e-Book

Legal Innovation
Data Protection Day

DIA INTERNACIONAL DA PROTEÇÃO DE DADOS

Autores:

Patricia Peck
Henrique Rocha
Camila Nascimento
Jéssica Guedes
Julia Lonardoni Ramos
Lucas Grandini Arthuso

Peck Advogados

Direito para Inovação Digital

INTRODUÇÃO

No Dia Internacional da Proteção de Dados Pessoais (28/01), o Peck Advogados em parceria com o Instituto Internacional de Estudos de Direito do Estado (IIEDE) promoveu o evento **Legal Innovation: Data Protection Day**, que reuniu diversos especialistas da área para discutir as melhores práticas e os principais desafios que envolvem a proteção de dados no país.

Com a participação de profissionais de diferentes setores e de grande relevância no mercado, o encontro on-line contou com seis painéis, numa manhã de muita troca de experiências, a apresentação de cases e a análise de tendências esperadas para 2022.

Além da sócia-fundadora da banca e Conselheira Titular do Conselho Nacional de Proteção de Dados (CNPD), **Patricia Peck**, outro destaque foi a presença de **Jônathas Assunção Salvador Nery de Castro**, Presidente do Conselho Nacional de Proteção de Dados (CNPD).

Confira mais detalhes neste material exclusivo, que traz uma retrospectiva de 2021 em relação à inovação e proteção de dados, bem como as principais tendências do setor para este ano.

IIEDE Instituto Internacional de Estudos de Direito do Estado

com o apoio de

Peck Advogados

Direito para Inovação Digital

apresentou:

Legal Innovation Data Protection Day

ABERTURA

Jônathas Assunção Salvador Nery de Castro - *Presidente do* ***Conselho Nacional de Proteção de Dados (CNPD)***

PAINEL 1

LGPD E O PROCESSO SANCIONADOR DA ANPD

Patricia Peck - *CEO do Peck Advogados e Conselheira Titular no* ***CNPD***
Annette Martinelli de Mattos Pereira – *Advogada no* ***Itaú Unibanco*** *e Conselheira Titular no* ***CNPD***
Fábio Medina Osório – *Presidente-Executivo no* ***IIEDE***
Filipe Calado – *Solution Architect na* ***Security***

PAINEL 2

LGPD - BOTS, ALGORITMOS INTELIGENTES E ELEIÇÕES

Leandro Bissoli – *Mediador (Sócio no* ***Peck Advogados****)*
Fabrício Medeiros – *Advogado e Professor*
Fabro Steibel – *Conselheiro Titular no* ***CNPD***

PAINEL 3

PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES

Sandra Tomazi – *Mediadora (Sócia no* ***Peck Advogados)***
Abílio Branco - *Head de Proteção de Dados na* ***Thales Group***
Genival Souza – *Advogado no* ***Peck Advogados***
José Castellian – *CEO e founder na* ***LawQuest***
Valdenice Minatel Melo de Cerqueira – *Diretora-Geral Educacional no* ***Colégio Dante Alighieri***

PAINEL 4

LGPD E O TRATAMENTO DE DADOS NOS MARKETPLACES E NA SAÚDE

Henrique Rocha – *Mediador (Sócio no **Peck Advogados**)*
Alexandre Ernest Reis - *Financial Lines and Cyber na **Tabapuã Seguros***
Evaldo Osório Hackmann - *Executivo Jurídico na **Sikur***
Juliana Oliveira Domingues – *Secretária Nacional do Consumidor no Ministério da Justiça e Segurança Pública (**Senacon**)*
Marcos Vinícius Ottoni – *Coordenador-Geral Jurídico na Confederação Nacional de Saúde (**CNSaúde**)*

PAINEL 5

TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS E DESAFIOS DOS DPO'S

Lorena Botelho – *Mediadora (Sócia no **Peck Advogados**)*
Gabriela Soares de Freitas – *DPO Compliance and Data Privacy na **Samsung***
Maria de Lurdes Gonçalves – *Associada no **VdA, Vieira de Almeida Sociedade de Advogados***
Moacir Klapouch - *Engenheiro de Soluções na **OneTrust***

PAINEL 6

MATURIDADE DOS PROGRAMAS DE PRIVACIDADE NO BRASIL E TENDÊNCIAS PARA 2022

Marcelo Crespo – *Mediador (Sócio no **Peck Advogados**)*
Andre Quintanilha - *Chief Privacy Officer na **Palqee Brasil***
Tawfiq Alashoor - *Assistant Professor na **Copenhagen Business School***
Sabrina Palme - *CEO & Data Protection Officer na **Palqee Technologies***

APOIADORES


CREDI
LINK®
INFORMAÇÕES DE CRÉDITO


SIKUR


tabapuã
CONSULTORIA EM SEGUROS


THALES
Together • Safer • Everywhere


OneTrust
PRIVACY, SECURITY & GOVERNANCE

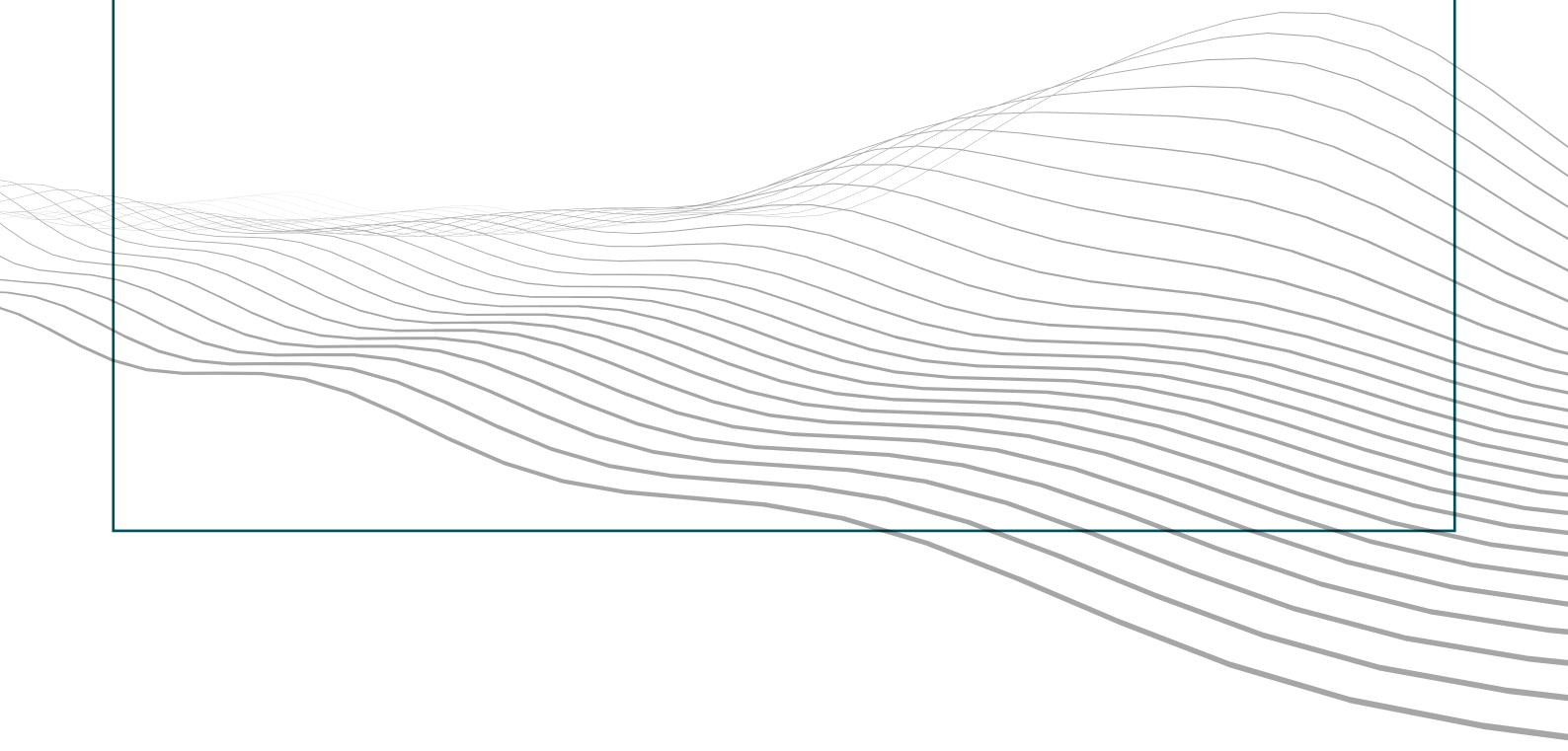

EXIN


securiti


palqee

RETROSPECTIVA

2021



FISCALIZAÇÃO PELA ANPD

A fiscalização da Autoridade Nacional de Proteção de Dados, como atribuição legal enquanto órgão fiscalizador, alcançou estágio de estruturação com a publicação do Regulamento Sancionador.

1. REGULAMENTO

No dia 29 de outubro de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) publicou a Resolução CD/ANPD nº 1, sobre o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador. Após realização de audiências públicas e avaliação do comitê interno, fixou-se esse regulamento que tem por objetivo estabelecer os procedimentos inerentes ao processo de fiscalização e as regras a serem observadas no âmbito do processo administrativo sancionador pela ANPD.

De acordo com o Regulamento, a atividade de fiscalização exercida pela ANPD terá inclusive a finalidade de orientar, prevenir e reprimir as infrações à Lei Geral de Proteção de Dados Pessoais (LGPD), com vistas a parte coercitiva que compete ao órgão de interromper situações de dano ou risco, reconduzir à plena conformidade e punir os responsáveis mediante a aplicação das sanções administrativas previstas no art. 52 da LGPD.

Por meio da aprovação deste Regulamento, também foram estabelecidos os requisitos e os procedimentos a serem aplicados pela ANPD na instauração de processo administrativo sancionador contra os agentes de tratamento de dados pessoais.

Importante ressaltar que as orientações para a dosimetria de aplicação de sanção ainda serão estabelecidas por meio de regulamentação específica a ser publicada, dentro da agenda regulatória da ANPD.

O Regulamento passou a vigorar na data da sua publicação, ou seja, 29 de outubro de 2021, e o primeiro ciclo de monitoramento seguindo as diretrizes dispostas iniciou-se em janeiro de 2022.

2. ACORDOS DE COOPERAÇÃO TÉCNICA FIRMADOS EM 2021 PARA ATUAÇÃO FISCALIZATÓRIA

• ANPD e Senacon - 22/03/2021 - Um dos objetivos é dar maior agilidade nas investigações de incidentes de segurança e proteger dados pessoais dos consumidores.

• ANPD e CADE - 02/06/2021 - Um dos principais objetivos é estabelecer a atuação coordenada em casos de infração à ordem econômica que envolvam dados pessoais.

• ANPD e NIC.br - 20/07/2021 - Dentre os principais pontos destacam-se o intercâmbio de informações e a realização de ações de interesse comum quanto à proteção de dados pessoais e à segurança da informação.

• ANPD e Agência Espanhola de Proteção de Dados (Memorando) - 26/10/2021 - Um dos objetivos primordiais é a promoção de mecanismos específicos de cooperação técnica que permitam a troca de conhecimentos e experiências, além da identificação das melhores práticas no campo da proteção de dados pessoais. O evento coincide com a entrada da ANPD como membro da Rede Ibero-Americana de Proteção de Dados.

• ANPD e TSE - 24/11/2021 - O objetivo é trazer benefícios para a sociedade, para os candidatos, eleitores, partidos políticos e demais agentes de tratamento e fortalecer o relacionamento entre o TSE e a Autoridade na aplicação da LGPD no âmbito eleitoral.

3. PANORAMA DE CONVENÇÕES INTERNACIONAIS

Convenção Africana para Cibersegurança[1]

Em 2014, os membros da União Africana (UA) aprovaram a Convenção da União Africana sobre Cibersegurança e Proteção dos Dados Pessoais. A Declaração estabeleceu um forte objetivo de ação para fomentar a cibersegurança e a proteção dos dados pessoais entre as nações africanas. Essa convenção também ajuda a orientar os países sobre como prevenir o cibercrime, que demonstra ser uma grande ameaça e um dos principais riscos para a economia, especialmente com a criação da Área de Livre Comércio Continental Africana (AfCFTA), que é a maior zona de livre comércio do mundo em número de participantes (todos os 55 países do continente).

Convenção de Budapeste

O Brasil aderiu à Convenção de Budapeste em 15 de dezembro de 2021. Essa Convenção sobre o Crime Cibernético, celebrada em Budapeste (Hungria, novembro de 2001), propõe facilitar a cooperação internacional para o combate aos crimes na internet.

A Convenção de Budapeste lista os principais crimes cometidos por meio da rede mundial de computadores e foi elaborada pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas, tornando-se o primeiro tratado internacional sobre cibercrimes.

Dentre os assuntos abordados na convenção, tem-se a criminalização de condutas cibernéticas, normas para investigação e produção de provas eletrônicas, meios de cooperação internacional e orientações aos países. O Brasil foi convidado a aderir à Convenção em dezembro de 2019 e até então o poder legislativo não havia confirmado a aceitação, o que ocorreu em dezembro de 2021.

1 - Disponível em: AUCPrivacyGuidelines_201809June_Final_Portuguese.indd (internetsociety.org).

Radar de jurisprudências

A judicialização de casos que envolvem violação à Lei Geral de Proteção de Dados Pessoais tem crescido nos últimos meses. Conforme pesquisa realizada em julho de 2021, foram ajuizadas mais de 600 ações que versam sobre a LGPD[2]. Destacamos os casos mais discutidos durante o ano de 2021:

1. Caso responsabilidade subjetiva - abril/21: trata-se de ação ajuizada em face de uma Empresa de Energia Elétrica, responsável pelo vazamento de dados pessoais da autora. O juízo, embora tenha reconhecido a ocorrência do vazamento de dados pessoais pela empresa, julgou o pedido de Danos Morais improcedente por ausência de comprovação de efetivo dano, tratando da responsabilidade subjetiva. O juízo considerou que as informações vazadas eram em sua maioria dados de qualificação do consumidor (como nome, RG e CPF), que não são cobertos por sigilo e não configuram ofensa ao direito de personalidade da autora. (Autos nº 1025226-41.2020.8.26.0405 TJSP).

2. Caso justa causa por violação à LGPD – abril/21: a funcionária entrou com reclamação trabalhista pleiteando a reversão de justa causa aplicada pelo empregador (Hospital em Balneário Camboriú) por ter vazado prontuário médico de um paciente. O juízo julgou improcedente os pedidos mantendo a justa causa por infração à LGPD. (Autos nº 0000463-60.2020.5.12.0040 TRT12).

3. Caso de improcedência de danos morais pela não comprovação do dano (responsabilidade subjetiva) - maio/21: ação ajuizada em face de uma seguradora de vida mediante alegação de vazamento de dados pessoais. O juízo, embora tenha reconhecido o ato ilegal da seguradora quanto ao vazamento de dados pessoais ante a não adoção de medidas de segurança da informação exigidas na LGPD, julgou improcedente o pedido de danos morais vez que o autor não comprovou o dano efetivo, o que se infere o entendimento pela responsabilidade subjetiva. (Autos nº 0003696-14.2020.8.26.0529 TJSP).

4. Caso de danos morais por divulgação do número de telefone de funcionária - junho/2021: o Tribunal Regional do Trabalho da 3ª Região manteve a condenação de uma empresa ao pagamento de danos morais no valor de 5 mil reais por violação à LGPD, vez que divulgou o número de telefone particular de uma funcionária em seu site de vendas sem autorização. O Tribunal entendeu que a inserção do número de telefone sem prova inequívoca de autorização implica em divulgação de dado pessoal que afronta sua vida privada. (Autos nº 0010337-16.2020.5.03.0074 TRT3).

2 - https://www1.folha.uol.com.br/mercado/2021/07/justica-ja-tem-600-decisoes-envolvendo-lei-de-protecao-de-dados.shtml

5. Caso de indenização por danos morais – responsabilidade objetiva - junho/21: a empresa divulgou indevidamente em seu website dados pessoais do titular, autor da ação. O juízo determinou a condenação por danos morais em 2 mil reais alegando a responsabilidade objetiva por falha na prestação de serviço (art. 14 do Código de Defesa do Consumidor), vez que a divulgação de dados pessoais em página eletrônica, acessível por terceiros, ainda que por curto período, é hábil a enseja indenização por danos morais. (Autos nº 1003122-23.2020.8.26.0157 TJSP).

6. Julho: caso citricultores - julho/2021: ação movida por um Sindicato de Trabalhadores em desfavor de uma cooperativa por violação aos dispositivos da LGPD e ao MCI. O pedido foi julgado parcialmente procedente e condenou a cooperativa a nomear um encarregado, na forma do art. 41 da LGPD. Ainda, entendeu pela desnecessidade da utilização da base legal do consentimento quando o tratamento de dados pessoais decorre da execução do contrato de emprego ou cumprimento de obrigação legal. Quanto a medidas de segurança e boas práticas, determinou a implementação e comprovação de medidas relacionadas à segurança e sigilo de dados, na forma dos arts. 6º, VII, 46 e 47 da LGPD. Por fim, discorreu a respeito do pedido de danos morais, defendendo que o fato de a empresa não ter implementado os comandos legais não faz reconhecer, por si só, a efetiva ocorrência de dano aos titulares dos direitos, ante a inexistência de fato demonstração de vazamento de dados ou outra utilização ilícita capaz de afetar a esfera de privacidade/dignidade dos trabalhadores substituídos. (Autos nº 0020043-80.2021.5.04.0261 TRT4).

7. Caso PIS/COFINS - julho/21: trata-se de um Mandado de Segurança impetrado em face do Fisco Federal, em que o juízo da 4ª Vara Federal de Campo Grande concedeu a segurança determinando que todas as despesas comprovadas de adequação à LGPD sejam consideradas como insumo para fins de creditamento de PIS e COFINS. Ainda, reconheceu o direito de compensação do valor pago. (Mandado de Segurança nº 5003440-04.2021.4.03.6000 TRF3).

8. Caso Facebook – outubro/2021: juíza titular do 4º Juizado Especial Cível de Brasília condenou o Facebook (Meta) ao pagamento de 44 mil reais, a título de danos materiais, às vítimas de golpe via WhatsApp. Defende o juízo que a empresa é responsável pelo serviço, respondendo objetivamente pelos danos causados aos consumidores. Citou em sua decisão a LGPD: “Sabe-se hoje que dados em mãos erradas podem causar grandes prejuízos. A Lei Geral de Proteção de Dados prevê, em seu Art. 42, que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo,

em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". Nesse sentido, entendeu que além de viabilizar que os dados da vítima estivessem sob domínio dos golpistas, a empresa não tomou medidas para impedir os prejuízos ocasionados. (Autos nº 0727775-94.2021.8.07.0016 TJDF).

CENÁRIO INTERNACIONAL

1. China aprova Lei de Proteção de Informações Pessoais (PIPL)[3]: o Comitê Permanente do Congresso Nacional do Povo da China aprovou no dia 20 de agosto de 2021 a Lei de Proteção de Informações Pessoais (PIPL) , visando aplicar maior rigor na proteção de dados pessoais de seus cidadãos. A PIPL entrou em vigor no dia 01 de novembro de 2021 e foi comparada ao *General Data Protection Regulation* (GDPR) da União Europeia, com disposições que obrigam as empresas a praticar, por exemplo, a minimização de dados e consentimento do usuário. Além disso, também são previstas sanções como o confisco de ganhos ilegais e multas que podem alcançar 50 milhões de Yuans ou 5% da receita anual do exercício financeiro anterior.

2. "Fim dos Cookies": o Google anunciou em janeiro de 2020 que deixaria de prestar suporte aos cookies de terceiros no navegador "Google Chrome" a partir de 2022. Porém, o "fim dos cookies" abre espaço para o *Federated Learning of Cohorts* (FLoC), que em português significa "Aprendizagem Federada de Grupos" e tem como objetivo monitorar o comportamento dos usuários online. A ferramenta permite que o navegador colete dados gerados pelo usuário, que são agrupados junto com outras informações coletadas de mais pessoas com comportamento de navegação semelhante. O recurso não impede o rastreamento dessas pessoas na internet, mas sim que apenas o Google seja o único a fazer isso.

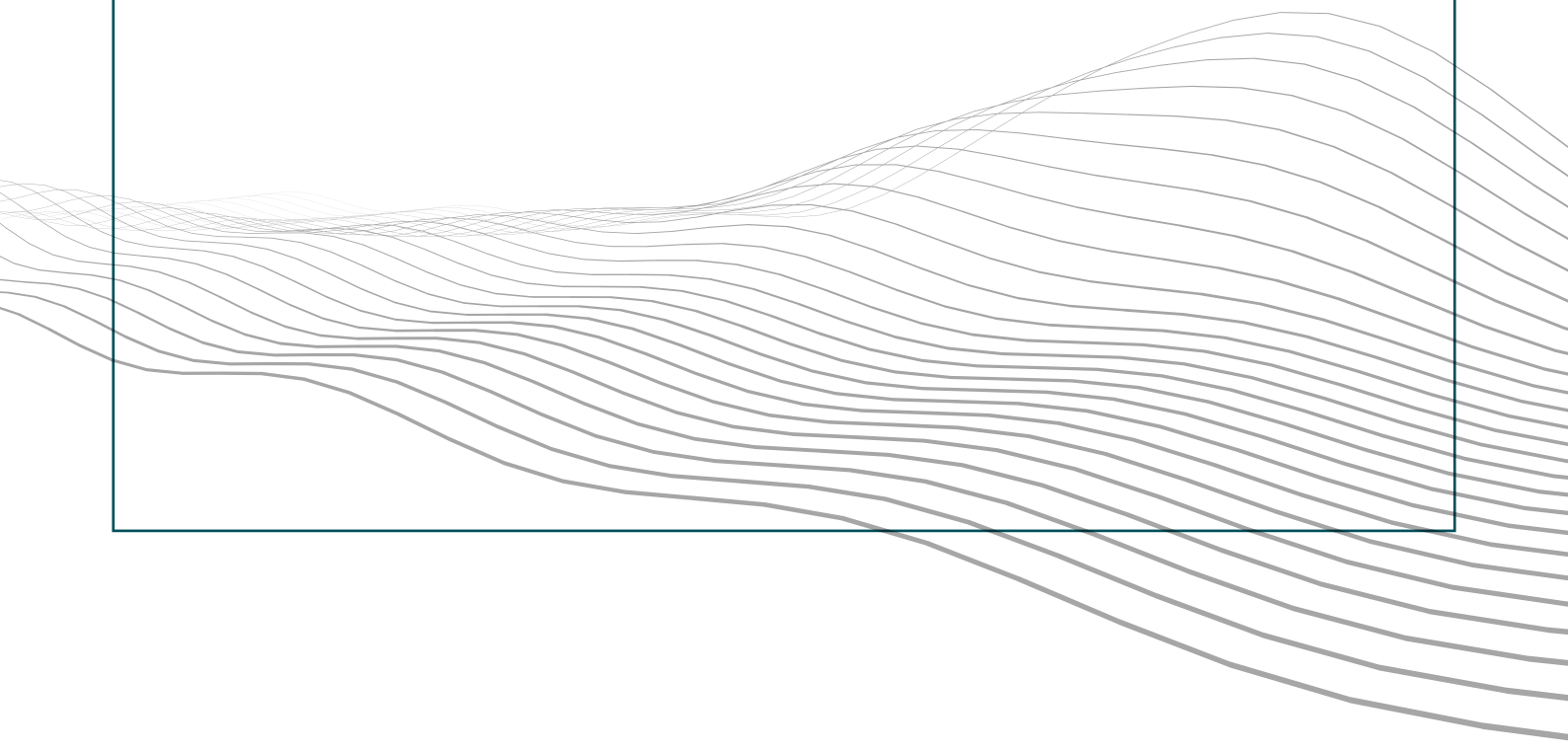
3. Nova Política de Privacidade do WhatsApp e atuação conjunta do CADE, ANPD e Senacon: em 2021, o WhatsApp anunciou que promoveria uma mudança em sua política de privacidade. Na nova versão, o aplicativo de mensagens detalhava o tratamento de dados pessoais dos usuários, afirmando não compartilhar informações com o Facebook, ambas empresas da Meta. Em atuação coordenada e com fundamento na defesa da concorrência e dos consumidores, os órgãos apontaram que a política de privacidade e as práticas de tratamento de dados apresentadas pelo WhatsApp poderiam, em princípio, representar violações aos direitos dos titulares de dados pessoais.

3 - Lei de Proteção de Informações Pessoais (PIPL). Disponível em: http://www.npc.gov.cn/npc/c30834/202108/a8c4e-3672c74491a80b53a172bb753fe.shtml

Para conferir a **Retrospectiva de 2021,** ouça o Podcast PeckNews, em que nossa sócia-fundadora Patricia Peck faz uma avaliação sobre o que foi mais relevante no tema de proteção de dados pessoais no último ano. Acesse no botão abaixo.

OUÇA AQUI A RETROSPECTIVA 2021

O QUE ESPERAR PARA 2022



LGPD E ELEIÇÕES [4]

Diante das eleições gerais, da plena vigência da Lei nº 13.709/2018 (LGPD) e do funcionamento pleno da Autoridade Nacional de Proteção de Dados (ANPD), o direito eleitoral tende a ser um dos principais pontos de discussão acerca de privacidade e proteção de dados no país em 2022.

Antecipando esse cenário, o Tribunal Superior Eleitoral (TSE) e a ANPD firmaram acordo de cooperação técnica no final de 2021 com três objetivos principais: (i) conscientizar os agentes de tratamento da importância da privacidade e proteção de dados nas campanhas eleitorais; (ii) informar os direitos dos titulares e alertar sobre os riscos do uso irregular dos dados pessoais e; (iii) desenvolver um ambiente de segurança jurídica para os agentes que tratam dados no contexto eleitoral.

Neste sentido, logo no início de janeiro de 2022, as autoridades divulgaram o "Guia orientativo para aplicação da LGPD por agentes de tratamento no contexto eleitoral[5]" . O material é um primeiro documento de diretrizes acerca da proteção de dados nas eleições no contexto brasileiro, e, portanto, deve ser observado na construção de toda a estrutura da campanha.

Para fins ilustrativos, podemos destacar cinco pontos interessantes do Guia que refletem a aplicação da LGPD nas eleições:

- **Uso de dados em campanhas:** o Guia reconhece que parte importante do processo eleitoral é que os candidatos e candidatas conheçam os hábitos e opiniões dos eleitores, o que, atualmente, perpassa pela coleta e tratamento de dados. Contudo, deve existir especial atenção ao tratamento de dados dos eleitores, uma vez que a operação pode envolver a existência de dados sensíveis.

- **Agentes de tratamento:** como esperado, o Guia destaca que os partidos, as coligações e os candidatos são agentes de tratamento, assim como instituições contratadas para prestar serviços específicos, sendo preciso analisar o caso concreto para averiguar se o agente estaria figurando como controlador, operador ou até em controladoria conjunta.

- **Legítimo interesse:** tratando das bases legais, o Guia reforça que o legítimo interesse não é aplicável ao tratamento de dados pessoais sensíveis (art. 11, §1º da LGPD). Como exemplos, indica que, no contexto eleitoral, não há legítimo interesse (i) na obtenção de dados custodiados pela administração pública ou por pessoa jurídica de direito privado (ii) na venda de cadastros eletrônicos por pessoas físicas e jurídicas e (iii) na utilização de dados pessoais para envio de propaganda eleitoral por telemarketing.

4 - Texto publicado originalmente no Conjur. Disponível em: <https://www.conjur.com.br/2022-fev-03/opiniao-lgpd-eleicoes--protecao-dados-contexto-brasileiro
5 - Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf. Acesso em: 07.01.2022.

- **Relatório de impacto à proteção de dados pessoais:** o Guia indica que a LGPD não estabelece os casos nos quais a elaboração do relatório é obrigatória. Contudo, destaca que "como no contexto eleitoral pode ocorrer o tratamento de um grande volume de dados sensíveis relacionados a opiniões e filiações políticas, o RIPD se torna um *instrumento importante de accountability.*"

- **Direitos do titular:** o Guia enfatiza que os agentes devem possibilitar que os titulares exerçam todos os direitos previstos pela LGPD e menciona a necessidade de disponibilizar canais de comunicação eficientes e facilmente acessíveis aos titulares.

Por óbvio, o desafio de adequar o processo eleitoral à LGPD é grande para todos os agentes envolvidos e, apesar do Guia apresentar diretrizes, ele não esgota o tema e tampouco exaure as dificuldades práticas que podem surgir. Por exemplo, com relação ao ponto do RIPD indicado acima, como os partidos tratam os dados dos filiados, é recomenda uma postura preventiva de elaboração do documento. Os partidos, via de regra, têm estrutura organizacional e financeira para dar seguimento a essa importante análise. Mas, e as campanhas? Também devem fazer um RIPD para um tratamento que dura somente o período eleitoral?

Igualmente, caso uma campanha não estruture um canal de comunicação para que o titular exerça seus direitos, qual pode ser a sanção aplicada pelo TSE? O Tribunal seguiria com a aplicação de multa ou alguma sanção mais severa poderia ser adotada? A ANPD também poderia adotar procedimentos de fiscalização no caso, e qual seria a dosimetria adequada da pena, com base no art. 52 da ANPD?

O Guia, de forma correta, destaca que o TSE e a ANPD têm funções distintas, e que a ANPD não detém competência para atuar em matérias de competência exclusiva da Justiça Eleitoral. Contudo, também menciona que um mesmo fato pode gerar repercussões a serem analisadas tanto pelo TSE, quanto pela ANPD. Os agentes de tratamento devem estar atentos à complexa relação entre os dois órgãos para evitar punições na seara eleitoral - que podem culminar em cassação do mandato, a depender da gravidade – e sanções da ANPD, que podem prejudicar a própria continuidade do tratamento de dados da campanha ou do partido.

Para além do Guia, este ano, temos novidades que devem obrigatoriamente serem observadas pelos candidatos. Recentemente, atualizando a resolução que trata sobre propaganda[6], o TSE determinou novas previsões para que a legislação eleitoral esteja em acordo com a LGPD.

A resolução exige que a finalidade da coleta deva ser respeitada no tratamento de dados para propaganda eleitoral, inclusive quando envolver dados tornados manifestamente públicos pelo titular, que pode inclusive opor-se ao referido tratamento. No mesmo sentido, se o tratamento realizado for de dados pessoais sensíveis ou quando for possível identificar

6 - Disponível em: https://sintse.tse.jus.br/documentos/2021/Dez/23/diario-da-justica-eletronico-tse-edicao-eleitoral/resolucao-no-23-671-de-14-de-dezembro-de-2021-altera-a-res-tse-no-23-610-de-18-de-dezembro-de-2019-q. Acesso em: 07.01.2022.

titular por meio do cruzamento de bases de dados, deve-se observar o art. 11 da LGPD.

Assim como orientado pelo Guia, as candidatas, os candidatos, os partidos, as federações e as coligações devem instituir canal de comunicação que permita que o eleitor exerça os direitos os titulares previstos no art. 18 da LGPD e informar de forma clara e acessível o meio de acesso ao canal e quem é o encarregado responsável pelo tratamento de dados pessoais.

Um outro ponto que deve continuar sendo destaque na relação entre LGPD e as eleições é o envio de mensagens entre partidos, campanhas e eleitores. É permitido realizar propaganda eleitoral para endereços cadastrados gratuitamente pelo agente de tratamento, desde que presente as hipóteses legais de tratamento com base nos arts. 7º ou 11 da LGPD. Contudo, deve ser oferecida a identificação completa do remetente e dispor mecanismos que permitam solicitar o descadastramento e a eliminação dos dados pessoais, condutas que devem ser adotadas pelo agente em até 48 (quarenta e oito) horas.

Como o envio de mensagens em massa foi um dos temas mais polêmicos das últimas eleições gerais, é preciso destacar o art. 34, II da resolução, que veda a realização de propaganda por meio do disparo em massa sem consentimento do(a) destinatário(a) ou a partir da contratação de expedientes não fornecidos pelo provedor de aplicação.

Interessante ressaltar que a resolução optou por prever expressamente que eventuais abusos e excessos em relação ao tema podem ser objeto de investigação judicial para apurar o uso indevido, desvio ou abuso do poder econômico ou do poder de autoridade, e a utilização indevida de veículos ou meios de comunicação social com base no art. 22 da Lei de Inelegibilidades.

Todo esse panorama indica que será um ano movimentado para a privacidade e proteção de dados pessoais no contexto eleitoral. Será interessante acompanhar como os agentes de tratamento estão se adequando aos preceitos da LGPD e como será a atuação do TSE e da ANPD no período eleitoral que se aproxima.

FISCALIZAÇÃO PELA ANPD E PERSPECTIVA DE REGULAMENTAÇÃO

No início de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) publicou a portaria que previa sua agenda regulatória, após ser aprovada pelo Conselho Diretor. Com vigência total de dois anos, o documento apresentava os 10 (dez) temas prioritários e as iniciativas a serem tomadas pela Autoridade no período, estabelecendo também a forma de regulação (portaria, resolução ou eventual orientação por guia de boas práticas).

Seguindo essa agenda regulatória, a ANPD divulgou o seu Regimento Interno e publicou os seguintes materiais:

- Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado[7];
- Guia orientativo de segurança da informação para agentes de tratamento de pequeno porte e checklist[8];
- Guia orientativo "Como proteger seus dados pessoais", elaborado em parceria com a SENACON/MJSP (Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública)[9];
- Guia orientativo de aplicação da LGPD (Lei Geral de Proteção de Dados Pessoais) no contexto eleitoral, elaborado em parceria com o TSE (Tribunal Superior Eleitoral)[10];
- Guia orientativo para tratamento de dados pessoais pelo poder público[11].

Sobre os regulamentos, a Autoridade já se manifestou:

- Regulamento do processo administrativo sancionador[12];
- Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte[13].

Para o ano de 2022, estão previstas na agenda regulatória da ANPD[14] a publicação das respectivas Resoluções sobre:

- Direitos dos titulares de dados pessoais;
- Estabelecimento de normativos para aplicação do art. 52 e seguintes da LGPD;
- Comunicação de incidentes e especificação do prazo de notificação;
- Relatório de Impacto à Proteção de Dadv os Pessoais (RIPD);
- Encarregado de proteção de dados pessoais;
- Transferência internacional de dados pessoais.

Também está prevista a elaboração de um guia de boas práticas acerca das hipóteses

7 - Disponível em: 2021-05-27-guia-agentes-de-tratamento_final.pdf (www.gov.br)
8 - Disponível em: guia-vf.pdf (www.gov.br) e Checklist alinhado - vf (www.gov.br)
9 - Disponível em: guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf (www.gov.br)
10 - Disponível em: guia_lgpd_final.pdf (www.gov.br)
11 - Disponível em: guia-poder-publico-anpd-versao-final.pdf (www.gov.br)
12 - Disponível em: RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 - RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 - DOU - Imprensa Nacional (in.gov.br)
13 - Disponível em: RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022 - RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022 - DOU - Imprensa Nacional (in.gov.br)
14 - Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

legais de tratamento de dados pessoais e de aplicação da LGPD, incluindo as hipóteses legais descritas no art. 7º (mas não restritas a ele), além de um material **orientativo sobre o tratamento de dados pessoais de crianças e adolescentes**.

SEGURANÇA DA INFORMAÇÃO

Ataques e incidentes cibernéticos marcaram o ano de 2021. Foram tantas ocorrências de vazamentos, roubos e sequestros de dados, que a cibersegurança virou manchete em vários noticiários no início de 2022[15].

Preservar a confidencialidade, integridade e disponibilidade é fundamental para garantir a segurança da informação e a proteção de dados pessoais.
Previstos na LGPD, os Princípios da Segurança e da Prevenção reforçam a necessidade dos agentes de tratamento aplicarem medidas técnicas e administrativas que sejam capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Art. 6º, VII), além de adotarem ações para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (Art. 6º, VIII).

Dessa forma, implementar medidas e controles de segurança da informação e a realização da análise de riscos, visando identificar vulnerabilidades e ameaças, inclusive aquelas decorrentes do tratamento de dados pessoais que podem afetar os direitos e liberdades dos titulares, não são apenas boas práticas a serem realizadas e aplicadas, mas, um verdadeiro dever legal a ser observado[16].

Muitas vezes deixado em segundo plano, o investimento em segurança da informação merece atenção especial, inclusive após o recente estudo realizado pela Cisco[17], que verificou que o retorno sobre o investimento (ROI, em inglês) para investimentos em privacidade e proteção de dados pessoais pode ser de até 3,3 vezes o valor investido, sendo que na média global para cada US$ 1 investido em privacidade e proteção de dados pessoais, o retorno do investimento é de US$ 2,70[18].
O interesse em segurança da informação atinge também os agentes de tratamento de pequeno porte, que podem aproveitar a indicação das medidas técnicas e administrativas

15 - Disponível em: https://valorinveste.globo.com/mercados/brasil-e-politica/noticia/2022/01/10/cibersegurana-entra-na-agenda-de-investimentos-para-este-ano-dizem-analistas.ghtml. Acesso em: 31/01/2022.
16 - Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
17 - Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2022.pdf?CCID=cc000742&DTID=esootr000875. Acesso em: 31/01/2022.
18 - Disponível em: https://valor.globo.com/legislacao/coluna/lgpd-empresas-ja-veem-retorno-do-investimento.ghtml. Acesso em: 31/01/2022.

de segurança da informação, além do checklist publicado pela ANPD no guia orientativo de segurança da informação direcionado aos agentes de tratamento de pequeno porte.

Portanto, com o início do ciclo de monitoramento da ANPD (como veremos no tópico a seguir), e o aumento dos casos de ataques e incidentes cibernéticos, a Segurança da Informação se manterá em alta em 2022, visando, também, a manutenção da confiança da marca perante o mercado, consumidores e parceiros.

AUDITORIAS INTERNAS: FOCO NA CONFORMIDADE

Dentre os princípios basilares da LGPD, a responsabilização e prestação de contas (Art. 6º, X) prevê que os agentes de tratamento devem ser capazes de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

Além disso, são requisitos mínimos de um Programa de Governança em Privacidade (Art. 50, §2º, I):

1. **Demonstrar o comprometimento do controlador em adotar processos e políticas internas** que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais (a);
2. Estar integrado a sua estrutura geral de governança e **estabelecer e aplicar mecanismos de supervisão internos e externos** (f);
3. Seja atualizado constantemente com base em informações obtidas a partir de **monitoramento contínuo e avaliações periódicas** (h).

Isso reforça a necessidade de possuir evidências capazes de demonstrar a efetividade do Programa de Governança em Privacidade ("Programa") quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas (Art. 50, §2º, II).

A auditoria é um processo sistemático, independente e documentado para obter evidência objetiva[19] e avaliá-la objetivamente, para determinar a extensão na qual os critérios de auditoria[20] são atendidos (Subitem 3.1, ISO/IEC 19011:2019).

A fim de mensurar sua conformidade, os agentes de tratamento podem executar auditorias internas (auditoria de primeira parte), submeter ou serem submetidos a auditorias conduzidas por partes interessadas na organização, como os fornecedores externos (auditoria de segunda parte). Por fim, também é possível submeter-se a auditorias que

19 - Evidência objetiva: Dados que apoiam a existência ou a veracidade dos controles (Subitem 3.8, ISO/IEC 19011:2019).
20 - Critérios de auditoria: Conjunto de requisitos usados como uma referência com a qual a evidência objetiva é comparada (Subitem 3.7, ISO/IEC 19011:2019).

visam a certificação e/ou acreditação conduzidas por organismos de auditoria independente (auditoria de terceira parte).

Fato é que um Programa de Governança em Privacidade envolve a necessidade de revisão e melhoria contínua das medidas e controles de segurança como todo processo (PDCA – *plan, do, check, act*). Já a auditoria é uma possibilidade que pode auxiliar na checagem da maturidade do Programa da organização, bem como contribuir na identificação de gaps que resultarão em planos de ação a serem executados para saná-los.

Em 28 de outubro de 2021, foi publicada a Resolução CD/ANPD nº 1 que aprovou o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Com isso, estabeleceu-se **o primeiro ciclo de monitoramento, com início em janeiro de 2022** (Art. 70, Res. CD/ANPD nº1).

Tendo em vista que podem ocorrer fiscalizações pela ANPD, uma tendência em 2022 para quem deseja alcançar a conformidade é a revisão dos controles e medidas de segurança implementados no âmbito do Programa de Governança em Privacidade. Não espere a ANPD bater à sua porta para verificar que os controles do Programa de Governança em Privacidade não são seguidos ou que não funcionam corretamente no dia a dia da organização.

PROTEÇÃO DE DADOS E DIREITO CONCORRENCIAL

Na atual era do *Big Data*, na qual os dados são considerados o "novo petróleo", as condutas anticompetitivas nada combinam com a realidade de uma Economia Digital. Para que o mercado corresponda à nova configuração que se desenha, é necessário estimular a promoção da livre concorrência e a apreciação de atos de concentração (fusões e aquisições) entre empresas, para que não haja atividades lesivas à ordem econômica.

Em 2021, a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Administrativo de Defesa Econômica (CADE) firmaram o Acordo de Cooperação Técnica nº 5/2021[21], para estabelecer a atuação coordenada em casos de infração à ordem econômica que envolvam dados pessoais, como é o caso de fusões e aquisições entre empresas com transferência de dados. Com o ACT, os referidos órgãos irão atuar de forma coordenada em atos de concentração e investigações de condutas anticompetitivas relativos a serviços que envolvam dados pessoais pelo prazo de 60 (sessenta) meses.

A livre iniciativa, a livre concorrência e a defesa do consumidor são fundamentos da proteção de dados pessoais (Art. 2º, VI) e, em 2022, a tendência é o crescimento da atuação

21 - Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf. Acesso em: 31/01/2022.

coordenada do CADE-ANPD com a fiscalização de infrações à ordem econômica que envolvam dados pessoais.

TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

O tratamento de dados pessoais de crianças e adolescentes é um assunto que vem levantando discussões em relação à interpretação dos dispositivos legais da LGPD, em razão de lacunas e omissões.

Nos termos do art. 14 da LGPD, o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

Outrossim, cabe ressaltar que a legislação brasileira considera como criança a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade, nos termos do artigo 2º da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente (ECA).

O primeiro ponto de discussão **refere-se à legitimação do tratamento de dados pessoais**. Nos termos do primeiro parágrafo do art. 14 da LGPD, o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal. Ainda, há a previsão de dispensa de consentimento quando a coleta dos dados for necessária para contatar os pais ou o responsável legal, uma única vez e sem armazenamento, ou para sua proteção, nos termos do parágrafo terceiro.

Referido dispositivo levanta questões como: o consentimento é a única base legal permissiva ao tratamento de dados pessoais de crianças? Em relação aos adolescentes, houve uma falha do legislador em não os mencionar ou sua omissão foi intencional? Há a possibilidade de legitimar o tratamento de dados pessoais nos artigos 7° e 11 da LGPD?

A respeito dessas indagações, entende-se que o tratamento de dados pessoais tanto de crianças, como de adolescentes, pode ser realizado mediante quaisquer bases legais constantes nos artigos 7º e 11 da LGPD em combinação com o artigo 14 da LGPD, situação em que se deve realizar uma análise casuística quanto ao melhor interesse.

Assim, quando a base legal for o consentimento, seja para o tratamento de dados pessoais ou dados pessoais sensíveis, este deve ser coletado na forma do parágrafo primeiro do artigo 14 da LGPD, ou seja, “específico e em destaque dado por pelo menos um dos pais ou responsável legal”.

Para além da problemática quanto à legitimação do tratamento, outro ponto de discussão por causa da omissão legislativa refere-se à necessidade ou não de se realizar um **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**, quando do tratamento de dados de crianças e adolescentes, de forma a identificar os riscos inerentes ao tratamento, bem como quanto melhor interesse.

Conforme conceitua a LGPD, o RIPD trata-se de um documento do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (art. 5º, inciso XVII, da LGPD).

A LGPD não trata da sua obrigatoriedade em nenhum caso, mencionando apenas que a Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitá-lo em atividades de monitoramento e fiscalização, como no caso da utilização da base legal do legítimo interesse, bem como poderá determinar sua realização, inclusive quando do tratamento de dados pessoais sensíveis.

A resolução de tais lacunas e omissões deve ser tratada com urgência, pois se trata de titulares vulneráveis e que merecem atenção especial. A Autoridade Nacional de Proteção de Dados (ANPD), em sua agenda regulatória para o biênio 2021-2022, publicada através da Portaria nº 11/2021, tinha como previsão a regulamentação do Relatório de Impacto à Proteção de Dados no primeiro semestre de 2021, contudo até o momento nenhuma resolução foi emitida pelo órgão.

Em relação às divergências acerca da legitimação do tratamento de dados pessoais, há a previsão de regulamentação das hipóteses legais de tratamento de dados pessoais para o segundo semestre de 2022. Entretanto, não se sabe se referida regulamentação abrangeria as questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes. De toda forma, trata-se de um assunto que merece atenção especial pela ANPD.

Contudo, enquanto não exista um posicionamento pelo órgão, a recomendação é que cada tratamento a ser realizado seja analisado individualmente, considerando o arcabouço jurídico de proteção de dados pessoais e as legislações vigentes sobre o tema, em especial o Estatuto da Criança e do Adolescente (ECA).

Ademais, é oportuno lembrar as **obrigações a serem cumpridas pelos controladores** quando do tratamento de dados de crianças e adolescentes:

> **(i)** a determinação de manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares (§2º, do art.14 da LGPD);
>
> **(ii)** a proibição de condicionamento de participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das

estritamente necessárias à atividade (§4º, do art. 14 da LGPD);

(iii) a necessidade de realizar esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis (§5º, do art. 14 da LGPD); e

(iv) o fornecimento das informações sobre o tratamento de dados deverá ser feito de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. (§6º, do art. 14 da LGPD).

Tais obrigações devem ser observadas pelos controladores de dados pessoais, de forma que o tratamento de dados de crianças e adolescentes ocorram em conformidade com a Lei Geral de Proteção de Dados Pessoais e as boas práticas de mercado.

CRIMINALIZAÇÃO DE CONDUTAS QUE VIOLEM A PROTEÇÃO DE DADOS PESSOAIS

A criminalização de condutas por violações à proteção de dados pessoais é um tema que vem sendo muito discutido. No ano de 2021, diversas empresas foram vítimas de ataques de ransomware.

Em um estudo realizado pela Sopho[22], empresa britânica de cibersegurança, o Brasil encontra-se em 15º lugar dos países que tiveram organizações atingidas por ransomware. Das 200 empresas entrevistadas, 38% sofreram ataques no último ano.

Condutas como ataques, indisponibilização, roubos de banco de dados pessoais, obtenção de vantagens indevidas pelo uso de dados pessoais, entre outras, devem ser criminalizadas de forma a garantir maior segurança aos titulares, bem como de organizações que realizam o tratamento dessas informações.

Embora seja obrigação dos agentes de tratamento a adoção de medidas técnicas e organizacionais de segurança, e de boas práticas de governança, é sabido que nem a melhor tecnologia disponível hoje no mercado é capaz de impedir ataques maliciosos.

Países como Portugal, Itália e Reino Unido já possuem legislações que criminalizam condutas que violam as legislações de proteção de dados.

22 - https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

- Em Portugal, a Lei nº 58/2019 tipifica crimes no tratamento de dados pessoais, como a utilização de dados de forma incompatível com a finalidade da recolha (Art. 46), o acesso indevido (Art. 47), o desvio de dados (Art. 48), a violação ou destruição de dados (Art. 49), a inserção de dados falsos (Art. 50), a violação do dever de sigilo (Art. 51), entre outros, com penas de prisão que variam de um a dois anos.[23]

- Já na Itália, o Decreto Legislativo 196/2003 (Código de Privacidade), tipifica condutas como o tratamento ilegal de dados (Art. 167), a comunicação e divulgação ilícita de dados pessoais sujeitos a tratamento em grande escala (Art. 167.2), a aquisição fraudulenta de dados pessoais sujeitos a tratamento em grande escala (Art. 167.3), entre outros, com penas de prisão que vão de seis meses a três anos.[24]

- No Reino Unido, por sua vez, a Lei de Proteção de Dados de 2018 (*Data Protection Act* 2018[25]) tipifica condutas como a obtenção ilegal de dados pessoais (Art. 170), a reidentificação de dados pessoais não identificados (Art. 171), a alteração etc. de dados pessoais para impedir a divulgação ao titular dos dados.

No ordenamento jurídico brasileiro há a tipificação de condutas que versam sobre a privacidade dos indivíduos, como a Lei Carolina Dieckmann (nº 12.737/12), que tipifica a conduta de invadir dispositivo informático com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obtenção de vantagem ilícita.

Entretanto, não há legislações que tratam especificamente de violações à proteção de dados pessoais, como ataques, roubos, indisponibilizações de dados com obtenção de vantagem econômica.

Assim, a criminalização de condutas que violam a proteção de dados pessoais é um assunto extremamente importante e que deve ser levado em consideração.

23 - https://www.uminho.pt/PT/uminho/protecao-de-dados/Paginas/Crimes-no-tratamento-de-dados-pessoais.aspx
24 - https://www.altalex.com/documents/news/2013/09/26/tutela-dell-interessato-e-sanzioni
25 - https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Quer saber mais sobre as principais tendências de 2022?

Acesse o vídeo no QRcode abaixo e confira a análise da nossa sócia-fundadora Patricia Peck do que esperar em relação à proteção de dados pessoais para este ano.

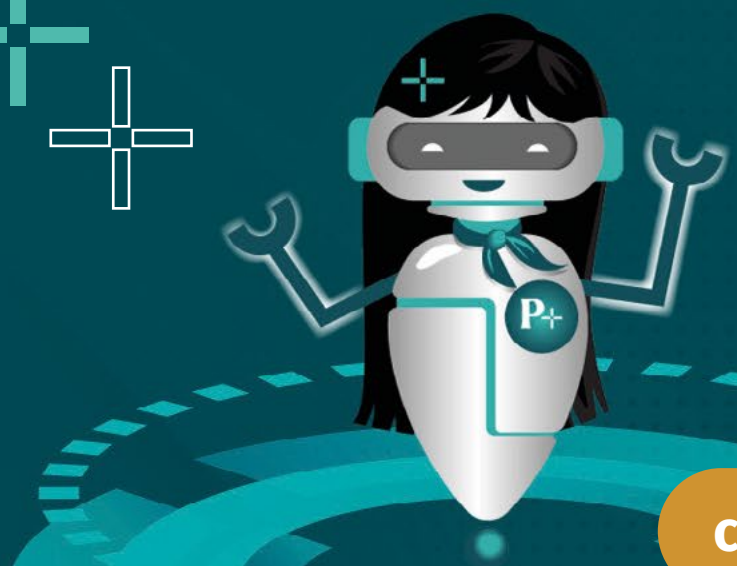
CLIQUE AQUI PARA VER

Peck+
Advogados

Direito para Inovação Digital

COM QUANTOS DADOS SE FAZ UMA PROTEÇÃO?

Jogue com sua equipe e descubra como está a conformidade da organização com a LGPD.



Privy+

CLIQUE PARA JOGAR

Legal | Innovation
Data Protection | Day

Peck+
Advogados
Direito para Inovação Digital

APOIADORES

CREDILINK® INFORMAÇÕES DE CRÉDITO
SIKUR
tabapuã CONSULTORIA EM SEGUROS
THALES Together • Safer • Everywhere
OneTrust PRIVACY, SECURITY & GOVERNANCE
EXIN
securiti
palqee

Siga-nos nas Redes Sociais: