afirmou que a causa é urgente e deve ser tratada como prioridade absoluta para a proteção de crianças e adolescentes, tanto no Brasil quanto no cenário internacional.

Lucas Lopes da Coalizão Brasileira pelo Fim da Violência contra Crianças e Adolescentes, concentrou-se na análise legislativa e institucional sobre a proteção de crianças no ambiente digital. Iniciou destacando a importância do plano de trabalho do grupo de trabalho que, ao segmentar a discussão em eixos – *riscos digitais, privacidade, saúde, governança, e demais* –, garante maior coerência legislativa. Ressaltou que esse método é compatível com a boa técnica legislativa, pois evita dispersão e facilita a construção de normas mais consistentes.

Apresentou o trabalho da Coalizão em parceria com o Fundo das Nações Unidas para a Infância (UNICEF) e outras organizações, que consistiu em mapear 238 projetos de lei em tramitação no Congresso Nacional sobre o tema. Desses, 61% se alinham aos princípios da proteção integral, mas 33% apresentam riscos ou falhas de técnica legislativa, e 5% não puderam ser plenamente avaliados. Entre os problemas identificados, estão tipificações penais sem estudos de impacto, conceitos jurídicos indeterminados em propostas de remoção de conteúdo e lacunas em relação à Lei Geral de Proteção de Dados (LGPD) e ao papel da Agência Nacional de Proteção de Dados (ANPD).

Alertou que, apenas em 2025, foram apresentados 124 novos projetos, dos quais 37% carregam riscos à proteção integral, revelando a aceleração da pauta parlamentar. Nesse cenário, reforçou a necessidade de "racionalização normativa", de modo a evitar sobreposição de normas, fragmentação de competências e insegurança jurídica. Lucas defendeu que a recente o chamado "ECA Digital" deve servir como marco de referência: novos projetos devem consolidar e preencher lacunas desse marco, sem criar contradições ou estruturas paralelas.

Por fim, apresentou recomendações preliminares: integração de fluxos de denúncia no eixo de riscos digitais; reforço da proibição de perfilamento e publicidade direcionada no eixo de privacidade; diretrizes gerais de bem-estar digital no eixo de saúde; e prevenção da sobreposição de governança no eixo institucional. Concluiu defendendo que o Parlamento aprove a consolidação legislativa com base na técnica, coerência e prioridade constitucional à infância, transformando quantidade de proposições em qualidade normativa. Sua fala foi marcada pelo alerta contra a aprovação apressada de normas mal estruturadas e pela defesa de uma harmonização sistêmica em prol da proteção de crianças e adolescentes.

Paula Alegria da Plan International Brasil, apresentou a trajetória da entidade destacando sua presença há mais de 25 anos no país, com projetos em mais de 130 comunidades, especialmente no Maranhão, Piauí, Bahia e São Paulo. Ressaltou que a organização atua em rede com movimentos sociais e tem como missão romper ciclos de

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br

violência contra crianças e adolescentes, com especial atenção às meninas, que vivem vulnerabilidades desproporcionais nos ambientes digitais.

Ela enfatizou que meninas e meninos experimentam os espaços digitais de forma distinta, pois as jovens são as principais vítimas de violências sexuais online. Trouxe dados preocupantes: globalmente, 650 milhões de meninas e mulheres já sofreram algum tipo de abuso sexual online, e no Brasil, 54% de crianças e adolescentes afirmam já ter vivenciado esse tipo de violência — *o que corresponde a mais de 9 milhões de pessoas*. Além disso, 94% delas não sabem como reagir em situações de risco, evidenciando falhas nos mecanismos de apoio e denúncia.

Em sua exposição, apresentou os resultados de uma pesquisa da Plan International em parceria com a CNN, realizada em nove países, incluindo o Brasil, que ouviu meninas diretamente sobre suas vivências online. Entre os achados, 75% relataram experiências prejudiciais, quase metade recebeu imagens sexuais indesejadas e mais de um terço mensagens de teor sexual impróprio. As respondentes apontaram como prioridades para mudar essa realidade: letramento digital, melhor orientação de familiares e medidas legais mais fortes e eficazes. Também cobraram das empresas de tecnologia maior responsabilidade e respostas mais rápidas em denúncias.

Por fim, reiterou as recomendações das próprias meninas para enfrentar os riscos: promoção da conscientização, ampliação da educação digital e responsabilização efetiva de agressores e plataformas. Defendeu iniciativas nacionais de segurança online lideradas pelo governo, em parceria com escolas, famílias, setor privado e sociedade civil, com foco em saúde mental, igualdade de gênero e criação de espaços seguros de diálogo. Concluiu que a proteção integral no ambiente digital exige protocolos claros, fluxos bem definidos e compromisso político, lembrando que sem tratar o abuso online como prioridade, o país continuará repetindo histórias de violência que poderiam ser evitadas.

DEBATES

A deputada **Laura Carneiro** (PSD/RJ) destacou a relevância do GT e sua função central ao ouvir especialistas e representantes da sociedade civil. Enaltecendo a importância de se debater a proteção de crianças e adolescentes no ambiente digital, a parlamentar evidenciou sua preocupação com a interface entre tecnologia, infância e segurança.

Na sequência, deputada **Rogéria Santos** (REP/BA) destacou que o Parlamento precisa se alinhar às demandas emergentes da sociedade, em especial diante do crescimento das violências online. Já a deputada **Antônia Lúcia** (REP/AC) lamentou a ausência de alguns autores dos requerimentos que deram origem à audiência, mas reforçou a importância do debate. Anunciou que está coletando assinatura para PEC para criação de delegacias especializadas em crimes de violência sexual contra crianças e adolescentes no ambiente digital, comparando sua relevância às delegacias da mulher na luta contra o feminicídio.

Setor Comercial Norte, Quadra 1, bloco F, Ed. America Office Tower
salas 125 a 131, Asa Norte, Brasília-DF - CEP: 70711-905
+55 (61) 3327 1289 | www.foco-relgov.com.br | foco@foco-relgov.com.br