

Tozzini Freire.

ADVOGADOS

BOLETIM
CYBERNEWS.

26ª Edição

Sumário

CYBERNEWS
26ª EDIÇÃO

01	CONTEXTO BRASILEIRO	
	5
	7

02	ORIENTAÇÕES GERAIS	
	9

03	PODER JUDICIÁRIO	
	11
	12

04	AUTORIDADES	
	14
	14

05	AVANÇOS NORMATIVOS	
	16
	17

05	DECISÕES INTERNACIONAIS	
	19

Contexto Brasileiro.

Publicado regulamento que estabelece as regras para aplicação das penalidades da LGPD

Em 27 de fevereiro de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) publicou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, que representa um avanço importante para assegurar a aplicabilidade da Lei Geral de Proteção de Dados (LGPD). O Regulamento tem como principais objetivos: (i) estabelecer os parâmetros e critérios para aplicação de sanções administrativas pela ANPD, bem como (ii) definir as formas e dosimetria para o cálculo do valor-base das sanções de multa.

Vale lembrar que a LGPD lista como possíveis sanções: advertências, suspensão do uso dos bancos de dados pessoais afetados, publicização da infração e a aplicação de multa, com limite total de R\$ 50.000.000,00 (cinquenta milhões de reais), entre outras.

De acordo com o Regulamento, serão aplicadas sanções proporcionais à infração, que poderão ser classificadas em leves, médias ou graves. Essa classificação tem como base 11 critérios na análise sobre (i) a gravidade e natureza das infrações e dos direitos pessoais afetados,

o (ii) grau de dano identificado, além da (iii) boa-fé do infrator, sua (iv) condição econômica e a (v) potencial vantagem auferida ou pretendida diante da infração. Ainda, é considerada (vi) a pronta adoção de medidas corretivas por parte do infrator, bem como se foram implementados (vii) mecanismos e procedimentos internos capazes de minimizar o dano.

No que diz respeito às sanções pecuniárias, a definição do valor-base da multa tem como ponto de partida uma metodologia objetiva prevista no Regulamento com o cálculo que será desenvolvido pela ANPD para tanto. Assim, serão considerados não apenas a (i) classificação da infração, mas ainda o (ii) grau do dano identificado, o (iii) faturamento do agente infrator, bem como eventuais (iv) circunstâncias atenuantes e agravantes presentes na infração.

Passado apenas um mês após a publicação do Regulamento, já foi possível perceber que a aplicação de sanções por descum-

primento à LGPD é concreta. Foram instaurados oito processos administrativos sancionatórios envolvendo majoritariamente órgãos do setor público federal, como o Ministério da Saúde, Secretaria de Educação do Distrito Federal e Secretaria de Estado da Saúde de Santa Catarina, por supostos vazamentos de dados pessoais, ausência de comunicação de incidente de segurança, ausência de encarregado, ausência de registros de operações envolvendo dados pessoais (Registro das Operações de Tratamento de Dados Pessoais – ROPA) e relatório de impacto de proteção de dados pessoais e/ou não atendimento a requisições da ANPD. Todos encontram-se na fase de instrução processual e estão prestes a serem julgados.

A ANPD tornou pública a relação desses processos, que contém o nome do órgão público ou empresa privada, a conduta realizada, o setor de atuação do ente fiscalizado, a fase em que se encontra o processo e o número do processo aberto na ANPD. No entanto, as sanções

que serão aplicadas para cada caso e o acesso aos documentos do processo somente se tornarão públicos após a conclusão da investigação.

Por fim, apesar de os primeiros processos envolverem, em sua maior parte, o setor público, a diretora da ANPD, Nairane Leitão, informou que esse não é o úni-

co alvo das fiscalizações, sendo que já existe um segundo lote de processos envolvendo empresas privadas com infrações além do vazamento de dados, como venda e compartilhamento indevido de dados.

Consulte a íntegra do Regulamento [aqui](#).

ANPD publica nota técnica quanto à aplicação da LGPD para pessoas falecidas

Em 17 de março de 2023, a ANPD publicou nota técnica posicionando-se pela não aplicação da LGPD no caso de tratamento de dados de pessoas falecidas.

A justificativa toma como base o art. 6º do Código Civil, de acordo com o qual a existência da pessoa natural termina com a morte. Assim sendo, pressupõe-se que a incidência da LGPD ocorre apenas no âmbito do tratamento de dados pessoais de pessoas naturais vivas.

Orientações Gerais.



Nova Orientação sobre desenvolvimento de jogos e proteção infantil é elaborada pela ICO

Uma nova orientação, voltada para a indústria de jogos, foi elaborada pela Autoridade de Proteção de Dados do Reino Unido, o Gabinete do Comissariado de Informação (ICO, na sigla em inglês). A orientação trata da proteção das crianças contra riscos online e foca em como os desenvolvedores de jogos, editores e operadores de plataformas podem entrar em conformidade com o Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês) e com a Lei de Proteção de Dados do Reino Unido de 2018 (DPA 2018).

Entre as disposições da nova orientação estão a elaboração de Relatórios de Impacto de Proteção de Dados (RPID), a fim de avaliar o risco do tratamento de dados pessoais de crianças. Além disso, a orientação da ICO sugere exibir informações claras sobre como os dados serão tratados e a preocupação em coletar um consentimento válido dos pais ou responsáveis das crianças.

O guia da ICO também incentiva os desenvolvedores de jogos a projetar os jogos de maneira que eles garantam os direitos à privacidade das crianças e impeça que os menores exponham, sem motivo, seus dados pessoais. Dessa maneira, espera-se que seja possível oferecer uma experiência de jogo mais segura para os jogadores menores de idade.

Poder Judiciário.



STF profere julgamento sobre fornecimento de dados de usuários por plataformas digitais

Após um grande período de suspensão, o julgamento da Ação Declaratória de Constitucionalidade (ADC) nº 51, que visa analisar a constitucionalidade do Acordo de Assistência Judiciária em Matéria Penal (MLAT, na sigla em inglês), foi finalmente finalizado no dia 23 de fevereiro de 2023.

Segundo o voto vencedor do ministro relator Gilmar Mendes, o qual foi seguido pela maioria dos demais ministros, o Supremo Tribunal Federal (STF) entendeu pela constitucionalidade do MLAT, sem prejuízo da aplicação direta do artigo 11 do Marco Civil da Internet (Lei nº 12.965/2014), o qual determina aos provedores de aplicação de internet a prestação de informações a autoridades brasileiras quanto a dados coletados no Brasil.

A controvérsia dos autos se referia ao argumento de defesa das empresas de tecnologia,

que não possuem servidores no Brasil, de que haveria submissão às regras de fornecimento de conteúdo previstas em território americano. Além disso, defendem que as autoridades brasileiras deveriam recorrer aos mecanismos de cooperação judiciária do MLAT para requisitar os conteúdos de usuários.

O entendimento da Suprema Corte foi pelo reconhecimento de que os mecanismos de cooperação judiciária previstos no MLAT devem ser aplicados nos casos em que as empresas de tecnologia não estejam sediadas no Brasil, nem possuam subsidiárias em território nacional. Quanto aos casos em que as empresas possuam filiais em território brasileiro, o Ministro Relator entendeu pela constitucionalidade da requisição direta de dados às empresas de tecnologia, sem a necessidade de comunicação com as autoridades americanas.

STJ entende que vazamento de dados pessoais não sensíveis não gera dano moral presumido

A 2ª Turma do Superior Tribunal de Justiça (STJ), ao reformar acórdão prolatado pelo Tribunal de Justiça de São Paulo (TJSP), entendeu que o vazamento de dados pessoais não tem o condão de gerar dano moral indenizável, sendo necessária a prova do dano decorrente da exposição das informações por parte do titular dos dados.

No tribunal estadual, a sentença de primeiro grau havia sido reformada para condenar a empresa concessionária de energia elétrica Enel ao pagamento de danos morais ao titular de dados. Contudo, como arguido pela empresa em sede de recurso especial, os dados vazados não se enquadram como sensíveis à luz da LGPD, de forma que o vazamento não poderia, por si só, causar lesão moral ao consumidor. A premissa central adotada pelo ministro relator Francisco Falcão foi a de que os dados cujo vazamento se relatou não seriam sensíveis, pois são dados de cadastro, como CPF, número de telefone e endereço. Tratando-se de dados fornecidos corriqueiramente, o ministro relator entendeu que o conhecimento desses por terceiro não teria o condão de violar o di-

reito de personalidade do titular de dados.

Ainda, o voto confirmou o entendimento de que, em que pese reprovável a falha no tratamento de dados pessoais por pessoa jurídica, o vazamento por si só não acarreta dano moral indenizável. Não se tratando de dano moral presumido, se mostra necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações, caracterizadas como dados não sensíveis.

Esse é o primeiro precedente do STJ acerca de indenização por vazamento de dados embasado especificamente nas previsões legais da LGPD e orientará a jurisprudência sobre o tema. Referido entendimento confirma a tônica dos julgados recentes já prolatados pela Corte, no sentido de que deve se evitar a banalização do dano moral haja vista que a indenização nesse sentido deve levar em consideração se houve prejuízo efetivo e que tenha excedido os limites do tolerável.

Autoridades.

0010010
01001 10110 010
0100010101001
0100111101010
1001 1101001 0100110



Correios noticiam vazamento de dados pessoais de usuários

No mês de fevereiro, em razão de falhas técnicas no aplicativo “Meu Correios”, houve vazamento de informações pessoais de usuários, como números de telefone e CPF. Após detectar o incidente, a organização enviou um comunicado à ANPD e providenciou novas medidas de Segurança.

A empresa não divulgou o número exato de contas expostas, tampouco as razões das

falhas técnicas, porém, informou que o impacto chegou a 5% de todos os cadastros. Ainda, alertou que, a vulnerabilidade poderia permitir que cibercriminosos relacionassem um número de CPF a um número de celular cadastrado.

Diante disso, os Correios orientaram a todos os seus usuários a trocarem suas senhas de acesso no aplicativo.

MPF notifica seus usuários sobre possível vazamento de dados

O Ministério Público Federal (MPF) enviou um e-mail com mensagem de alerta aos usuários de seu sistema, Protocolo Eletrônico do MPF notificando possível vazamento de dados pessoais não sensíveis, como nome, e-mail, telefone e IP.

Não foram vazadas informações sensíveis aptas à geração de perfis falsos ou rou-

bos de identidade e fraudes. No entanto, o MPF receia o uso dessas informações para aplicação de golpes nos usuários do sistema.

O órgão, além de enviar e-mail aos usuários informando sobre o incidente de segurança, já notificou também a ANPD. Além disso, tomou as medidas necessárias para cessar o

possível acesso indevido e prevenir novos incidentes.

Não há indício de que os dados tenham ou estejam sendo utilizados para fins inadequados ou ilegais.



Avanços Normativos.

Conselho da UE elabora documento para esclarecer a interação da Lei de Resiliência Cibernética com a IA e as leis de segurança de produtos

O Conselho da União Europeia (UE) divulgou, por meio da presidência sueca, um documento esclarecendo a correlação entre a Lei de Resiliência Cibernética, a Lei de Inteligência Artificial e a Lei de Segurança de Produtos, todas da UE. Esse novo documento está focado nas formas de implementar as leis mencionadas no setor de segurança cibernética e estratégia digital.

O documento explora a ideia da “resiliência da segurança cibernética”, especialmente em uma década em que as ameaças ci-

bernéticas e os incidentes de segurança apenas crescem, mostrando como as três complementam-se na construção de uma estrutura de segurança de rede.

O documento também fornece informações sobre como a Lei de Resiliência Cibernética e a Lei de Inteligência Artificial entrarão em vigor, a avaliação de conformidade – e que tipos de produtos deverão ser comunicados às autoridades de proteção de dados –, a aplicação das leis e suas penalidades.

Sequestro de dados (ransomware) pode ser incluído como crime no Código Penal do Brasil

O Projeto de Lei (PL) nº 879/2022, de autoria do senador Carlos Viana (PL/MG), propõe alterar o Código Penal (Decreto-Lei nº 2848/40) para incluir o art. 154-C. A alteração seria pautada pela inclusão de mais um tipo penal à seção IV do Código, que trata dos crimes contra a inviolabilidade dos segredos. O PL também aumenta a pena para o crime de invasão de dispositivo informativo de 1 a 4 anos, para 2 a 5 anos (art. 154-A, §3, Código Penal), além de multa.

Caso seja aprovado, o PL incluirá ao Código Penal o crime de “sequestro de dados informáticos”, com algumas qualificadoras. A justificativa do PL, conforme o parlamentar, é que, com a recorrência dos ataques ransomware “a sociedade clama pela criação de um tipo penal específico para desestimular a prática da conduta popularmente chamada de ‘sequestro de dados’, uma espécie de ataque cibernético que ainda não encontra perfeita subsunção à norma penal vigente no Brasil”.

Decisões Internacionais.



OB

Autoridade de Proteção de Dados Francesa multa Discord em EUR 800.000

A Autoridade Francesa de Proteção de Dados (CNIL, na sigla em francês) multou uma plataforma de comunicação e mensagens instantâneas, o Discord, em 800.000 euros, por não cumprir com o GDPR. Essa multa é o resultado de uma investigação da CNIL sobre a incapacidade do Discord em fornecer informações claras sobre o uso de cookies.

Na visão da CNIL, o Discord, que é utilizado por milhões de pessoas no mundo inteiro, não informou adequadamente seus

usuários sobre as atividades de tratamento de dados que estão sendo realizadas na plataforma. Além disso, a CNIL concluiu que o Discord não coletou de forma válida o consentimento de seus usuários para realizar certas atividades de tratamento.

Além da multa, a CNIL ordenou que o Discord ajuste suas práticas para cumprir com o GDPR, tais como coletar o consentimento de uma forma válida e fornecer informações claras sobre como trata dados pessoais.

Este boletim é um informativo da área de Cybersecurity & Data Privacy de TozziniFreire Advogados.

**SÓCIAS RESPONSÁVEIS
PELO BOLETIM:**

Marcela Waksman Ejnisman

-  Patrícia Helena Marta Martins
-  Carla do Couto Hellu Battilana
-  Bruna Borghi Tomé
-  Luiza Sato
-  Sofia Kilmar

Mais informações em:
tozzinifreire.com.br

**Tozzini
Freire.**
ADVOGADOS