

Proteção de Dados:

panorama sobre as sanções no mundo
e previsão de multas da ANPD a partir
de fevereiro



20

23

Por: Daniela Machado e Míriam Ferreira
Diagramação: Anaís Moura
Coordenação: Clarissa Luz
Equipe de Privacidade, Proteção de Dados e Tecnologia:
privacy@felsberg.com.br

INTRODUÇÃO

Fevereiro, alegria, carnaval e... sanções da ANPD? Em diversos eventos ocorridos na última semana do (longo) mês de janeiro, o presidente da Autoridade Nacional de Proteção de Dados (ANPD), Waldemar Gonçalves, afirmou que o “Regulamento de Dosimetria e Aplicação de Sanções Administrativas” encontra-se em fase final de elaboração, devendo ser aprovado ainda em fevereiro.

E o que isso representa para as empresas, uma vez que a Lei Geral de Proteção de Dados Pessoais (LGPD) está em vigor desde 18 de setembro de 2020?



Significa dizer que, além das indenizações que já vem sendo aplicadas no âmbito do Poder Judiciário – em litígios individuais e coletivos – e pelos órgãos que integram o Sistema Nacional de Defesa do Consumidor, como a Secretaria Nacional do Consumidor¹ (Senacon) e os Procons², a ANPD passará, muito em breve, a aplicar sanções às empresas que tratam dados pessoais.

Trata-se, portanto, de um passo fundamental no caminho para a concretização da eficácia plena da LGPD e do estabelecimento de uma cultura que contemple a proteção a dados pessoais no Brasil. Ao definir claramente os parâmetros e a metodologia para fixação das sanções previstas no artigo 52 e respectivos incisos da LGPD, a ANPD garante aos agentes de tratamento maior segurança jurídica, vez que permite maior previsibilidade sobre as consequências de atos contrários à referida lei.



O tema foi objeto de consulta pública iniciada em agosto de 2022, tendo recebido **2.504** contribuições de entidades e membros da sociedade civil, empresas e profissionais da área. Prevê-se que, com a conclusão do normativo, a ANPD passe a atuar de maneira mais incisiva na fiscalização e penalidade aos agentes de tratamento, a começar por **08** processos pendentes de decisões da autoridade, conforme mencionado por Waldemar Gonçalves.

Frise-se que o [Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador](#) foi aprovado pela Resolução CD/ANPD nº 1/2021, outro normativo de extrema relevância que, somado aos critérios de dosimetria, assegura aos agentes de tratamento o respeito aos princípios constitucionais do devido processo legal, contraditório e ampla defesa.

Na tentativa de ilustrar os impactos da consolidação de leis de privacidade e proteção de dados mundo afora e da atuação de autoridades nacionais de proteção de dados, preparamos uma pesquisa³ que buscou identificar, a nível global, as condenações de maior destaque dos últimos anos, a evolução dos valores de multas aplicadas e a abrangência das condutas penalizadas.

A seguir, apresentamos algumas reflexões acerca dos dados encontrados a partir dessa pesquisa:

1 - Disponível em [aquí](#). Acesso em 02.02.2023 2 - Disponível em [aquí](#). Acesso em 02.02.2023

3 - A pesquisa é de natureza qualitativa e não quantitativa, baseada nas informações disponíveis em sites de autoridades nacionais de proteção de dados, tribunais, órgãos administrativos e páginas especializadas em compêndios de temas jurídicos internacionais, a exemplo do "Data Guidance" e "GDPR Enforcement Tracker".

Maiores multas encontradas



Estados Unidos



China

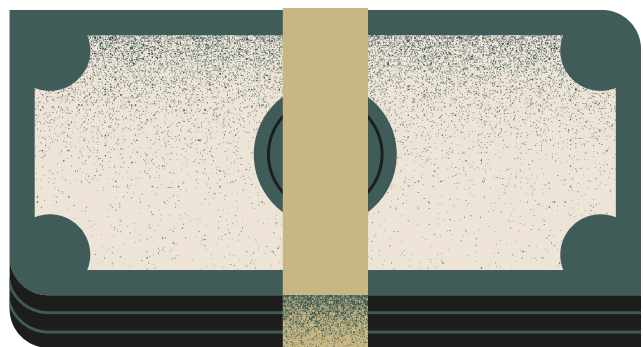




















União Europeia



Concentram as maiores multas, com cifras entre centenas de milhões a bilhões de dólares. Com icônicas decisões, se havia alguma dúvida, têm-se demonstrado que deve haver uma nova forma de operar com dados no mercado: as condenações voltam-se a punir não apenas os incidentes de segurança graves, como vazamento de dados pessoais, como também a falta de transparência e adequação às bases legais e finalidades para um legítimo tratamento de dados pessoais.

Destacamos aqui as condenações com as maiores multas aplicadas até o momento⁴:



PAÍS	ANO	SETOR	MULTA	VIOLAÇÃO
 Estados Unidos	2019	 Tecnologia	USD 5 bilhões	Falta de transparência sobre o tratamento de dados pessoais
 China	2022	 Tecnologia	USD 1,2 bilhões	Coleta de informações por meio de printscreen do album de fotos dos celulares de usuários e coleta biometria facial de passageiros sem o fornecimento de informações aos titulares e obtenção do consentimento para o tratamento dos dados
 Luxemburgo	2021	 Tecnologia	EUR 746 milhões (~ USD 877 milhões)	Tratamento de dados de clientes para fins de marketing direto sem a devida coleta de consentimento para tal finalidade
 Irlanda	2022	 Tecnologia	EUR 405 milhões (~ USD 429 milhões)	Exposição excessiva de dados pessoais de crianças e adolescentes, por configuração padrão da plataforma, que permitia a visualização indiscriminada por terceiros de dados como e-mail e telefone
 Irlanda	2023	 Tecnologia	EUR 390 milhões (~ USD 413 milhões)	Falta de transparência sobre o tratamento de dados pessoais
 Estados Unidos	2022	 Comunicação	USD 350 milhões	Falha na adoção de medidas eficazes de segurança da informação, resultando no vazamento de dados de mais de 75 milhões de consumidores
 Irlanda	2021	 Tecnologia	EUR 225 milhões (~ USD 255 milhões)	Falta de transparência sobre as finalidades e meios de tratamento dos dados aos seus titulares
 Estados Unidos	2020	 Varejo	USD 200 milhões	Falha na adoção de medidas de segurança da informação hábeis a proteger a integridade dos dados tratados, resultando na exposição indevida de dados de 40 milhões de indivíduos
 Estados Unidos	2022	 Fintech	USD 190 milhões	Falha na adoção de medidas eficazes de segurança da informação, resultando no vazamento de dados de mais de 100 milhões de pessoas

A aplicação de multas em tamanha proporção, porém, é resultado de um processo evolutivo, sendo que o Regulamento Europeu de Proteção de Dados (*General Data Protection Regulation – GDPR*), referência para a criação da LGPD e leis de demais países, foi também um evento propulsor da defesa da privacidade e da proteção dos dados pessoais pela União Europeia afora.

GDPR sem fronteiras

Ultrapassando fronteiras, a pesquisa revelou uma grande repercussão do GDPR em todo o mundo, sendo patente o reforço do caráter protetivo do poder estatal e a ênfase na força coercitiva e punitiva.

Observou-se uma expansão da esfera de proteção aos direitos à privacidade e proteção de dados para além da União Europeia, um efeito cascata motivado, em grande parte, pelos mecanismos previstos pelo GDPR para a transferência de dados pessoais para fora do Espaço Econômico Europeu.

Os impactos alcançaram também a natureza das violações, até então essencialmente centradas na proteção ao consumidor em casos de vazamentos de dados ou uso ilegítimo de dados em ações de marketing. Mesmo em países desprovidos de legislação específica sobre o tema, verificou-se, a partir da vigência do GDPR, um processo de empoderamento dos titulares sobre suas informações pessoais e uma crescente atuação estatal na repressão ao uso indiscriminado dessas informações.





EUA

Nos Estados Unidos, as maiores multas anteriores à GDPR recaíam exclusivamente sobre incidentes graves de vazamentos de dados pessoais e representavam ainda percentual ínfimo do faturamento das empresas condenadas:

[SAIBA MAIS](#)



BRASIL

Antes da entrada em vigor da LGPD, as condenações no Brasil relativas à privacidade e proteção de dados respaldavam-se nos princípios constitucionais, no Código de Defesa do Consumidor, Marco Civil da Internet, entre outros, sendo que as situações que alcançavam os tribunais de forma mais recorrente versavam quase exclusivamente sobre o uso não autorizado de dados para marketing direto, as quais ocasionaram módicas condenações por dano moral – com valores que giravam em torno de R\$ 5.000,00 a R\$ 10.000,00.

[SAIBA MAIS](#)



FELSBERG
ADVOGADOS

Estados Unidos



MEADOS DE 2017

Um ataque hacker que expôs os dados de aproximadamente 40 milhões de cartões de crédito e débito gerou diversas ações contra a Target, empresa do setor de varejo, resultando em condenações que somam **USD 18,5 milhões**⁵.



MAIO DE 2018



Foi julgado um dos maiores incidentes de vazamento de dados pessoais – a exposição de informações de aproximadamente 3 bilhões contas de usuários do Yahoo!, com a condenação da empresa ao pagamento de multa no valor de **USD 35 milhões**⁶.

Com a entrada em vigor do GDPR, as multas aumentaram expressivamente, e passaram a punir, inclusive, situações que não envolviam vazamento ou dano patrimonial direto, mas também a mera violação da transparência e da autonomia dos titulares quanto ao controle sobre o tratamento realizado sobre seus dados pessoais:

OUTUBRO DE 2018

A Uber foi condenada a pagar uma multa no montante de **USD 148 milhões**, pelo vazamento de dados de 57 milhões de usuários em um incidente de segurança ocorrido em 2016⁷.



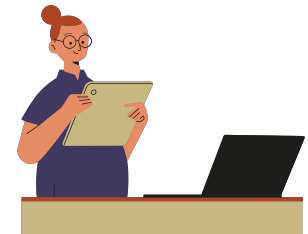
JULHO DE 2019



Outro julgamento, levou à condenação da Equifax, também por vazamentos de dados. A multa inicial de **USD 575 milhões** pode chegar a **USD 700 milhões** até o fim do prazo prescricional para a propositura de demandas de titulares prejudicados pelo incidente, o que ocorrerá apenas em janeiro de 2024⁸.

MEADOS DE 2019

A Federal Trade Commission condenou a então Facebook, Inc. ao pagamento de **USD 5 bilhões** pela falta de transparência e assertividade nas informações prestadas aos usuários de sua plataforma de rede social quanto ao uso e monetização de seus dados pessoais no contexto do famoso caso Cambridge Analytica⁹.



Brasil



Apenas em casos esparsos mais icônicos houve multas na cifra de milhões de reais, como a condenação de uma das maiores empresas de telecomunicação brasileiras à época em **R\$ 1,5 milhões** pelo compartilhamento não autorizado de dados pessoais, em 2017¹⁰.

A partir do segundo semestre de 2018, porém, as repercussões da GDPR se fizeram sentir também em solo brasileiro. No mês de dezembro, uma rede de farmácias foi multada em **R\$ 7 milhões** pela falta de transparência quanto às finalidades do cadastro de dados pessoais em sua plataforma¹¹.

Enfrentando grandes *players* do mercado, em março de 2021, a Microsoft firmou um Termo de Ajustamento de Conduta em decorrência de uma ação civil pública motivada pela coleta de dados sem a devida autorização dos usuários para as finalidades empregadas em seu tratamento, resultando em um pagamento de **R\$ 2,5 milhões** para reparação de danos¹².

Mantendo a tendência a multas mais elevadas, em junho de 2022 a Decolar.com foi condenada pela Senacon a pagar **R\$ 2,5 milhões** por violação ao princípio da transparência pela utilização de dados para a prática de *geopricing*¹³.



10 - 1ª Vara Federal de Campo Grande - Processo nº 0000909-02.2013.403.6003 - Sentença publicada em 20/10/2017. Disponível [aqui](#). Acesso em 03.02.2023.

11 - [Link](#)

12 - Disponível [aqui](#). Acesso em 03.02.2023.

13 - [Link](#)

Outras Localidades

Abaixo, segue breve comparativo entre os valores e as motivações de condenações pré e pós vigência do GDPR em diferentes jurisdições:



Hong Kong¹⁴

MAIOR CONDENAÇÃO ANTES DO GDPR

HK\$ 16.000,00 (~ USD 2.040,00)



Ausência de consentimento para uso de dados pessoais em marketing direto

MAIOR CONDENAÇÃO APÓS O GDPR

HK\$ 84.000,00 (~ USD 10.705,00)



Desrespeito à solicitação para cessação da utilização de dados pessoais para marketing direto

14 - [Link 1](#) | [Link 2](#)



Cingapura¹⁵

MAIOR CONDENAÇÃO ANTES DO GDPR

SG\$ 60.000,00 (~ USD 45.556,00)



Vazamento de dados pessoais

MAIOR CONDENAÇÃO APÓS O GDPR

SG\$ 1 milhão (~ USD 759.270,00)



Vazamento de dados pessoais

15 - [Link 1](#) | [Link 2](#)



Reino Unido¹⁶

MAIOR CONDENAÇÃO ANTES DO GDPR

£ 325.000,00 (~ USD 394.434,00)



Exposição de dados pessoais por falha de segurança no procedimento de exclusão

MAIOR CONDENAÇÃO APÓS O GDPR

£ 20 milhões (~ USD 24.272.900,00)



Vazamento de dados pessoais

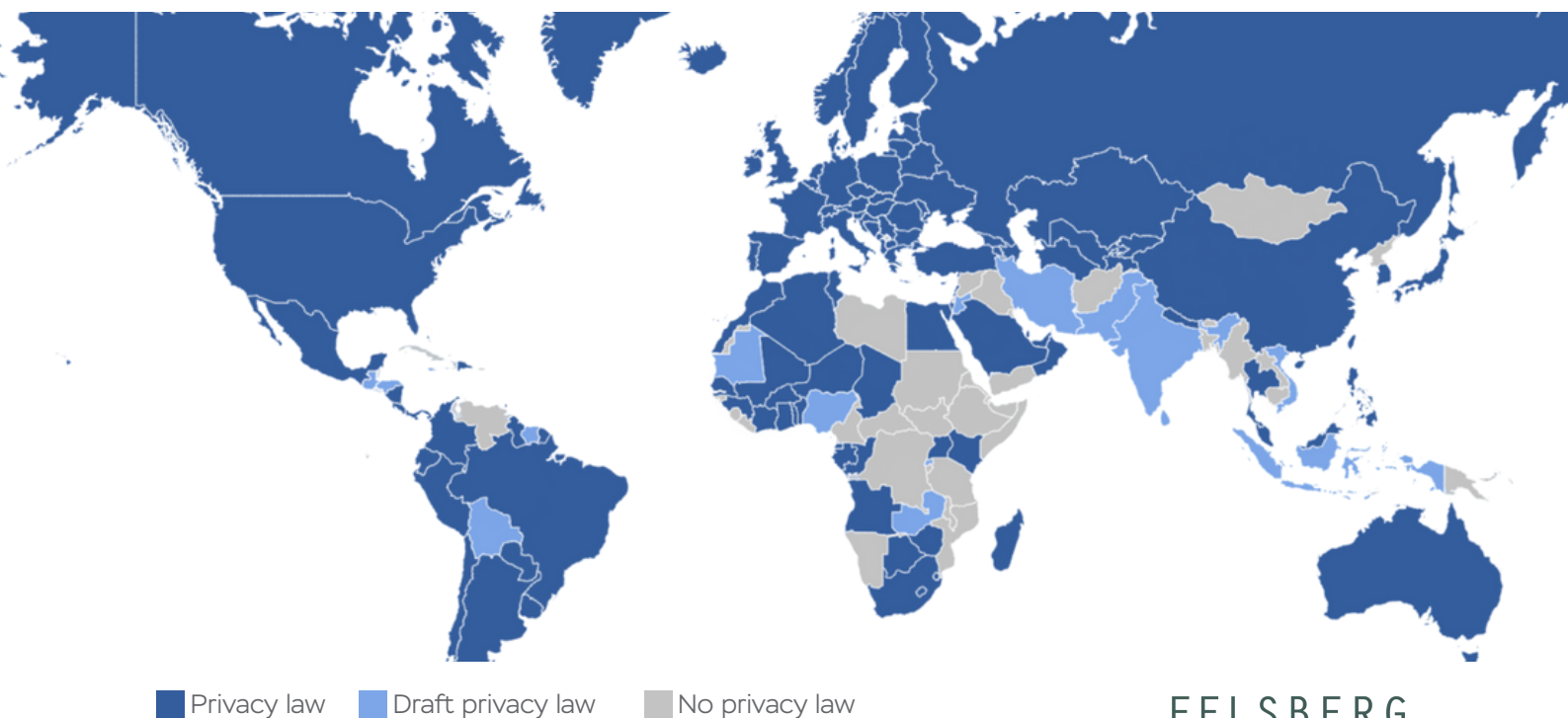
16 - [Link 1](#) | [Link 2](#)

CONCLUSÃO

A análise do panorama mundial, desde a perspectiva histórica até o momento atual, e as recentes movimentações da ANPD com relação a medidas sancionadoras reforçam a importância da adequação da atividade empresarial à LGPD. Na Era dos Dados, levar a sério a proteção às informações dos indivíduos não é apenas uma opção, mas um requisito crucial para a sobrevivência da empresa e sua operação no novo mercado.

A consolidação da tutela dos direitos de privacidade e proteção de dados a nível mundial demanda a atenção das empresas aos princípios que regem a regulamentação desses direitos e buscam garantir aos titulares o tratamento ético dos seus dados, sob pena de perda de mercado e de relações comerciais transfronteiriças.

O mapa abaixo é um reflexo do engajamento global na edição e/ou atualização de normas protetivas aos direitos de privacidade e proteção de dados pessoais¹⁷:



17 - Disponível [aqui](#). Acesso em 02.02.2023.

As legislações nacional e internacional fomentaram uma ampliação tanto da abrangência da tutela, quanto do valor das penalidades aplicadas, sendo que o valor das multas é apenas a ponta do *iceberg* dos reveses causados à empresa em decorrência de uma condenação. Fatores como a perda de credibilidade e de valor de mercado, o alto investimento necessário para restabelecer a integridade de um sistema vítima de incidente de segurança e o monitoramento posterior dos dados afetados podem representar impactos de ordem financeira e reputacional inestimáveis.

A privacidade veio para ficar. Segundo declarações proferidas por Waldemar Gonçalves em eventos de comemoração do Dia da Privacidade, as denúncias recebidas pela ANPD até o momento já ultrapassam 6,9 mil, quantidade que evidencia a evolução de uma cultura de privacidade, na qual os indivíduos compreendem o valor de seus dados e buscam a garantia de seus direitos.

A construção de um programa de governança eficaz em privacidade e proteção de dados e a adoção de uma postura de respeito em relação aos titulares, tornaram-se requisitos básicos para a conquista da confiabilidade dos consumidores.

Cabe às empresas enxergar o “copo meio cheio” e transformar a proteção de dados pessoais em um agregador de valor aos seus produtos e serviços perante o mercado e a sociedade.



2023

Por: Daniela Machado e Míriam Ferreira
Diagramação: Anaís Moura
Coordenação: Clarissa Luz
Equipe de Privacidade, Proteção de Dados e Tecnologia:
privacy@felsberg.com.br