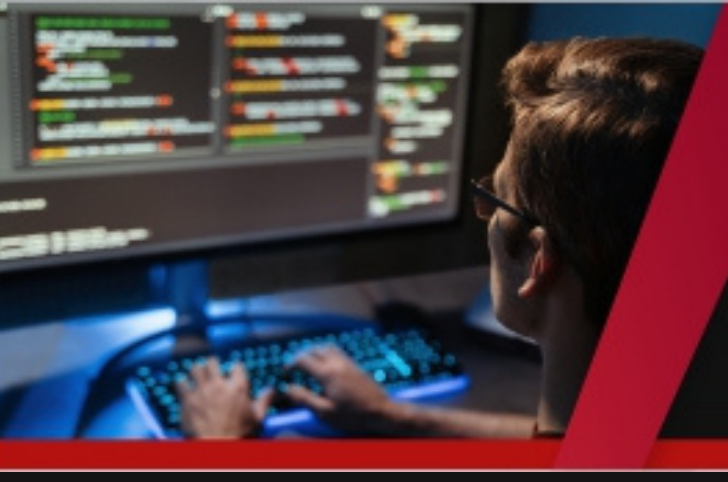


MPMT Ministério Público DO ESTADO DE MATO GROSSO | CAO CIBER

BOLETIM INFORMATIVO

cao.ciber@mpmt.mp.br

Edição n° 02/2024

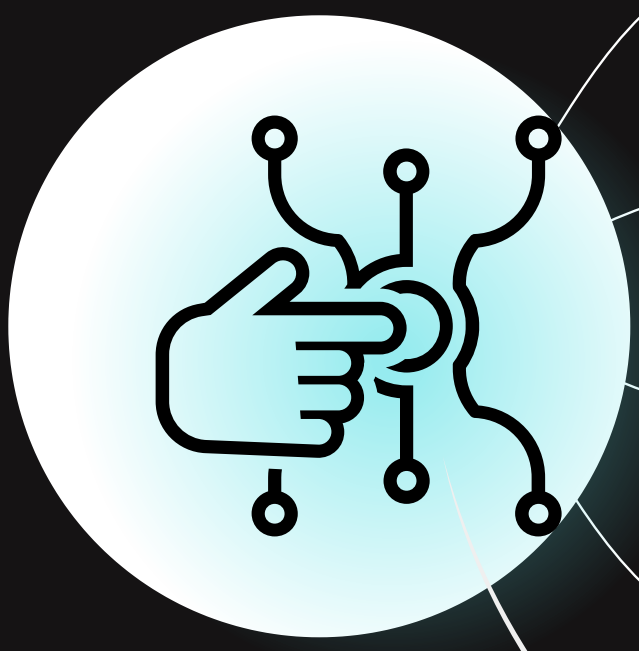
MPMT Ministério Público DO ESTADO DE MATO GROSSO

APRESENTAÇÃO:

Trata-se de Centro de Apoio Operacional de Crimes e Ilícitos Digitais, estabelecido por meio do Ato Administrativo nº 1.173/2023-PGJ, que tem como missão principal auxiliar as procuradorias e promotorias do Ministério Público Estadual em suas atividades funcionais, assim como, em parceria com os Procuradores (as) e Promotores (as) de Justiça do Estado de Mato Grosso, garantir medidas judiciais e extrajudiciais necessárias para reprimir os crimes telemáticos no âmbito estadual.

MPMT
Ministério Público
DO ESTADO DE MATO GROSSO

SUMÁRIO



Equipe:

Daniel Carvalho Mariano
Promotor de Justiça - Coordenador

Leandro Volochko
Promotor de Justiça - Coordenador Adjunto

Claudir Santos da R. Junior
Auxiliar Ministerial

Matheus Henrique A. Ribeiro
Residente Jurídico

MPMT
Ministério Público
DO ESTADO DE MATO GROSSO

1. NOTÍCIAS

Anatel investiga uso de software encontrado na Abin capaz de “invadir” rede 4G.

TJ-SP condena influenciadora por publicidade enganosa em curso online.

Adolescente do ES é vítima de grupo que induzia a crimes na internet.

Projeto submete relação com redes sociais ao Código do Consumidor.

ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD.

Ncyber/MPDFT obtém condenação inédita em caso de ataque ransomware.

Caixa não indenizará homem que depositou R$ 2.350 a falsa namorada virtual.

Mãe de aluno que praticou cyberbullying no WhatsApp indenizará vítima.

Novo vírus que desvia transferências em mais de 60 bancos é detectado.

Criminosos manipulam imagens de apresentador da CNN para promover aplicativo falso.

‘DEEPFAKE’: Golpistas usam Inteligência Artificial e criam reunião falsa com diretor financeiro de multinacional, que transfere R$ 129 milhões a criminosos.

- TJ-SP condena por improbidade servidoras que burlaram sistema para obter passe escolar.
- Ação controlada: STJ valida provas por espelhamento do WhatsApp Web.
- STF anula provas obtidas a partir de dados preservados sem ordem judicial.
- Corretora deve restituir criptomoedas transferidas após sequestro de cliente.
- Denúncias de abuso sexual infantil na web batem recorde no Brasil.
- PF combate comércio de moeda falsa pela internet.
- Gravação com câmera espiã em quarto de hospedagem é crime.
- Suspeitos de vender dados do presidente do STF são presos pela PF.
- Projeto de lei quer proibir menores de 12 anos nas redes sociais.
- Operação do CyberGAECO resulta em prisão em flagrante por pornografia infantojuvenil.
- Operação Takedown é deflagrada para desarticular organização criminosa especializada em fraudes cibernéticas.

MPMT
Ministério Público
DO ESTADO DE MATO GROSSO

2. DESTAQUES

Ncyber/MPDFT obtém condenação inédita em caso de ataque ransomware.

O Núcleo de Combate a Crimes Cibernéticos (Ncyber) do Ministério Público do Distrito Federal e Territórios (MPDFT) obteve nesta quinta-feira, 8 de fevereiro, a condenação dos cibercriminosos responsáveis pelos crimes de extorsão qualificada e invasão de dispositivo informático após invadirem sistemas de instituição bancária da capital federal e exigir o pagamento de resgate dos dados sigilosos obtidos ilegalmente.

Os ataques ransomware são praticados por criminosos com elevado conhecimento de informática, que se utilizam de programas de computador especializados em invadir e criptografar dados sigilosos para, em seguida, extorquir as vítimas titulares desses dados.

Com a deflagração da Operação Black Hat pela Delegacia Especializada de Combate a Crimes Cibernéticos da Polícia Civil do Distrito Federal e Territórios, os autores foram identificados por meio de avançadas técnicas de investigação aplicadas com o apoio dos peritos do Instituto de Criminalística da PCDF.

CLIQUE AQUI PARA ACESSO A NOTÍCIA

Ministros do STF destacam importância de normas aprovadas pelo TSE sobre manipulações digitais nas eleições.

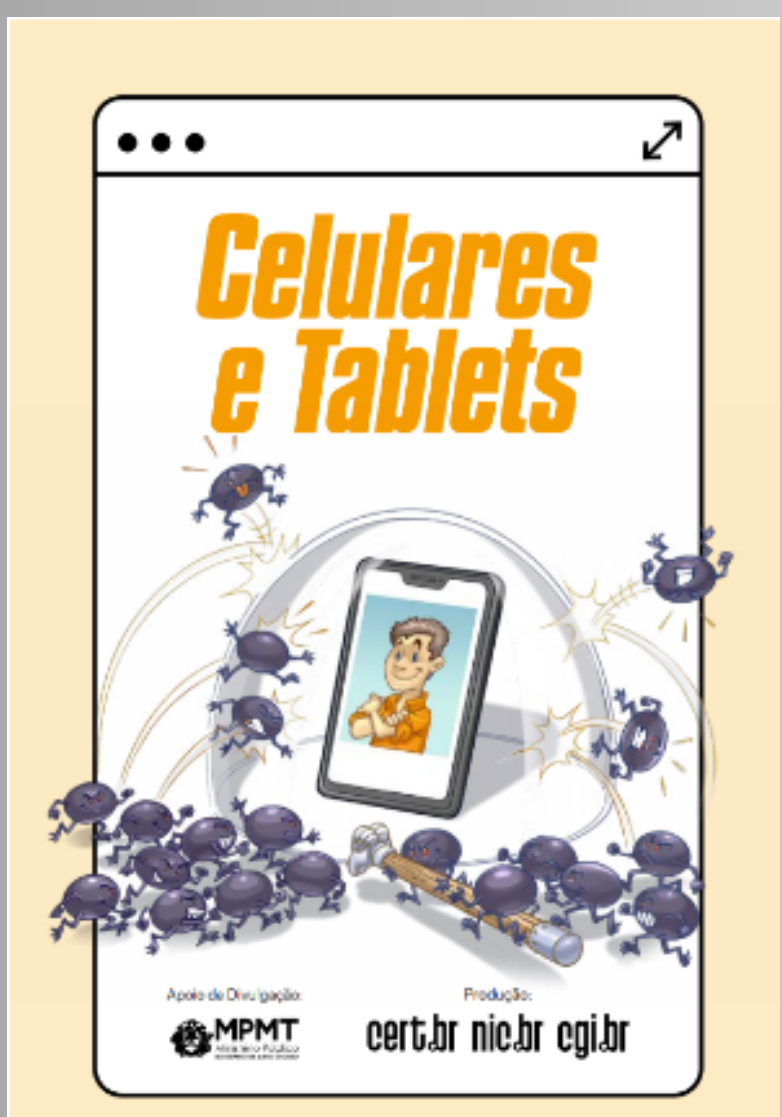
A ministra Cármen Lúcia compartilhou com o Plenário do Supremo Tribunal Federal (STF), nesta quarta-feira (28), informações sobre o enfrentamento da desinformação e do uso indevido de inteligência artificial (IA) nas Eleições Municipais de 2024. O tema veio à tona em razão da sessão realizada ontem (27), no Tribunal Superior Eleitoral (TSE), que aprovou 12 resoluções, relatadas pela ministra, que também integra aquela corte, disciplinando regras a serem aplicadas nas eleições deste ano.

Ao analisar questões sobre propaganda eleitoral e a influência das novas tecnologias na democracia, o TSE acolheu proposta da ministra Cármen Lúcia de atualizar normas eleitorais em razão de avanços tecnológicos. “É preciso saber o que é aceitável do ponto de vista constitucional, legal e na jurisprudência do TSE quanto ao uso dessas novas tecnologias que influem diretamente na escolha livre do eleitor”, ressaltou.

CLIQUE AQUI PARA ACESSO A NOTÍCIA

3. MATERIAL DE APOIO

SEGURANÇA NO BANCO ON-LINE. Com o avanço da tecnologia, o uso de aplicativos de banco por meio da internet se tornou cada vez mais comum e prático. No entanto, é fundamental estar atento à segurança das suas informações financeiras ao utilizar essas plataformas. Para garantir a proteção dos seus dados, é essencial adotar algumas medidas de segurança. Certifique-se de baixar o aplicativo oficial do seu banco, disponível nas lojas de aplicativos confiáveis. Evite baixar aplicativos de fontes desconhecidas, pois podem ser falsos e utilizados para roubar suas informações. Mantenha o seu celular atualizado com as últimas versões do sistema operacional e do aplicativo do banco. As atualizações costumam corrigir falhas de segurança e garantir a proteção dos seus dados. Opte por conexões seguras, como o Wi-Fi de casa ou os dados móveis do seu celular. Na cartilha ao lado você encontrará essas e muitas outras dicas para um uso mais seguro desses aplicativos.



USO SEGURO DE TABLETS E CELULARES. Para garantir a segurança, durabilidade e bom funcionamento de celulares e tablets, é importante seguir algumas orientações. A cartilha produzida pelo Cert.br / Nic.br / CGI.br disponibiliza informações que vão te auxiliar a prolongar a vida útil do seu dispositivo eletrônico e utilizá-lo de forma segura. Conforme os tópicos elencados no material, é recomendado limitar o acesso de outras pessoas ao seu aparelho, ter cuidado ao utilizar comunicação por proximidade, ajustar as permissões dos aplicativos de acordo com a necessidade, ser cauteloso ao se conectar em redes Wi-Fi públicas, bloquear a tela de início do dispositivo, evitar clicar em todos os links recebidos, desabilitar funções na tela bloqueada, proteger o CHIP SIM com uma senha, combinar senha forte com biometria nos aplicativos financeiros, não gravar senhas de serviços financeiros no celular, ajustar limites para reduzir os prejuízos financeiros e usar cartões de crédito virtuais para pagamentos não presenciais. Essas medidas contribuem para a preservação do seu dispositivo.

4. OPINIÃO

A DECISÃO JUDICIAL E O USO DA INTELIGÊNCIA ARTIFICIAL

por REINALDO RODRIGUES DE OLIVEIRA FILHO
quinta-feira, 22 de fevereiro de 2024, 14h27

A Constituição Federal de 1988 estabelece que toda decisão emanada de órgão judicial deve apresentar os motivos e fundamentos que lhe deram substância (art. 93, IX, da CR/1988). O dever constitucional de fundamentação das decisões judiciais, além de uma garantia processual em favor das partes, revela uma diretriz de legitimação do Poder Judiciário e consolidação do Estado Democrático de Direito. Entre as premissas que justificam a natureza constitucional do dever de motivação e/ou fundamentação das decisões judiciais destacam-se: a) demonstração do uso de argumentação racional no processo de construção decisória; b) controle da juridicidade da decisão; c) legitimação do exercício do poder jurisdicional; d) proteção do devido processo legal e promoção de várias de suas garantias; e) redução do quantitativo de recursos; e f) promoção da segurança jurídica ao definir a interpretação dos dispositivos normativos e tornar possível a homogeneização jurisprudencial pelos Tribunais Superiores.

O Código de Processo Civil (art. 11, caput), na esteira da diretriz constitucional, estabelece como norma diretiva do sistema processual a fundamentação qualificada dos pronunciamentos judiciais e, mais adiante (§ 1.º do art. 489), na seção que trata dos elementos e dos efeitos da sentença, enumera os casos de fundamentação deficiente, equiparando-os à falta de fundamentação. É evidente que a fundamentação qualificada deve se fazer presente em qualquer pronunciamento jurisdicional – seja em processos individuais ou coletivos – e, por via de consequência, deve iluminar a atuação do órgão judicante em todas as fases do iter processual. Tema que vem despertando grande discussão na comunidade processual é a possibilidade da utilização de ferramentas tecnológicas, em auxílio a juízes e tribunais, na elaboração de decisões judiciais. A aplicação da inteligência artificial (IA) poderia contribuir para o aumento da velocidade de funcionamento dos tribunais e, por conseguinte, proporcionar uma expressiva redução na avalanche de processos que tramitam nos tribunais brasileiros? A figura o magistrado poder ser substituída pelo uso de programas de IA de última geração?

A IA pode ser concebida como um conjunto de algoritmos planificado a executar tarefas e/ou atividades propostas pelo ser humano, com propensão a alcançar elevados níveis de exatidão (acurácia) em reduzido espaço de tempo. Os primeiros estudos relacionados ao campo da IA remontam – segundo referenciais demarcados por doutrina especializada –, à primeira metade do século XX e no contexto conturbado da Segunda Guerra Mundial (1940), obtendo progresso exponencial em virtude das descobertas científicas alcançadas até hoje.

(...)

Para ter acesso ao texto completo , **CLIQUE AQUI**

Por **REINALDO RODRIGUES DE OLIVEIRA FILHO**. Promotor de Justiça no Estado de Mato Grosso. Mestre em Direito Público pela Universidade Estadual Paulista – UNESP. Doutor em Direito Processual Civil pela PUC/SP e Professor da FESMP.

5. JURISPRUDENCIA EM TESES

Inicialmente cumpre salientar que a denúncia imputa a prática dos delitos de injúria e difamação, mas o faz distinguindo duas circunstâncias fáticas passíveis de recorte: I) a charge e as hashtags que a acompanham; e II) o texto objeto de compartilhamento.

Assim, consta da inicial que a denunciada realizou uma postagem em sua rede social com ofensas à honra subjetiva do Procurador-Geral da República e do Presidente da República à época dos fatos, contendo expressões que se entendeu injuriosas, veiculadas por meio de hashtags expostas em uma charge na qual o Presidente da República segurava o Procurador-Geral da República por uma coleira.

Na mesma postagem, fez-se acompanhar de texto que se reputou difamatório, consistente na afirmação de ter sido o Procurador-Geral da República adquirido pelo Presidente da República, submetendo a sua autoridade e comando a serviço dos interesses deste e de seus familiares.

Nesse contexto, o elemento fático do crime de injúria relaciona-se às afirmações injuriosas veiculadas por meio de hashtags e a charge exposta, ao passo que a difamação relaciona-se com o texto que acompanha a postagem.

CLIQUE AQUI PARA O INTEIRO TEORNO NO SITE DO STJ

A ministra Nancy Andrighi, relatora do recurso, observou que, nos termos do artigo 14, parágrafo 1°, do Código de Defesa do Consumidor (CDC), o serviço é considerado defeituoso quando não fornece a segurança que o consumidor dele espera, levando-se em consideração circunstâncias relevantes, como o modo de seu fornecimento, o resultado e os riscos que razoavelmente dele se pressupõem, e a época em que foi fornecido.

A relatora explicou que o dever de segurança consiste na exigência de que os serviços ofertados no mercado ofereçam a segurança esperada, ou seja, não tenham por resultado dano aos consumidores individual ou coletivamente. Segundo Nancy, é com base nisso que o artigo 8º do CDC admite que se coloquem no mercado apenas produtos e serviços que ofereçam riscos razoáveis e previsíveis, isto é, que não sejam potencializados por falhas na atividade econômica desenvolvida pelo fornecedor.

"É dever da instituição financeira verificar a regularidade e a idoneidade das transações realizadas pelos consumidores, desenvolvendo mecanismos capazes de dificultar a prática de delitos. O surgimento de novas formas de relacionamento entre cliente e banco, em especial por meio de sistemas eletrônicos e pela internet, reafirmam os riscos inerentes às atividades bancárias. É imperioso, portanto, que instituições financeiras aprimorem continuamente seus sistemas de segurança", afirmou.

CLIQUE AQUI PARA O INTEIRO TEORNO NO SITE DO STJ

MPMT
Ministério Público
DO ESTADO DE MATO GROSSO

MPMT
Ministério Público
DO ESTADO DE MATO GROSSO