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

Audiência Pública: Reforma da Legislação Penal, Processual Penal e repressão aos crimes cibernéticos contra crianças e adolescentes

O Grupo de Trabalho sobre Proteção de Crianças e Adolescentes em Ambiente Digital realizou, na terça-feira (21), sua oitava audiência pública na Câmara dos Deputados. Na sessão presidida pela deputada **Rogéria Santos** (REP/BA) estiveram presentes:

- **George Neves Lodder**, procurador da República no Distrito Federal e membro do Grupo de Atuação Especial no Combate aos Crimes Cibernéticos e aos Crimes praticados mediante o uso de Tecnologias de Informação (GACCTI);
- **Joao Paulo de Carvalho da Costa**, promotor de Justiça do Ministério Público da Bahia e coordenador do Núcleo de Combate aos Ilícitos Cibernéticos (NUCCIBER);
- **Luana Tavares**, fundadora do Instituto Nacional de Combate ao Cibercrime (INCC);
- **Felipe Rodrigues**, especialista em Inteligência Artificial.

George Neves Lodder da PRDF/GACCTI, destacou a importância de fortalecer a legislação e a cooperação internacional no enfrentamento aos crimes de abuso sexual infantil no ambiente digital. Segundo ele, o Brasil possui um arcabouço penal robusto, com o Estatuto da Criança e do Adolescente (ECA) e leis correlatas, mas ainda carece de atualização em dois pontos principais.

O primeiro é a criação de um tipo penal específico para abarcar imagens realísticas produzidas por inteligência artificial que simulem crianças em contextos sexuais, uma lacuna que o país mantém mesmo sendo signatário da Convenção de Budapeste sobre crimes cibernéticos. O segundo ponto é o aprimoramento da legislação processual, de modo a permitir maior agilidade e segurança na preservação e obtenção de provas digitais, muitas vezes armazenadas em servidores localizados fora do Brasil.

Explicou que a Convenção de Budapeste trouxe instrumentos modernos de cooperação jurídica internacional, mas sua aplicação plena ainda depende de ajustes internos, especialmente na definição de tipos penais e de regras processuais mais claras. Abordou, como exemplo, a importância da preservação imediata de provas por provedores de internet antes mesmo da autorização judicial formal, para evitar a perda de informações essenciais às investigações. Também defendeu a ampliação do conceito de "dados cadastrais" previsto em lei, argumentando que informações técnicas como endereços de IP e cookies são fundamentais para identificar criminosos que tentam ocultar sua identidade no ambiente digital.

Mencionou ainda o Segundo Protocolo da Convenção de Budapeste, atualmente em atualização na Europa e já adotado por países como Chile e Costa Rica, que prevê mecanismos mais céleres de cooperação, como o contato direto entre autoridades e provedores internacionais em situações de urgência e a formação de equipes conjuntas de investigação. Em suas considerações finais, afirmou que o sistema penal brasileiro é, em geral, suficiente para lidar com esses crimes, exceto pela lacuna referente às imagens geradas por inteligência artificial, e que o maior desafio hoje está na efetividade processual e na rapidez da cooperação internacional. Ressaltou ainda que as práticas e instrumentos defendidos são compatíveis com democracias consolidadas e altamente protetivas em relação à privacidade e aos dados pessoais, como as europeias.

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

João Paulo de Carvalho da Costa do MPBA/NUCCIBER, destacou em sua fala a urgência de modernizar a legislação penal e processual diante da crescente complexidade dos crimes cometidos no ambiente digital, especialmente aqueles que vitimam crianças e adolescentes. Segundo ele, as redes sociais, originalmente concebidas para aproximar pessoas, tornaram-se terreno fértil para práticas ilícitas graves, exigindo uma resposta institucional rápida, coordenada e tecnicamente atualizada. Ressaltou que a criminalidade digital se diferencia pela volatilidade e transnacionalidade das provas, o que impõe ao Estado o desafio de adaptar sua estrutura jurídica, ainda muito voltada para crimes tradicionais com vestígios físicos, à realidade do ciberespaço.

Entre os principais obstáculos enfrentados pelo Ministério Público, apontou três: a dificuldade de identificar autores devido ao uso de ferramentas de anonimização e redes como a TOR – *rede global de servidores voluntários que permite a comunicação anônima na internet, dificultando o rastreamento das atividades online dos usuários*–; a necessidade de garantir a integridade e validade jurídica das provas digitais por meio de uma cadeia de custódia moderna e adaptada; e a falta de definição mais clara sobre as responsabilidades das plataformas e provedores, incluindo prazos de guarda de registros, dever de comunicação imediata de indícios de exploração sexual infantil e colaboração com as autoridades, à semelhança do que já ocorre em países como Canadá e Estados Unidos.

Defendeu ainda a criação de novos tipos penais e o agravamento de penas para condutas que envolvem aliciamento virtual ou "*grooming*", sextorsão, produção e disseminação de conteúdos falsos envolvendo crianças por meio de deepfakes e uso de inteligência artificial. Ele ressaltou que a legislação atual, como o artigo 241-A do ECA e o artigo 218-C do Código Penal, é insuficiente para abranger o aliciamento psicológico e as novas formas de manipulação digital, gerando insegurança jurídica e proteção deficiente dos bens jurídicos tutelados — *em especial a dignidade e a integridade psicológica de crianças e adolescentes.*

Também reforçou a importância de o Brasil implementar integralmente o Segundo Protocolo da Convenção de Budapeste, que permite cooperação direta com provedores estrangeiros e agiliza investigações transnacionais. Defendeu, ainda, o fortalecimento dos núcleos especializados em crimes cibernéticos nos Ministérios Públicos e polícias de todo o país, com mais infraestrutura técnica, interoperabilidade de sistemas e pessoal capacitado.

Enfatizou que a repressão deve ser acompanhada de educação digital e prevenção, destacando projeto premiado do Ministério Público da Bahia voltado à alfabetização digital infantil e à conscientização de pais e educadores sobre os riscos da exposição online. Afirmando que a transformação tecnológica é inevitável, mas a forma como a sociedade reage a ela é uma escolha ética e política, reafirmou o compromisso do órgao em cooperar tecnicamente com o Parlamento e demais instituições para construir um sistema de justiça digitalmente preparado, humano e eficiente, capaz de garantir que a internet seja um espaço de conhecimento, liberdade e proteção às crianças e adolescentes.

Luana Tavares do INCC, iniciou sua fala ressaltando a importância estratégica do tema e o papel do Estado, da sociedade civil e do setor privado na construção de políticas públicas de proteção de crianças e adolescentes no ambiente digital. Explicou que o Instituto Nacional de Combate ao Cibercrime (INCC) foi criado em 2023 e, desde então, vem cooperando com órgãos federais, empresas e organizações sociais. Em 2024, o Instituto entregou ao Gabinete de Segurança Institucional (GSI/PRE) um relatório de 90 páginas com diagnóstico e 20 propostas para a Estratégia Nacional de Cibersegurança, elaborado em parceria com mais de 15 instituições e baseado em dados nacionais e internacionais.

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

Apresentou dados sobre o avanço da criminalidade digital no Brasil, indicando que entre 2018 e 2023, os crimes cibernéticos contra menores aumentaram 360%, colocando o país entre os três com maior número de conteúdos de exploração sexual infantil reportados ao *National Center for Missing and Exploited Children* e à Interpol. Apesar do crescimento das denúncias, menos de 10% resultam em ação penal e apenas 3% em condenação, evidenciando falhas estruturais na cadeia de custódia digital, na preservação de provas e na cooperação entre autoridades e plataformas. Ressaltou que, além dos crimes de exploração sexual, há o crescimento de práticas como aliciamento virtual, *sextorsão*, cyberbullying e desafios perigosos que incitam automutilação e suicídio entre jovens, problemas que seriam agravados pelo uso de criptomoedas, redes anônimas e pela atuação transnacional de grupos organizados na *dark web*.

Defendeu o fortalecimento da cooperação internacional, com destaque para a Convenção de Budapeste e outros tratados multilaterais, e ressaltou a necessidade de alinhamento entre o debate legislativo brasileiro e o recém-apresentado PL 4752/2025, que institui o Marco Legal da Cibersegurança. Segundo ela, o projeto propõe a criação de uma Autoridade Nacional de Cibersegurança, capaz de complementar a atuação da ANPD na prevenção e combate a crimes digitais, o que beneficiaria diretamente a proteção de crianças e adolescentes. O INCC, que participa da elaboração desse marco, apresentará em novembro um relatório específico ao grupo de trabalho da Câmara com sugestões para harmonizar as propostas legislativas em curso.

Entre as principais recomendações, considerou a atualização do Código Penal e o agravamento de penas para crimes cibernéticos cometidos contra menores, incluindo a criação de tipos penais específicos para a produção de *deepfakes* com aparência infantil, transmissão ao vivo de abusos, aliciamento e chantagem sexual. Propôs também o agravamento de penas quando houver uso de anonimato, criptomoedas ou plataformas estrangeiras; a criação de um rito sumário para acelerar investigações e denúncias; e a formação de uma Rede Nacional de Preservação de Provas Digitais, integrando Ministério Público, Polícia Federal, polícias civis e provedores.

Além disso, sugeriu a criação de uma base nacional de *hashes* de conteúdos de exploração sexual infantil, interoperável com bancos internacionais, e a atualização do Marco Civil da Internet à luz do ECA Digital, para prever um “dever de cuidado proporcional” das plataformas, impondo a obrigação de detectar, bloquear, impedir a recirculação de conteúdos ilícitos e notificar imediatamente as autoridades. Enfatizou que a responsabilização deve alcançar não apenas plataformas, mas também agentes econômicos que lucram com a exploração da vulnerabilidade infantojuvenil.

Encerrando sua fala, sublinhou que proteger crianças e adolescentes no ambiente digital não é apenas uma pauta criminal, mas também uma pauta de direitos humanos, saúde mental, educação e segurança pública. Lembrou que “enquanto o Estado leva meses para obter uma quebra de sigilo, criminosos podem destruir a infância de uma vítima em segundos”, e defendeu que a sociedade seja mais ágil e articulada que os próprios criminosos.

O especialista **Felipe Rodrigues** focou no uso de IA generativa por adolescentes e defendeu que crianças não deveriam ter acesso a esse tipo de tecnologia. Apresentou dados recentes indicando ampla adoção: 7 em cada 10 alunos do ensino médio já usam ferramentas como ChatGPT e Gemini para trabalhos escolares, mas só 32% receberam orientação adequada; 72% dos adolescentes norte-americanos já interagiram com “AI companions” – 52% entre os usuários regulares – e, no Brasil, 40% de crianças e adolescentes recorrem à IA por companhia ou apoio emocional — *fenômeno que chamou de “terceirização do afeto”*. No mesmo período, 64% das denúncias online envolvendo menores dizem respeito a abuso e exploração sexual, com quase 50 mil denúncias entre janeiro e julho de 2025. Entre as práticas mais

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

frequentes estão montagens pornográficas com IA, comercialização dessas imagens em aplicativos de mensagens, cyberbullying e chantagem sexual, inclusive em ambientes escolares.

Para ilustrar riscos concretos, mostrou interações reais em aplicativos populares de "companheiros de IA" – como o Character AI, com dezenas de milhões de downloads – que, em poucos cliques, expõem adolescentes a roteiros eróticos e a narrativas de professor-aluno sexualizadas. Exibiu também a facilidade de alcançar conteúdo impróprio em apps de edição/geração de imagem e casos de respostas perigosas em produtos voltados a crianças. Demonstrou como é trivial criar deepfakes e manipulações simples para humilhar, chantagear ou aplicar golpes. Alertou ainda para riscos de privacidade em cadastros e reconhecimento facial, questionando se a LGPD, sozinha, dá conta dos novos usos.

Como respostas, enfatizou formação digital de famílias e escolas, monitoramento ativo e diálogo: checar histórico de navegação, apps recém-baixados, tempo de tela por aplicativo, pedir que mostrem o que fizeram e observar sinais de alerta nas crianças como mudanças súbitas na qualidade de trabalhos, linguagem muito avançada ou inadequada, ou alterações de comportamento. Concluiu que a tecnologia se move mais rápido que o Estado e que é preciso se antecipar, combinando educação e supervisão com medidas regulatórias e de desenho de plataformas para reduzir exposição e danos a crianças e adolescentes.

O deputado **Osmar Terra** (PL/RS) defendeu que o PL **3066/2025** – *já aprovado na Comissão de Previdência e Família e em análise na CCJ* – seja o "projeto-mãe" para tipificar e agravar crimes ligados ao uso de IA em pornografia infantil; elogiou o GT, relatou caso recente de homicídio de adolescente em Brasília e sugeriu ouvir autoridades de segurança pública.

A deputada **Delegada Ione** (AVANTE/MG) reafirmou apoio como presidente da Frente contra a Pedofilia e citou seu PL 4022/2025, que tipifica a "adultização" abusiva de crianças nas redes.

A deputada **Rogéria Santos** informou a prorrogação do GT por mais 60 dias, após um primeiro ciclo de 30 dias em que oito projetos foram aprovados na Semana da Criança, e reforçou a linha "inovar com proteção".

Nas considerações finais, **George Loder** alertou para o efeito de bolhas online e também de chats de IA que validam condutas abusivas e defendeu calibragem regulatória para não travar a inovação, mantendo-se disponível para colaborar.

João Paulo de Carvalho da Costa invocou a prioridade absoluta do art. 227 da Constituição e pediu reforma penal-processual integrada: penas proporcionais à lesão ampliada no digital, regras claras de cadeia de custódia e preservação de provas para evitar nulidades.

Luana Tavares propôs modelo do *National Center for Missing & Exploited Children* (NCMEC), que prevê obrigatoriedade de reporte pelas plataformas, inclusive de chats privados e alinhamento com o Marco Legal da Cibersegurança, além de cooperação internacional e rede de preservação de provas.

Felipe Rodrigues fechou lembrando usos positivos da IA na educação, mas insistiu no protagonismo de famílias e escolas na alfabetização digital e no acompanhamento cotidiano. A coordenação encerrou reforçando que o Brasil precisa de inovação com guarda-chuva protetivo, letramento digital e engajamento ativo das famílias.

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