

## PL PREVÊ REGRAS PARA PROTEGER CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL



No dia 28 de novembro de 2024, a Comissão de Comunicação e Direito Digital (CCDD) aprovou o Projeto de Lei 2628/2022, que busca implementar medidas para proteger crianças e adolescentes no mundo virtual.

A visa combater práticas como bullying, exploração sexual, incentivo a vícios e outros comportamentos prejudiciais.

Entre as medidas sugeridas, destaca-se a exigência de ferramentas eficazes para verificar a idade dos usuários nas plataformas, além de incentivar uma supervisão mais ativa das atividades online pelos responsáveis legais.

Para as empresas de tecnologia e telecomunicações, o projeto determina a implementação de sistemas para notificar abusos e conteúdo de exploração sexual, com a obrigação de reportar esses casos às autoridades competentes. Também estabelece a remoção imediata desses materiais após denúncia, garantindo a preservação de dados relevantes para investigações.

Outro ponto importante do PL é a obrigação de que aplicativos com mais de um milhão de usuários menores de 18 anos apresentem relatórios detalhados, a cada seis meses, sobre as denúncias recebidas e as ações tomadas em resposta a elas.

## AUSTRÁLIA PROÍBE O USO DE REDES SOCIAIS POR MENORES DE 16 ANOS

O parlamento australiano deu um passo inédito ao aprovar uma medida que proíbe crianças e adolescentes menores de 16 anos de usarem redes sociais. A lei é a primeira do mundo nesse sentido.

Gigantes como TikTok, Instagram, Facebook, Snapchat, Reddit e X enfrentarão penalidades severas, chegando a 50 milhões de dólares australianos (cerca de R\$ 194 milhões), caso não consigam evitar que menores de 16 anos criem contas em suas plataformas.

A aprovação no Senado contou com 34 votos favoráveis e 19 contrários, enquanto a Câmara dos Representantes já

havia respaldado a proposta com ampla maioria, registrando 102 votos a favor e apenas 13 contrários.

Antes de entrar em vigor, a Câmara ainda precisará ratificar as alterações propostas no Senado, algo considerado apenas um trâmite burocrático, já que o governo indicou seu apoio às emendas.

Após a sanção, as empresas terão um prazo de um ano para implementar mecanismos que garantam o cumprimento da lei, antes que as penalidades comecem a ser aplicadas.

# ATAQUE HACKER NÃO EXCLUI RESPONSABILIDADE POR PROTEÇÃO DE DADOS

*“O tratamento de dados pessoais configura-se irregular quando deixa de fornecer a segurança que o titular poderia esperar, consideradas as circunstâncias relevantes do caso”.*

Com esse entendimento, a 3ª Turma do Superior Tribunal de Justiça confirmou a responsabilidade da Enel pelo vazamento de dados pessoais de uma consumidora, após um ataque hacker.

A consumidora teve expostos nome completo, números de RG e CPF, endereço, endereço de e-mail e telefone. A ação foi ajuizada para cobrar indenização da empresa, que à época ainda se chamava Eletropaulo.

A Enel, defendeu-se alegando que o ataque hacker é ato de terceiro apto a justificar a excludente de responsabilidade, conforme prevista no artigo 43, inciso III, da Lei Geral de Proteção de Dados.

Entretanto, os magistrados entenderam que a ocorrência do ataque hacker mostra uma falha da empresa.



*“O tratamento de dados pessoais configura-se irregular quando deixa de fornecer a segurança que titular poderia esperar, consideradas circunstâncias relevantes do caso”*, apontou. A votação na 3ª Turma foi unânime.

## O JULGAMENTO DO ARTIGO 19 DO MARCO CIVIL DA INTERNET

O voto do Ministro Toffoli, no julgamento do STF acerca do artigo 19 do Marco Civil da Internet, traz problemas ao tentar solucionar demanda já antiga acerca da regulação das redes.

Isso porque, ao determinar a remoção de conteúdo mediante notificação extrajudicial, abre espaço para que conteúdos não necessariamente infringentes sejam removidos. Nesse caso, podemos ter a medida utilizada indevidamente para manipular o conteúdo das redes.

Quanto aos critérios para remoção independente de notificação, o problema é ainda maior. A decisão do ministro parece ignorar que a “divulgação de notícias falsas para incentivar violência física”, por exemplo, depende de juízo de valoração, inicialmente sobre o que é notícia falsa e, posteriormente, sobre o que é incentivo à violência física. A valoração deste, e de outros quesitos apresentados pelo Ministro, só pode caber ao judiciário, visto que a remoção de conteúdo não é atividade corriqueira: sempre prejudicará a parte que postou. Ademais, cabe ponderar, também, a principal alegação das big techs: Como monitorar as redes para detectar conteúdo com bases subjetivas? A inteligência artificial disponível atualmente não é capaz de fazer tal varredura.

Assim, caso seja seguido pelos demais ministros em seu voto, o remédio pode ser pior que a doença, no sentido de que restará às redes sociais, para sua própria proteção, restringir ao máximo a liberdade de expressão em seus ambientes.

## VANTAGENS DE SE TER UM DPO TERCEIRIZADO

A figura do DPO é obrigatória nas empresas, e muitas dúvidas surgem na hora de nomear alguém. Veja 06 benefícios de contar com um serviço de DPO terceirizado:

**Serviço Especializado:** Um DPO terceirizado representa um profissional, assessorado por equipe própria, especializado em privacidade e proteção de dados. Essa especialização leva anos e requer dedicação exclusiva às leis de proteção de dados nacionais e internacionais.

**Redução de Custos:** A contratação de um DPO no mercado é muito cara, e a promoção de um funcionário não especializado ao cargo, além de prejudicial, demanda aumento de salário e sujeita a empresa a alegações de acúmulo de função. Um DPO terceirizado é mais barato do que parece, especialmente quando esquematizado em pacotes de horas.

**Independência e Imparcialidade:** Um DPO terceirizado pode fornecer uma perspectiva ampla e imparcial sobre questões de conformidade.

**Redução de Riscos:** Com o DPO terceirizado, a empresa pode minimizar o risco de violações de dados e as consequências legais e financeiras associadas a elas.

**Foco nos negócios da empresa:** Com um DPO externo, os funcionários podem se concentrar nas atividades principais de seus departamentos, sem destacamento para exercer a função.

**Apoio na Gestão de Incidentes:** Em caso de violação de dados, um DPO terceirizado pode fornecer orientação especializada, ajudando a minimizar o impacto e a cumprir os requisitos de notificação obrigatória.