Tozzini Freire.
ADVOGADOS

BOLETIM

CYBERNEWS.

31ª Edição | 2023

Sumário

01 Realidade Brasileira.

ANPD publica relatórios e políticas institucionais

Entre agosto e setembro, a Autoridade Nacional de Proteção de Dados (ANPD) se mostrou bastante ativa com a publicação de alguns documentos institucionais, dos quais os principais pontos estão descritos abaixo:

Relatório de Ciclo de Monitoramento (RCM) – traz a avaliação das atividades fiscalizatórias de 2022 e o seus principais resultados, por exemplo, o recebimento de 1.045 requerimentos, os quais incluem denúncias de violações à Lei Geral de Proteção de Dados (LGPD) e das petições de titulares. Os setores com maior quantidade de requerimentos foram plataformas digitais, finanças, telecomunicações e agregadores de dados. Com relação a comunicações de incidentes de segurança, foram recebidas 473 notificações, sendo a maioria referente a casos de sequestro de dados provocados por falhas de segurança em sistemas de informação (ramsomware).

Política de Comunicação Social – tem por objetivo orientar as ações estratégicas de comunicação social da ANPD para promoção do empoderamento dos titulares de dados pessoais.

Relatório de Acompanhamento Semestral – detalha o andamento dos projetos da Agenda Regulatória 2023-2024. Segundo o relatório, é esperado que as seguintes ações ocorram até o final deste ano: aprovação do Regulamento de Comunicação de Incidente com Dados Pessoais; consulta pública do Regulamento sobre Atuação do Encarregado; e publicação de guias orientativos.

Realizado debate sobre a atividade sancionatória da ANP

Em agosto, foi realizada audiência pública, pela Comissão de Desenvolvimento Econômico (CDE) da Câmara dos Deputados, sobre sanções administrativas aplicadas pela ANPD no caso de vazamento de dados pessoais. O objetivo da audiência foi discutir a destinação de multas por vazamentos de dados e outras possíveis melhorias na LGPD.

Na audiência, o coordenador-geral de Fiscalização da ANPD, relembrou que a LGPD e a ANPD vão além de vazamento, sendo que a atuação da autoridade se baseia na atitude do fiscalizado de forma progressiva – desde o monitoramento, a orientação até a repressão, quando necessário.

02 Poder Judiciário.

CNJ inicia ciclo de monitoramento para implementação de resolução da LGPD

Em 25 de agosto, o Conselho Nacional de Justiça (CNJ) lançou o ciclo de monitoramento e avaliação do resultado regulatório da Resolução nº 363/2021, que estabelece diretrizes para a adaptação à LGPD nos tribunais pátrios. Isso ocorreu durante o 1º Simpósio Nacional sobre LGPD no Poder Judiciário, promovido pelo Tribunal de Justiça da Bahia (TJBA), no qual reuniu diversas instituições, incluindo o Superior Tribunal de Justiça (STJ), CNJ, Tribunais Estaduais e Federais, e ANPD.

O conselheiro Luiz Fernando Bandeira de Mello, coordenador do Comitê Gestor de Proteção de Dados Pessoais (CPGD) e responsável pelo tratamento de dados pessoais no CNJ, ressaltou que o campo da proteção de dados ainda está em desenvolvimento no Brasil. Além disso, destacou que a avaliação regulatória tem como objetivo discutir os resultados e impactos da regulamentação com base em dados empíricos.

Para ele, a resolução desempenha um papel crucial na efetivação do direito fundamental à proteção de dados pessoais. “Nosso objetivo é identificar onde estamos, ou seja, mapear os desafios regulatórios, as medidas preventivas e corretivas necessárias para abordar essas questões. Esse modelo de avaliação foi projetado para garantir esse processo”, aponta.

O CNJ encaminhará um questionário aos Tribunais Estaduais para coletar informações cruciais, o qual será dividido em: identificação, avaliação e percepção. Também será mantido um canal permanente para esclarecer dúvidas durante o preenchimento da pesquisa, reconhecendo a complexidade das demandas regulatórias decorrentes da Resolução nº 363.

03 Autoridades.

MPSP apura possível ilegalidade no envio de dados de alunos para empresas de publicidade pelo Governo de SP

O Ministério Público do Estado de São Paulo (MPSP) iniciou uma investigação para verificar se a Secretaria Estadual de Educação (SEDUC) infringiu a LGPD e violou o direito à privacidade dos alunos ao, supostamente, coletar suas informações pessoais durante a pandemia e as encaminhar para empresas especializadas em publicidade.

As denúncias foram feitas pela ONG Human Rights Watch (HRW), que relatou que a irregularidade teria ocorrido através do Centro de Mídias da Educação de São Paulo (CMSP) e de outras plataformas que prestaram serviços à SEDUC. De acordo com a HRW, os sites não apenas monitoravam os estudantes em salas de aula virtuais, como também durante todo o período em que navegavam na internet, obtendo informações sobre a vida privada de crianças e adolescentes.

Com base na pesquisa da HRW, a promotora Sandra Lucia Garcia Massud abriu uma investigação e deu um prazo de 30 dias para a SEDUC fornecer uma cópia dos documentos assinados com as plataformas prestadoras de serviços, a fim de analisar os contratos e verificar se houve coleta e tratamento de dados, bem como a sua divulgação para empresas de publicidade.

A administração do governador de São Paulo, Tarcísio de Freitas, afirmou que não firmou nenhum contrato ou manteve relação com as plataformas mencionadas na denúncia. Os contratos teriam sido assinados pelas administrações anteriores e foram encerrados em 2021 e 2022. O Centro de Mídias continua em funcionamento, mas com um tratamento de dados pessoais reduzido apenas ao necessário para prover a finalidade educacional.

CONAR arquiva processo contra a propaganda que recriou Elis Regina com IA

O processo iniciado pelo Conselho Nacional de Autorregulamentação Publicitária (CONAR) para analisar a campanha da Volkswagen foi arquivado pelo Conselho de Ética no dia 22 de agosto de 2023. A campanha, lançada em 4 de julho e criada com Inteligência Artificial (IA), foi analisada para averiguar eventual violação ao Código Brasileiro de Autorregulamentação Publicitária.

A representação ética iniciada no CONAR decorreu de divergências de consumidores sobre dois aspectos principais: (i) questionamento se um anúncio em vídeo que utilizou IA generativa híbrida para recriar a imagem da cantora Ellis Regina, falecida em 1982, foi feito com respeito e ética; e (ii) indagação sobre a necessidade de incluir informações explícitas no anúncio quanto à utilização de ferramenta de IA na sua composição.

Em nota oficial, o Conselho esclareceu que o colegiado considerou improcedente o questionamento de desrespeito à figura da artista "uma vez que o uso da sua imagem foi feito mediante consentimento dos herdeiros e observando que Elis aparece fazendo algo que fazia em vida".

Em relação à obrigação de divulgar o uso da técnica de IA chamada 'deepfake', o CONAR comunicou que avaliou várias orientações de boas práticas já existentes sobre o assunto, "bem como a ausência de regulamentação específica em vigor". Em vista disso, a maioria dos conselheiros optou por arquivar a reclamação.

Ainda, o órgão acrescentou em nota que a transparência, como princípio ético fundamental, foi respeitada, enfatizando que o processo tramitou com ampla defesa.

04 Avanços Normativos.

Novas orientações sobre o envio de comunicação em massa são publicadas pela Autoridade Britânica de Proteção de Dados

A Autoridade Britânica de Proteção de Dados (Information Commissioner's Office – ICO) emitiu, em 30 de agosto, novas diretrizes com orientações a respeito do envio de e-mails em massa, alertando as organizações sobre os riscos nesse processo. Em suas Diretrizes, a ICO traz à tona recomendações de boas práticas relacionadas à proteção de dados pessoais.

A relevância de fazer uso de métodos adequados ao enviar comunicações em massa é enfatizada com base em ações recentes de fiscalização da ICO, que tem identificado recorrentes casos de divulgação desnecessária de dados a partir de erro cometidos no envio de comunicações por e-mail. Ainda que no Brasil ainda não haja orientação específica da ANPD sobre o tema, as diretrizes da ICO se apresentam em direta sintonia com as premissas das normas de proteção de dados aplicáveis.

Centro Canadense de Segurança Cibernética emite recomendações sobre proteção de dados em aplicativos

O Centro Canadense de Segurança Cibernética publicou, em agosto, algumas recomendações para usuários, titulares de dados e organizações sobre a proteção de dados pessoais ao utilizar aplicativos móveis.

O texto contém orientações sobre dados que os aplicativos móveis podem coletar, os riscos inerentes ao compartilhamento de dados com esses aplicativos, como os usuários podem se proteger desses aplicativos, entre outras informações. É possível ler as orientações e recomendações na íntegra aqui.

05 Julgados.

TJSP afasta condenação a danos morais em caso de vazamento de dados

A 25ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo (TJSP) afastou a presunção de dano moral em caso de vazamento de dados. Em suma, o Tribunal entendeu que os dados não eram sensíveis e que não houve prova de dano, já que não teve prejuízo real causado pelo incidente.

Trata-se de ação de indenização movida por consumidor, sob alegação de uso indevido de seus dados por estelionatários, após contratação de seguro de vida com empresa seguradora.

Em primeira instância, a empresa seguradora foi condenada a pagar R$ 10 mil, mas após interposição de recurso, o Tribunal reverteu a decisão. O relator destacou que o vazamento não foi responsabilidade da seguradora e que não há conexão entre os danos alegados e o incidente de dados.

Afirmou, ainda, que os dados vazados não se enquadram na definição de "dados sensíveis" segundo o artigo 5º da LGPD, o que não justifica a condenação da seguradora.

STJ restringe fornecimento de dados pela Google para identificação de usuários

A 6ª Turma do STJ, deu parcial provimento ao recurso da empresa Google Brasil sob entendimento que é necessário o fornecimento de dados à Justiça a fim de auxiliar investigação de crime. Contudo, o entendimento da Corte é que a abrangência da quebra de sigilo de dados deve ser limitada às informações suficientes para a identificação dos usuários, tais quais registros de conexão e de acesso, afastando-se o acesso amplo e irrestrito a conteúdos como e-mail e fotos.

O caso envolve inquérito policial instaurado para investigar crime de roubo que resultou em homicídio. Inicialmente, o juízo de 1ª instância autorizou, a pedido formulado pelo delegado de polícia, "a quebra de sigilo de dados telemáticos dos usuários que, eventualmente, tenham utilizado os serviços da Google num raio de 500 metros das coordenadas geográficas no período abrangido entre as 18h e 22h de 22 de maio de 2022".

Já no julgamento do recurso interposto contra tal ordem em sede do STJ, em um primeiro momento, a relatora ministra Laurita Vaz proferiu voto asseverando que a decisão impugnada não foi redigida de maneira genérica, tampouco viola o direito à intimidade e à privacidade dos usuários. O ministro Rogério Schietti acompanhou a relatora.

Em razão da divergência apresentada pelo voto do ministro Sebastião Reis, que entendeu que a prestação de informações por parte da Google deveria ser limitada e que a empresa deveria "prestar única e exclusivamente aquelas informações necessárias para identificação do IP", a relatora reconsiderou seu voto e concordou com a necessidade de limitar o conjunto de dados a ser fornecido pela empresa. Os demais ministros, Rogério Schietti e Saldanha Palheiro, também concordaram com a evolução do entendimento.

Ao final, ainda constou em julgamento - com concordância por parte de todos os ministros - que nada impede o requerimento de outras informações dos investigados no futuro, desde que de forma justificada.

Juiz de São José dos Campos entende pela responsabilidade objetiva de instituição financeira por vazamento de dados de correntista

O juiz Marcos Alexandre Bronzatto Pagan, da 2ª Vara do Juizado Especial Cível de São José dos Campos (SP), condenou instituição financeira a restituir o valor total de R$ 32.800,00 à correntista vítima de fraude e induzida a realizar transferências bancárias, após ter seus dados pessoais vazados.

Os fatos discutidos apontam pela realização de transferência de valores, via Pix, pela consumidora correntista a golpista que utilizou informações confidenciais obtidas a partir de seu cadastro bancário.

Como fundamentos da decisão, o magistrado observou a suficiência das provas apresentadas pela consumidora - comprovantes das transações, e-mails trocados com colaborador da instituição financeira, extrato da conta e registros das ligações telefônicas. Além disso, foi presumida a boa-fé da correntista e que não teria registros de antecedentes com ocorridos semelhantes.

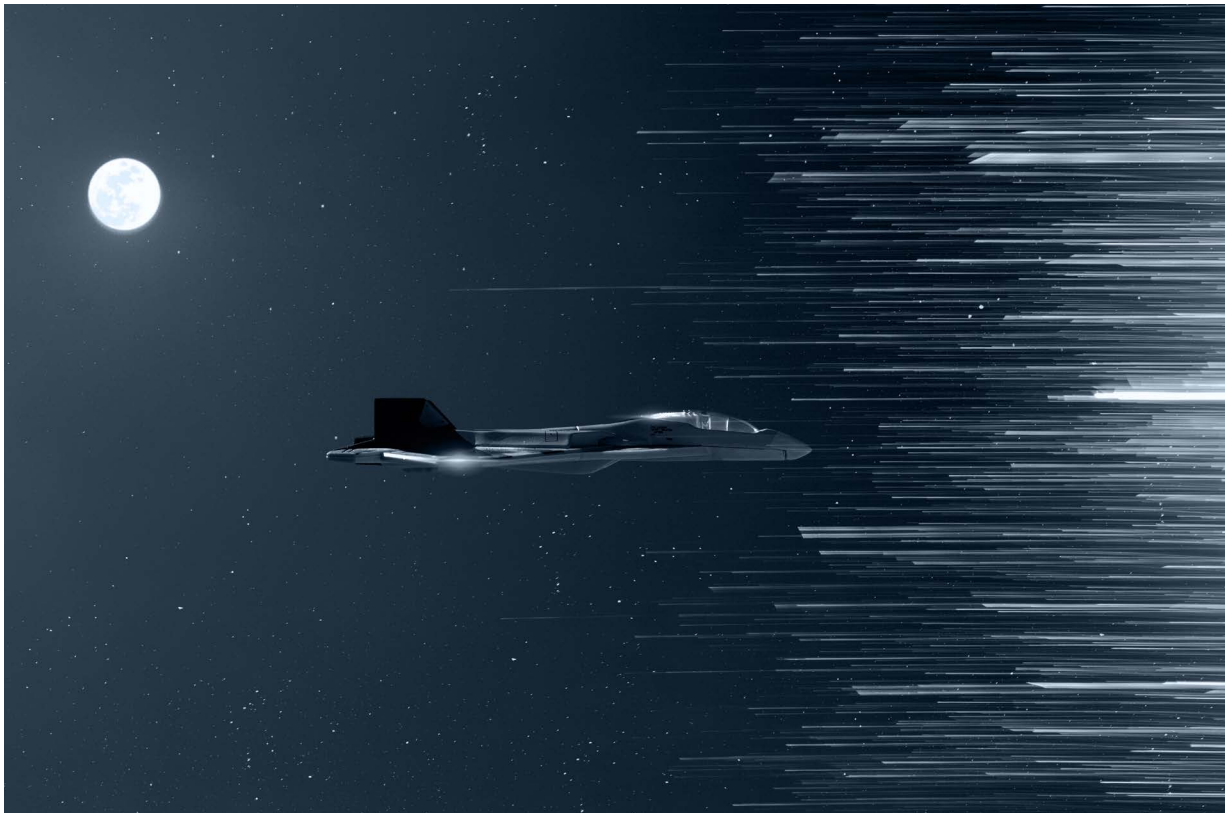
Embasada, portanto, nos ditames do Código de Defesa do Consumidor e nas premissas de que houve o vazamento de dados sensíveis da correntista pela instituição financeira em razão de "um representante ou através dos canais de atendimento bancário, ou seja, quando gerado por um incidente interno", a decisão condenou a instituição financeira à reparação dos valores despendidos pela consumidora em razão da fraude, seguindo a jurisprudência recente do TJSP.

06 Cenário Internacional.

Espanha cria a primeira agência de supervisão de IA na Europa

No final de agosto, o Conselho de Ministros da Espanha aprovou o estatuto da Agência Espanhola de Supervisão de Inteligência Artificial (AESIA), autorizando a sua criação, tornando-se o primeiro país europeu a dispor de uma agência para regular esse tema e antecipando a entrada em vigor do Regulamento Europeu de Inteligência Artificial. A AESIA objetiva a proteção dos cidadãos, a supervisão do desenvolvimento da IA inclusiva, sustentável e centrada nos cidadãos, e aplicação de regulamentos sobre inteligência artificial.

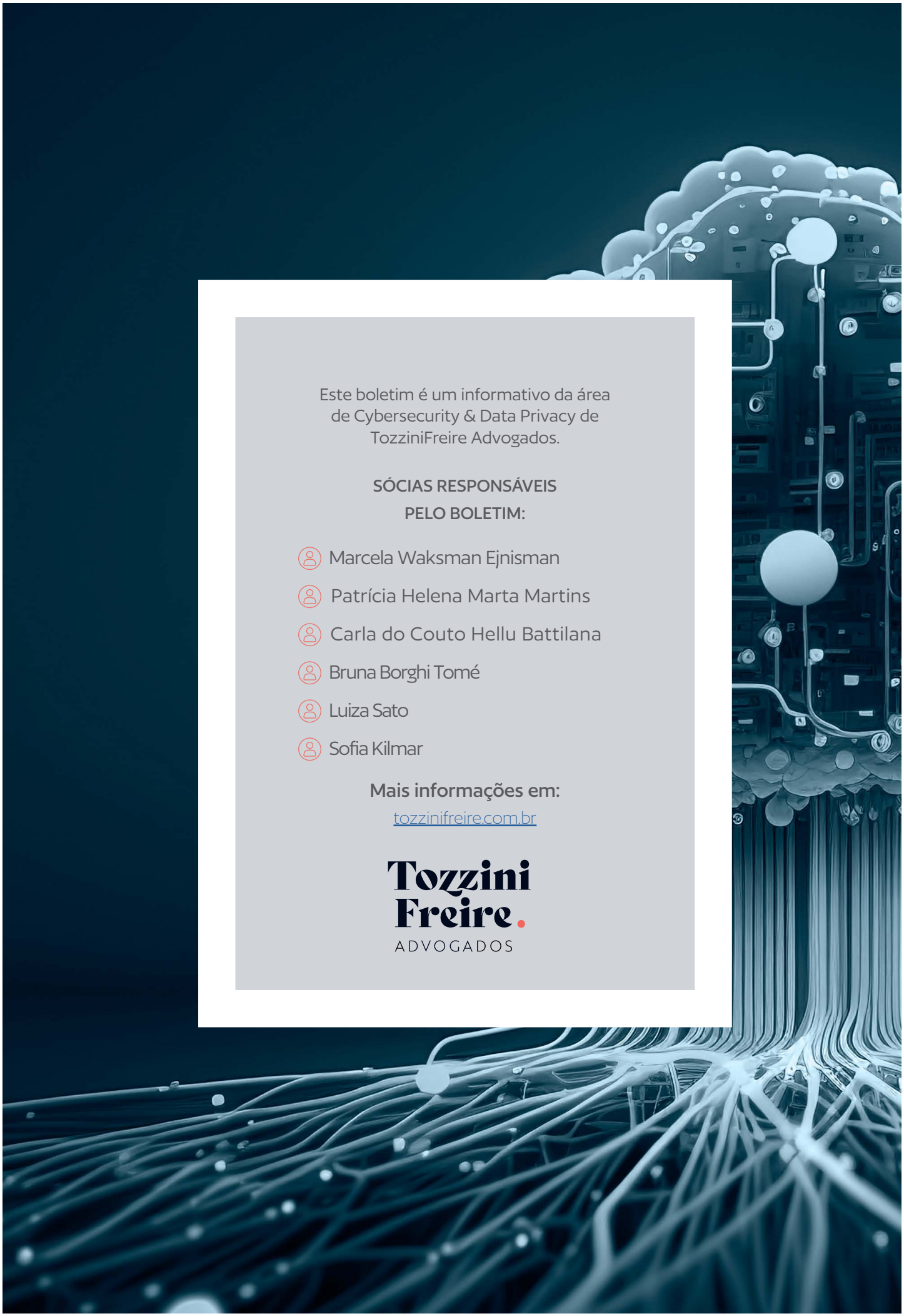
Veja a íntegra do comunicado do ministério aqui.



Atualização no quadro de aprovação dos organismos de certificação de encarregados na França

Na França, determinadas entidades, previamente aprovadas pela Comissão Francesa de Proteção de Dados (CNIL, na sigla em francês), podem emitir certificação de encarregados de proteção de dados. Esse certificado é um mecanismo voluntário e opcional que comprova que aquele encarregado de fato cumpre os requisitos de competências e conhecimento do Regulamento Europeu de Proteção de Dados (GDPR, na sigla em inglês).

A aprovação concedida pela CNIL a entidades certificadoras é feita com base na análise de diversos requisitos, que foram atualizados em agosto. Dentre as modificações, destacamos que agora passa a ser necessário que o encarregado em busca da certificação comprove seu domínio sobre o tema por meio de apresentação de documentos específicos - ainda que os fundamentos de certificação permaneçam inalterados. Além disso, agora, as entidades certificadoras não estão mais obrigadas a demonstrar experiência prévia na área de certificações de pessoas.



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