

# INDICADORES GLOBAIS

ATUAÇÃO DAS AUTORIDADES NACIONAIS DE  
PROTEÇÃO DE DADOS EM PROCESSOS  
SANCIONATÓRIOS ENVOLVENDO AGENTES  
DE TRATAMENTO

3ª EDIÇÃO

Lançado em 2006 pelo Conselho da Europa e inspirado pela Convenção 108, o pioneiro tratado multilateral em matéria de proteção de dados pessoais, o **Data Privacy Day – o Dia da Proteção de Dados** - é celebrado anualmente no dia 28 de janeiro. O dia foi escolhido para homenagear a data de adoção da Convenção 108, em 28 de janeiro de 1981 e, desde então, tem ganhado reconhecimento e celebração em diversas partes do mundo.

Simbolicamente, o **Data Privacy Day** tem sido repercutido em várias partes do mundo e tem como objetivo trazer visibilidade, fomentar a conscientização e provocar discussões especializadas sobre privacidade e proteção de dados pessoais para indústria, governos, academia, sociedade civil e os titulares de dados.

A ideia de celebrar essa data festiva tem sido mantida e amplificada por várias iniciativas, como seminários, campanhas de conscientização, publicações acadêmicas e debates jurídicos ao redor do globo. Elas refletem a importância crescente que a proteção de dados assume em diversas esferas sociais e profissionais. Essas atividades não apenas educam, mas também incentivam organizações e indivíduos a adotarem práticas mais robustas, bem como transparentes de maneira que possam assegurar a proteção de informações e dados pessoais, fortalecendo o compromisso com a privacidade e proteção de dados como direitos fundamentais, a serem garantidos e potencializados em várias áreas da vida social.

## Sobre o estudo

Nesta **terceira edição** da publicação Indicadores Globais sobre Privacidade e Proteção de Dados, buscamos oferecer a visão geral da atuação e perfil institucional de Autoridades Nacionais de Proteção de Dados pelo mundo, sobretudo para servir de base de conhecimento para os agentes de tratamento na indústria e titulares de dados no Brasil.

A ideia de um estudo dessa natureza também é o de proporcionar uma visão analítica sobre como a Autoridade Nacional de Proteção de Dados (ANPD) poderá aproveitar as melhores práticas e experiências comparadas, de modo a construir um arcabouço estável e previsível nos processos sancionatórios envolvendo agentes de tratamento no Brasil.

Importante destacar que, em outubro de 2023, a ANPD foi oficialmente reconhecida como [membro integral do Global Privacy Assembly](#) ("GPA"). De acordo com a própria ANPD, essa nova posição como membro efetivo consolida um marco de cooperação internacional em questões de proteção de dados, de modo a incrementar a proteção legal para cidadãos e corporações brasileiras e de facilitar o fluxo e intercâmbio de dados pessoais para além das fronteiras nacionais. A ANPD também reconheceu que sua inclusão no GPA contribui para uniformizar leis e regulamentos relacionados a dados pessoais em nível global e promover ações conjuntas e mais eficazes entre os órgãos reguladores internacionais de proteção de dados.

Por outro lado, é também esperado que a ANPD tenha condições de manter suas ações em consonância com os indicadores globais produzidos a partir da experiência das Autoridades Nacionais de Proteção de Dados ao redor do mundo. Esse aspecto também sugere o objetivo de harmonização dos esforços regulatórios e práticas institucionais em matéria de privacidade e proteção de dados, o que é sinal positivo para a indústria e empresas que operam em múltiplas jurisdições. A uniformidade é sempre benéfica, sobretudo por proporcionar um entendimento mais claro das expectativas regulatórias, independentemente das fronteiras geográficas.

Boa leitura!

# Introdução

Na [primeira edição desta publicação](#), lançada em 2022, [o time de Privacidade e Proteção de Dados de L.O.Baptista](#), liderado pelos sócios **Esther Jerussalmy Cunha** e **Fabricio Polido**, realizou o estudo inédito e pioneiro no Brasil, para retratar o desenvolvimento robusto de indicadores globais em data privacy, com foco na atuação das Autoridades Nacionais de Proteção de Dados em processos sancionatórios envolvendo agentes de tratamento.

Já em 2023, a [segunda edição](#) foi elaborada de modo a verificar o desenvolvimento dos processos sancionatórios por países e regiões considerados estratégicos e estabelecer as estimativas de valores de multas aplicadas por setores da indústria mais visados.

Nesta terceira edição, enriquecemos o estudo com novos elementos. Mantivemos o objetivo central do trabalho de analisar comparativamente as experiências e práticas envolvendo os processos fiscalizatórios e sancionatórios em matéria de proteção de dados, com o objetivo de informar e conscientizar agentes de tratamento, autoridades governamentais, organizações da indústria e titulares de dados.

Ao longo das rodadas de estudos, em 2021, 2022 e 2023, no entanto, observamos o comportamento mais robusto das Autoridades Nacionais de Proteção de Dados na apuração de violações às leis de privacidade, detalhamento das infrações por agentes de tratamento, autuações promovidas e maiores e menores valores das multas aplicadas pelas Autoridades mapeadas. Sem dúvida, esse caminho evolutivo permitiu que L.O. Baptista pudesse trabalhar concretamente sobre indicadores globais em privacidade e proteção de dados e mediá-los para o contexto brasileiro.

Igualmente, notamos 2023 como um ano representativo de aumento considerável das multas aplicadas globalmente sobre agentes de tratamento, a expansão de temas envolvendo **proteção de dados e Inteligência Artificial** na agenda regulatória das Autoridades e seus processos sancionatórios, juntamente com outros assuntos de ampla repercussão, muitos deles recorrentes em todas as jurisdições analisadas.

## Temas de destaque

- Proteção de dados e privacidade online de crianças e adolescentes
- Proteção de direitos de titulares em atividades de compartilhamento e transferência internacional de dados
- Implicações de sistemas de reconhecimento facial e uso por autoridades de segurança pública e aplicação das leis
- Necessidade de maior transparência no tratamento de dados pessoais, particularmente em publicidade comportamental
- Implementação e comprovação de medidas técnicas e organizacionais de governança e supervisão de segurança da informação
- Necessidade de comprovação de cultura organizacional em privacidade e proteção de dados pessoais, incluindo treinamento adequado para os agentes de tratamento
- Implementação de medidas de avaliação e mitigação de riscos decorrentes de ameaças à segurança da informação que possam afetar dados pessoais.

Uma maior tendência para **judicialização de casos envolvendo privacidade e proteção de dados** também entra no radar dos Indicadores Globais de 2024 e próximos anos – seja por ações ajuizadas por associações representativas dos direitos dos titulares e organizações de direitos digitais contra agentes de tratamento, seja por recursos administrativos e judiciais das empresas sancionadas questionando as sanções e multas aplicadas e obtendo redução de valores ou reversão das decisões perante os tribunais judiciais, como observado na União Europeia.

Outra tendência é que os países que ainda não possuem legislação específica de proteção de dados – ou que estão em processo de aprovação – aprovarão leis e regulamentos de privacidade robustos nos próximos anos. Por fim, é bastante provável que as investigações das Autoridades Nacionais de Proteção de Dados ao redor do mundo abordem a atuação de empresas em relação à **governança de Inteligência Artificial (IA), à transferência internacional de dados e salvaguardas de proteção e segurança da informação**, todos esses temas em ascensão na agenda tecnológica global.

# Relevância para experiência brasileira e metodologia

Como observado nas edições anteriores, o objetivo de realizar continuamente a análise dos prognósticos para o ano que se inicia, especialmente por ocasião do Data Privacy Day, está centrado em fornecer subsídios para **comparação das Melhores Práticas Internacionais (MPIs) em privacidade e proteção de dados. Esta análise foca na perspectiva regulatória e sancionatória.**

Nossa preocupação ao revisitar os Indicadores Globais é também a de **verificar de que forma a Autoridade Nacional de Proteção de Dados (ANPD) passará a se posicionar no cenário global e como ela se comportará institucionalmente no Brasil**, como uma autoridade responsável por aplicar a lei e fazer valer compromissos que o Estado brasileiro adota internacionalmente.

O ano de 2023 trouxe avanços significativos na regulamentação das sanções administrativas associadas à LGPD, conforme planejado na Agenda Regulatória do Biênio 2023/2024 da ANPD.

Em fevereiro, a Resolução nº 4/2023 foi um verdadeiro marco para os atores da indústria, ao estabelecer os parâmetros para as sanções pecuniárias e a metodologia para o cálculo do valor-base das multas, além de aperfeiçoar o processo de fiscalização e o regime sancionador pela ANPD, em linha com as ações de repressão ao descumprimento da legislação. No mês seguinte, em março, a ANPD atendeu a pedidos de transparência ao divulgar os processos sancionatórios pendentes de conclusão das investigações, que incluem empresas e órgãos públicos.

Dentre os processos sancionadores instaurados, dois foram concluídos em primeira instância, com a aplicação de penalidades monetárias e advertências a diferentes entidades, devido a infrações variadas à LGPD.

Em julho de 2023, a Coordenação-Geral de Fiscalização da ANPD notificou, através de publicação no Diário Oficial da União datada de 6 de julho, a aplicação de uma sanção à Telekall Infoservice, resultante do término de um procedimento sancionatório administrativo.

A penalidade financeira imposta à empresa, categorizada como microempresa, foi limitada a 2% do seu faturamento bruto anual, seguindo o que determina o artigo 52, inciso II, da LGPD, culminando em um total de R\$ 14.400,00 em multas.

# R\$ 14.400

foi o valor da multa aplicada à **Telekall Infoservice**.

Em outubro de 2023, a Coordenação-Geral de Fiscalização da ANPD finalizou um processo administrativo sancionador em relação ao IAMSPE, conforme divulgado no Diário Oficial da União. O órgão descumpriu o artigo 49 da LGPD por não garantir a segurança no armazenamento e no tratamento de dados pessoais dos servidores estaduais de São Paulo e de seus dependentes. Além disso, o IAMSPE não realizou a comunicação adequada sobre um incidente de segurança, violando o artigo 48 da LGPD. Como resultado, a CGF aplicou ao IAMSPE duas sanções de advertência, refletindo as infrações identificadas.

Outros números e tendências se mostram evidentes aos se observar o [Relatório Inicial de Monitoramento](#), publicado em dezembro de 2023 e que detalha as atividades e esforços de supervisão da ANPD até a metade do ano de 2023, a saber:

Durante o período de janeiro a junho de 2023, a ANPD iniciou dois novos procedimentos de fiscalização. O primeiro investiga a adequação das práticas de coleta e compartilhamento de dados de menores de idade em plataformas educacionais digitais, afetando uma série de empresas operando nesta área. O segundo busca avaliar as operações de tratamento de dados no setor farmacêutico, com foco em específicas corporações do ramo. Ademais, várias inspeções prévias, iniciadas nos anos de 2021 e 2022, seguem em processo.

No que se refere à conclusão de processos de fiscalização, a Coordenação-Geral de Fiscalização finalizou quatro em 2023. Além disso, oito procedimentos administrativos sancionadores foram abertos no ano anterior. No entanto, a ausência de diretrizes claras para a aplicação de sanções resultou na suspensão desses processos até a promulgação de um regulamento específico. Com a publicação da Resolução CD/ANPD nº 4/2023 em 27 de fevereiro, que estabelece as regras para aplicação de sanções, os processos foram retomados. Um novo processo sancionador foi adicionado ao portfólio, totalizando nove (dentre eles os processos da Telekall Infoservice e da IAMSPE, já concluídos em primeira instância).

Em relação aos Comunicados de Incidente de Segurança, houve um registro de 163 ocorrências na ANPD no primeiro semestre de 2023. Isso representa um aumento de 15,6% em relação ao mesmo período do ano anterior. A ANPD observa que, embora esses números sejam expressivos, eles ainda são baixos quando comparados com os de países com populações menores, o que indica a possibilidade de subnotificação e um potencial para aumento no número de reportes de incidentes.

A tendência natural, como também observado nas edições anteriores deste estudo, seria a de avaliar a **evolução das atividades das autoridades nacionais de proteção de dados** a partir da experiência e prática consolidada da União Europeia e do Espaço Econômico Europeu, considerando que a LGPD brasileira é fortemente influenciada pelo **Regulamento Geral de Proteção de Dados** (também conhecido pela sigla em inglês “GDPR”).

Cada vez mais, no entanto, estudos e projeções comparados no Brasil se valem apenas de uma comparação plana entre a lei brasileira e a normativa europeia, sem o cuidado de observar que o regime global de proteção de dados é mais amplo, sobrevive graças ao fluxo de dados cruzando fronteiras, alimenta o comércio e investimentos e enfrenta as diferenças culturais e institucionais relevantes entre países e regiões. Essas nuances são significativas para que a própria prática brasileira em matéria de proteção de dados e atuação da ANPD sejam diferenciais e projetem o Brasil dentro da comunidade de agentes no campo da proteção de dados.

Desse modo, e justamente para dar maior ênfase à atuação dos órgãos nacionais e à experiência comparada na área de proteção de dados, além da **prática das autoridades na União Europeia**, foram observados durante o período relevante de análise – janeiro de 2023 a janeiro de 2024 – novos indicadores do **Reino Unido** (tendo em vista o fortalecimento do ICO e o processo de saída do Reino Unido da União Europeia), e de países considerados estratégicos nas Américas, como **Uruguai, Argentina, Canadá e Estados Unidos** (em especial o Estado da Califórnia). Por fim, foram analisados indicadores da **Austrália**, considerando a atuação crescente da Australian Communications and Media Authority (ACMA) no país e a exportação de leis e regulamentos da Austrália para outras regiões do globo.



Para manter a consistência, a linearidade e a integridade da pesquisa, delimitamos o intervalo temporal estabelecido para compilação da pesquisa e análise cumulativa de dados, permanecendo entre 2021-2022 (primeira edição); 2022-2023 (segunda edição) e 2023-2024 (terceira edição), com a inclusão de dados emergentes e consolidados segundo a atuação das autoridades nacionais já no primeiro mês do ano em 2024.

Seguindo a tendência dos anos anteriores, as autoridades de proteção de dados de países membros da União Europeia começaram o ano de 2024 multando e publicando decisões em processos sancionatórios. Um exemplo notável é a decisão proferida pela Autoridade Francesa de Proteção de Dados (CNIL), que impôs uma multa de 32 milhões de Euros (ou equivalente a 171.914.681,44 Reais) para subsidiária da Amazon (Amazon France) por violação de regras do Regulamento Europeu de Proteção de Dados (GDPR).



[Veja a decisão aqui](#)

O ano que passou representou mais um recorde em termos de aplicação das regras sancionatórias do GDPR. As autoridades nacionais de proteção de dados dos Estados Membros da União Europeia impuseram algo em torno de 1,78 bilhão de Euros (1,94 bilhão de Dólares/9,58 bilhão de Reais) ao longo de 2023. Essa cifra representou aumento de mais de 14% em relação ao total de multas aplicadas no ano de 2022 (em referência ao período analisado entre 28 de janeiro e 31 de dezembro de 2022). Como indicado adiante, as bases de atuação dos agentes de tratamento pelas autoridades europeias dizem respeito, fundamentalmente, à (i) não conformidade com as regras de tratamento de dados na UE; (ii) ausência de medidas técnicas e organizacionais insuficientes para garantir a segurança da informação; (iii) ausência de especificação das bases legais para tratamento de dados pessoais e 'medidas de segurança adequadas' no tratamento de dados, entre outras.

No contexto da União Europeia, a Irlanda permanece na dianteira de 2023 pela expressiva soma das sanções aplicadas, consolidando-se como líder no valor total de multas desde a entrada em vigor do GDPR, em 25 de maio de 2018.

A posição de liderança do país é ainda mais evidente ao considerarmos a maior multa individual imposta por infrações às leis de proteção de dados no período: um total de 1,2 bilhão de euros (1,31 bilhão de dólares/6,46 bilhão de Reais) aplicada contra a Meta em 2023.



[Veja a decisão aqui](#)

Com isso, o valor das multas do GDPR impostas pela autoridade irlandesa ao longo de 2023 passa a ser de 2,86 bilhões de euros (3,12 bilhões de dólares/5,3 bilhões de reais). Esse comportamento é explicado pelo fato de a Irlanda ser um dos países preferidos pelas empresas de tecnologia, de diferentes portes, para estabelecer sua principal sede de negócios na União Europeia, em razão dos benefícios fiscais e trabalhistas existentes.

Da mesma forma, a Autoridade de Proteção de Dados Irlandesa é a autoridade que lidera muitos dos processos administrativos relacionados a casos envolvendo transferência internacional de dados. Estes casos frequentemente têm implicações diretas para o Conselho Europeu de Proteção de Dados (EDPB), que tem como uma de suas atribuições estabelecer a harmonização e a consistência de mecanismos de solução de disputas por autoridades nacionais europeias.

Grandes plataformas, redes sociais e gigantes de tecnologia têm sido os principais alvos para as multas recordes aplicadas naquele país. Vale lembrar que até o início do ano passado (janeiro de 2023), ainda no caso da autoridade irlandesa, as 'big techs' enfrentaram processos administrativos sofisticados, com multas elevadíssimas, que totalizavam cerca de 1,06 bilhão de Euros (período de referência entre setembro de 2022 e janeiro de 2023).

Seguindo nossa metodologia, os critérios relevantes selecionados pelo time de Privacidade e Proteção de Dados de L.O. Baptista para o estudo podem ser conferidos na próxima página.

# 1 PREVALÊNCIA SETORIAL

Quais áreas da indústria são mais recorrentes nos processos.

# 2 BASE DE ATUAÇÃO

Quais as principais bases de atuação pelas autoridades nacionais dos diversos países e regiões nos processos envolvendo atividade sancionatória.

# 3 NATUREZA DAS SANÇÕES

Quais as principais sanções aplicadas pelas autoridades.

# 4 VALOR DAS MULTAS

Quais os valores em multas aplicadas, por setor da indústria e por autoridade mapeada.

# 5 TEMAS DE REPERCUSSÃO PÚBLICA

Quais temas principais de repercussão pública foram abordados pelas autoridades nacionais nos processos sancionatórios e suas decisões.

# 6 POTENCIAL DE LITÍGIO

Quais casos tiveram potencial de serem re-litigados nos tribunais judiciais (por ações e recursos contra decisões administrativas das autoridades).

O conjunto de variáveis acima permite uma avaliação profunda e multilateral dos desenvolvimentos no campo da privacidade e proteção de dados. O resultado é uma ferramenta valiosa não só para profissionais da área legal, mas também para gestores de empresas que buscam orientação estratégica e insights para melhor navegar o panorama regulatório global. Para a comunidade de agentes e indústria no Brasil, os indicadores servem para auxiliar as estratégias e planejamento adequados dentro dos programas e projetos em privacidade e proteção de dados.

# Áreas da indústria afetadas e sancionadas

No balanço comparativo sobre a aplicação das leis nacionais de proteção de dados no último ano (2023), do ponto de vista das sanções direcionadas a agentes de tratamento, os setores da indústria mais visados são os seguintes:



Nota-se que, pelo terceiro ano consecutivo de análise, a prevalência setorial da indústria nas jurisdições analisadas refere-se ao conjunto de agentes econômicos atuantes nos setores de tecnologia, telecomunicações, financeiro e indústria de varejo/comércio, seguidos da indústria de serviços de internet, mídias digitais e plataformas.

Em todos esses segmentos, de modo geral, existe significativa exposição de titulares a atividades intensivas de tratamento de dados pessoais realizadas pelas empresas, evidenciando a atenção contínua à gestão de dados nestas áreas vitais para a economia digital e a preocupação com setores que lidam com grande volume de dados pessoais de consumidores.

Por isso, as autoridades nacionais de proteção de dados intensificam a atuação fiscalizatória e sancionatória, variando de acordo com o perfil cultural e institucional – por exemplo, se mais tendentes a aplicação de sanções e multas corretivas, ou se mais tendentes a medidas preventivas e educativas, com multas aplicadas para efeitos de desestimular novas práticas infrativas.

# Bases de atuação pelas autoridades

Considerando as áreas de indústria analisadas vs. autoridades analisadas por país, as principais bases para atuação de empresas e aplicação das sanções foram as seguintes:

Bases legais insuficientes para o tratamento de dados pessoais; ausência de medidas técnicas e organizacionais para assegurar proteção de dados pessoais e relativas à finalidade do tratamento; ausência da elaboração e apresentação de relatório de impacto à proteção de dados; não conformidade com os princípios gerais de tratamento de dados pessoais previstos no GDPR, como confidencialidade e integridade; violação de obrigações relacionadas a 'privacy by design' e 'privacy by default', especificação das bases legais para tratamento de dados pessoais e 'medidas de segurança adequadas' no tratamento de dados (art.32 GDPR) (União Europeia);

Marketing direto sem consentimento do titular de dados, falhas na implementação de medidas técnicas e organizacionais para assegurar a proteção de dados pessoais e a segurança das bases de dados (Reino Unido e Austrália);

Publicidade indesejada e uso inadequado de sistemas de vigilância por vídeo (Uruguai);

Violação de direito de acesso a dados pelo titular e tratamento de dados pessoais ilegais (Argentina);

Notificações para que controladores adotem medidas corretivas com relação ao tratamento de dados pessoais dos consumidores à luz da lei aplicável, no caso a *California Consumer Privacy Act* - CCPA (Califórnia/Estados Unidos);

Violação aos Princípios da Segurança e da coleta do Consentimento dos Titulares de Dados (Princípios 4.7 e 4.3, respectivamente, da *Personal Information Protection and Eletronic Documents Act* – PIPEDA) (Canadá).

Assim como na apuração concluída para o ano de 2022, observa-se que grande parte das sanções aplicadas em 2023 não estão ligadas propriamente ao vazamento de dados pessoais, mas à **violação de obrigações legais relativas ao tratamento de dados e de direitos dos titulares de dados pessoais**.

As sanções resultam em decisões de autoridades que reconhecem ou atestam o descumprimento das leis e regulamentos nacionais e regionais (no caso do GDPR europeu) pelos agentes de tratamento. Em cada um deles, as autoridades estão empenhadas em aplicar as regras que estabelecem suas correspondentes atividades regulatória, fiscalizatória e sancionatória.

Na terceira edição dos Indicadores Globais, outros casos também de destaque permanecem quanto às ações de **marketing direto não solicitado**, originadas de comunicações intrusivas realizadas via telefone, mensageiros instantâneos ou e-mail.

Novidades, contudo, foram identificadas, como processos sancionatórios de grande repercussão envolvendo violações das leis de privacidade por **técnicas de reconhecimento facial e uso de dados biométricos, transferência internacional de dados e violações das leis de proteção de dados** por entes públicos (órgãos governamentais, ministérios, agências).

# Principais sanções e valores de multas aplicadas

Em relação às **sanções** impostas, dentre elas **multas, advertências e imposição de medidas saneadoras ou preventivas**, é possível destacar duas vertentes principais, que foram percebidas ao longo das edições anteriores dos Indicadores Globais. Enquanto a União Europeia e o Reino Unido permanecem referenciais na imposição de pesadas multas, cada vez mais recorrentes e elevadas, nos demais países observa-se a aplicação de multas menores ou apenas advertências e medidas educativas ou saneadoras. Estas últimas são instrumentalizadas mediante notificações e termos de compromissos celebrados entre as autoridades e agentes de tratamento.

Em relação à **imposição de multas**, alguns setores da indústria sofreram impactos mais significativos ao longo dos anos de 2022 e 2023. Para exemplificar, o **setor de telecomunicações e mídias sociais** na **União Europeia e no Reino Unido**, com valores oscilando entre **€ 5.000 e € 1,2 bilhões** no período de referência (janeiro de 2023 a janeiro de 2024) sem contar os **custos materiais, reputacionais e indenizatórios** incorridos pelas empresas e instituições qualificadas como agentes de tratamento. Apenas a título comparativo, no período de referência anterior para 2022, os valores oscilavam entre **€ 150 e € 405 milhões**.

Na **Austrália**, a **Australian Communications and Media Authority (ACMA)** tem se mostrado bastante ativa, aplicando multas que variam entre **300 mil a 2 milhões** de dólares australianos (respectivamente 973.386,94 e 6.489.246,27 de reais) em razão de violações de proteção de dados, no período analisado.

Na **Argentina**, os valores das multas aplicadas às empresas são definidos conforme o grau da infração (leve e grave) e variam entre 25 mil e 10 milhões de pesos argentinos, aplicados pela **Autoridade Argentina de Proteção de Dados**. Interessante notar que a grande maioria dos casos de aplicação de multas se deve a ligações de marketing não solicitadas. A empresa Telefónica Móviles Argentina S.A., por exemplo, foi multada oito vezes em razão desta infração apenas no ano de 2023, totalizando aproximadamente **26 milhões de pesos** em multas.



Nos **Estados Unidos**, a aplicação de multas oscila entre **1 milhão** e **35 milhões** de dólares nos casos julgados em 2023.

A nível federal, algumas multas se referem a casos julgados pela 'Securities and Exchange Commission' (SEC) que esbarram no tema de proteção de dados. Apesar disso, a nível estadual, como no Estado da Califórnia (a seguir indicado), destaca-se a aplicação de medidas corretivas e recomendações, como tem ocorrido no Canadá e no Uruguai.

As multas, em muitos dos processos iniciados pelas autoridades analisadas, sofreram redução de seus valores seja por: (i) procedimentos administrativos de reconsideração ou por recurso, seja como (ii) resultado de decisões das autoridades contestadas em juízo (portanto, sob ações e remédios típicos de controle judicial nos países analisados e segundo as regras processuais existentes).

Essas variáveis normalmente afetam os valores individuais de multas por agente de tratamento e as bases de infração identificadas e aplicadas.

# Especificidades das jurisdições e instituições de privacidade e proteção de dados

**Informações sobre as autoridades nacionais.** Como mencionado na introdução do estudo, os Indicadores contam com a análise de informações e estatísticas disponíveis no sites oficiais da:

Comissão Irlandesa de Proteção de Dados (CDP)  
Autoridade Portuguesa de Proteção de Dados (CNPD)  
Autoridade Belga de Proteção de Dados (APD)  
Autoridade Italiana de Proteção de Dados (Garante)  
Autoridade Francesa de Proteção de Dados (CNIL)  
Autoridade Grega de Proteção de Dados (HDDPA)  
Autoridade Holandesa de Proteção de Dados (AP)  
Autoridade de Supervisão Norueguesa (Datatilsynet)  
Autoridade Finlandesa de Proteção de Dados (Ombudsman)  
Autoridade Islandesa de Proteção de Dados ('Persónuvernd')  
Autoridade Húngara de Proteção de Dados (NAIH)  
Autoridade Croata de Proteção de Dados (AZOP)

Autoridade Sueca de Proteção de Dados (IMY)  
Autoridade Turca de Proteção de Dados (KVKK)  
Autoridade Romena de Proteção de Dados (ANSPDCP)  
Autoridade de Proteção de Dados da República Tcheca (UOOU)  
Autoridade Austríaca de Proteção de Dados (DSB)  
Autoridade Polonesa de Proteção de Dados (UODO)  
Information Commissioner's Office (ICO)  
Office of the Attorney General (OAG) - Gabinete do Procurador Geral / California (EUA)  
Office of the Privacy Commissioner of Canada (OPC)  
Unidad Reguladora y de Control de Datos Personales (URCDP)  
Agencia Española de Protección de Datos (AEPD)  
Agencia de Acceso a la Información Pública (AAIP)

Do resultado das pesquisas realizadas foi possível identificar algumas outras especificidades, que são características das distintas culturas e ambientes institucionais dos países nos quais as autoridades operam.



## União Europeia

A proteção de dados é primordialmente regulada pelo Regulamento Geral sobre a Proteção de Dados (GDPR), que oferece um quadro robusto para o tratamento de dados pessoais dentro dos Estados Membros. Cada país da UE conta com sua própria autoridade de proteção de dados, que trabalha em conjunto com o Comitê Europeu de Proteção de Dados (European Data Protection Board - EDPB) para garantir a aplicação uniforme do GDPR e a consistência dos mecanismos de solução de disputas em matéria de proteção de dados. O GDPR é conhecido por suas pesadas multas e medidas rigorosas de compliance. Em 2023, observou-se um aumento na aplicação de sanções significativas, refletindo o compromisso contínuo das autoridades em proteger os direitos de privacidade dos indivíduos e a integridade dos dados pessoais em um mercado único digital.

## Reino Unido

Após o Brexit, o Reino Unido adotou o UK GDPR, que espelha muitos dos princípios e requisitos do GDPR da UE, com algumas adaptações locais. A Information Commissioner's Office (ICO) é a autoridade independente estabelecida para manter as informações dos indivíduos seguras, promover a transparência de dados e incentivar as boas práticas. O ICO tem sido extremamente proativo na aplicação de sanções, orientações e políticas, mantendo uma abordagem firme para proteção de dados e privacidade que se alinha, em grande parte, com as práticas da UE. No ano de 2023 a Autoridade continuou enfatizando a importância da responsabilidade das organizações no tratamento de dados pessoais, particularmente no que diz respeito a tecnologias emergentes como IA e implementação de medidas técnicas e organizacionais adequadas por agentes de tratamento.



## Estados Unidos

Existem várias leis federais e estaduais de proteção de dados que abrangem diferentes aspectos da privacidade de dados, como dados de saúde, informações financeiras ou dados coletados de crianças. No estado da Califórnia, a Procuradoria Geral do Estado da Califórnia (o Office of the Attorney General – “OAG”), a quem é atribuída a tarefa de fazer cumprir a ‘California Consumer Privacy Act’ (CCPA) de 2018, geralmente não divulga informações ao público sobre suas investigações. Em agosto de 2022, uma das maiores empresas da indústria cosmética havia sido multada em USD 1,2 milhões pela violação da CCPA e da Unfair Competition Law, uma vez que esta empresa vendia dados pessoais de consumidores sem informá-los ou fornecer a eles mecanismos de [opt-out para tal consentimento](#). Em 2023, o número total de registros de reclamações da CCPA aumentou significativamente em relação ao ano anterior, subindo de 52 registros em 2022 para 100 registros em 2023, [um aumento de 92%](#), indicando uma maior aplicação da lei no estado. A OAG segue fornecendo informações randomizadas a título de exemplos ilustrativos de situações em que a autoridade enviou uma notificação de alegada violação e quais foram as medidas tomadas por cada empresa em resposta a tais notificações. Outros estados, como Virgínia, Colorado, Connecticut e Utah aprovaram leis semelhantes à CCPA no último ano, e pelo menos 16 estados apresentaram [projetos de lei de privacidade em 2023](#).

No âmbito federal, destacam-se duas leis: (i) [Privacy Act of 1974](#), que estabelece como os órgãos federais podem coletar e usar dados sobre indivíduos em seu sistema de registros; e (ii) [Health Insurance Portability and Accountability Act](#) (HIPAA), que cria padrões para o tratamento de dados pessoais de pacientes por prestadores de serviços de saúde e proteção de informações de saúde de pacientes. O Congresso Americano também está debatendo a legislação de privacidade online, incluindo a discussão sobre Inteligência Artificial (IA). No final de outubro, o presidente Joe Biden emitiu uma [Ordem Executiva](#) estabelecendo padrões para a segurança e proteção de IA, de modo a assegurar a privacidade dos cidadãos americanos.



## Canadá

Existem várias leis e regulamentos relativos aos direitos de privacidade que disciplinam a proteção de informações pessoais nos setores público e privado no Canadá, compilados em um diploma normativo conhecido como 'The Canadian Privacy Statutes'. Há duas leis federais de privacidade que são aplicadas pela Secretaria do Comissário de Privacidade do Canadá: o 'Privacy Act' (que dispõe acerca da forma como o Governo Federal daquele país trata as informações pessoais) e o [The Personal Information Protection and Electronic Documents Act](#) (PIPEDA). O que é distintivo entre o regime de proteção dos direitos de privacidade e a proteção de dados do Canadá é o fato de que certas províncias (Alberta, Nova Escócia, Colúmbia Britânica e Quebec) também têm sua própria legislação, típica de sistemas jurídicos a conviver entre si sob um mesmo Estado.

O Office of the Privacy Commissioner of Canada ("OPC") é a autoridade responsável por conduzir as investigações e auditorias e emitir análises e opiniões sobre a legislação e questões relacionadas à privacidade perante o Parlamento. Desse modo, com base na PIPEDA (artigos 13 e 14), o OPC prepara um relatório contendo os resultados das investigações, as suas recomendações e eventuais acordos realizados entre as partes. A aplicação das multas não ocorre na esfera administrativa, sendo impostas pelos Tribunais. Ao longo de 2023, esteve em discussão o Projeto de Lei C-27, que visa substituir a PIPEDA, propondo a criação da "Carta Digital" com o objetivo de ampliar a abordagem normativa sobre privacidade e proteção de dados e inteligência artificial. O Projeto foi apresentado em novembro de 2022 e atualmente segue em análise no comitê da [Câmara dos Comuns canadense](#).



## Austrália

O Australian Communications and Media Authority (ACMA) é a autoridade responsável por estabelecer e gerenciar regras de serviços e mercados de comunicação e mídia na Austrália. O órgão conduz investigações e aplica multas a empresas que realizam o tratamento de dados pessoais desse setor específico. Em 2023, foi possível observar alguns casos de repercussão, como a aplicação de multas a diversas empresas do referido setor de tecnologias, comunicação e mídia, inclusive a [plataforma de transporte por aplicativo Uber](#), em razão de contatos de marketing direto sem consentimento do titular de dados pessoais. A empresa foi multada em aproximadamente US\$ 260.248.00 (ou o equivalente a R\$ 1,29 milhão).

No caso descrito, a plataforma Uber foi alvo de inúmeras reclamações de consumidores na ACMA por violações de regras da Spam Act 2003. A Autoridade declarou que recebeu reclamações de que a plataforma havia enviado e-mails de marketing aos consumidores sem um recurso de cancelamento de inscrição, depois que consumidores e clientes Uber haviam revogado seu consentimento na plataforma para receber marketing. Concluídos os procedimentos de investigação, a ACMA apurou que, em 18 de janeiro de 2023, a plataforma disparou mais de 2 milhões de e-mails de marketing a clientes sem provê-los com recurso de cancelamento de assinatura e enviou mais de 500.000 e-mails a clientes que haviam cancelado a assinatura anteriormente, violando os Parágrafos Seções 18(1) e 16(1) da Spam Act de 2003.



## Argentina

A Lei Argentina de Proteção de Dados (Ley nº 25.326) está em vigor desde 30 de outubro de 2000 - atualizada em julho de 2018 - e é fiscalizada pela Agencia de Acceso a la Información Pública (AAIP). Em julho de 2018, a AAIP emitiu a Resolução 47/2018, que introduziu diversas disposições da lei em consonância com padrões internacionais de privacidade e proteção de dados pessoais. A AAIP disponibiliza uma lista com todas as empresas que foram sancionadas com base na [lei de proteção de dados local](#).

## Uruguai

Por outro lado, a autoridade uruguaia, Unidad Reguladora y de Control de Datos Personales (URCDP) [não atualiza seus dados no site desde 2017](#), porém publica as decisões de seus processos sancionadores de modo regular. A URCDP não impõe multas às empresas autuadas, mas adverte violações à Lei de Proteção de Dados Uruguaia (Ley nº 18.331/2008) e impõe medidas saneadoras e/ou preventivas.

A escolha da pesquisa das autoridades é baseada no fato de que elas dispõem de poderes e atribuições legais para implementar medidas fiscalizadoras e sancionatórias afetas às leis de privacidade e proteção de dados. Outras fontes de suma importância para as conclusões da pesquisa aqui são o Data Guidance, a Ferramenta online GDPR Enforcement Tracker, a base de dados do Conselho Europeu de Proteção de Dados, a base de jurisprudência da Corte de Justiça da União Europeia e os sites das próprias autoridades nacionais.

# Temas de repercussão pública e tendências

## Judicialização dos casos de proteção de dados: conformidade, transparência e uso de IA no tratamento de dados pessoais

A pesquisa anual para Indicadores Globais de L.O. Baptista também considerou dois critérios adicionais para a terceira edição de 2024, buscando identificar: (i) temas principais de repercussão pública e políticas regulatórias em proteção de dados que foram abordados pelas autoridades nacionais nos processos sancionatórios e suas decisões envolvendo as partes sancionadas; e (ii) casos de potencial judicialização em matéria de proteção de dados. Neste último, foram observados alguns casos complexos envolvendo sanções e multas que foram litigados ou re-litigados nos tribunais judiciais, como por ações e recursos contra decisões administrativas das autoridades.

O surgimento desses litígios reflete um cenário de crescente complexidade e litigiosidade no campo da proteção de dados, à medida que as legislações, como o GDPR, amadurecem globalmente.

Sobre temas de repercussão, ao longo de 2023 as autoridades europeias enfrentaram a interpretação de regras do GDPR em concreto, como decisões e sanções sobre condutas de agentes de tratamento envolvendo desde violação de obrigações relacionadas à transparência nas atividades de tratamento de dados, **transferência internacional de dados, segurança da informação e proteção de dados de crianças e adolescentes**.

Essas decisões foram baseadas em casos envolvendo a **violação de obrigações legais** relacionadas ao tratamento de dados e aos direitos de titulares de dados.

Por isso mesmo, a não conformidade com princípios fundamentais das leis de proteção de dados (e.g. no GDPR) permanece como base de autuação e imposição de sanções e multas nos países analisados, além das violações dos princípios de legalidade das operações de tratamento e transparência.



No caso do GDPR, multas decorrentes da violação do princípio da integridade e da confidencialidade, de segurança no tratamento de dados (que também encontram paralelo na LGPD brasileira) – também continuam a ser verificadas a partir das decisões adotadas pelas autoridades nacionais.

Outro tema de repercussão pública crescente, indiscutivelmente, diz respeito ao uso de Inteligência Artificial (IA) em processos das organizações associados ao tratamento de dados, decisões automatizadas e interações com titulares de dados pessoais.

As autoridades nacionais na Europa, por exemplo, concentraram-se em diferentes modelos regulatórios como princípios, diretrizes e guias orientativos (atribuições que também são asseguradas à ANPD brasileira) sobre o tema. Por exemplo, o Comitê Europeu de Proteção de Dados publicou orientações sobre questões setoriais em tratamento de dados pessoais e IA, como uso de aplicações de reconhecimento facial em segurança pública e aplicação das leis.

Autoridades Nacionais desenvolveram infográficos, ferramentas e opiniões sobre o uso lícito de tecnologias de IA para o tratamento de dados pessoais e reforço dos princípios de uso responsável, protetivo e confiável de IA ([Canadá](#), Espanha, Itália, Países Baixos, Reino Unido).

Um dos processos sancionatórios de grande destaque em 2022 se refere à empresa de tecnologia Clearview AI Inc., que enfrentou multas significativas em diversos países europeus (França, Grécia, Itália, Reino Unido) por práticas que violaram a legalidade e a transparência no tratamento de dados biométricos na internet e divulgação por meio de uma ferramenta de reconhecimento facial.

Em 2023, seguindo esse movimento, a Clearview AI Inc. foi multada novamente por não cumprir com as ordens estabelecidas pelas [Autoridades no ano anterior](#).

Outros países também se destacaram em processos sancionatórios envolvendo empresas do ramo da IA. No Canadá, por exemplo, o Office of the Privacy Commissioner of Canada ('OPC') iniciou uma investigação contra o ChatGPT/OpenAI em maio, com o objetivo de examinar se a empresa tem realizado o tratamento de dados pessoais de acordo com as leis de proteção de [dados do país](#).

À medida que tecnologias de IA (incluindo IA Generativa) avancem, espera-se que seja um tópico cada vez mais crescente nas discussões de privacidade e proteção de dados, envolvendo a atuação das autoridades nacionais de proteção de dados ao redor do mundo.

Em relação à judicialização, algumas decisões de autoridades nacionais de proteção de dados da União Europeia foram questionadas nos tribunais judiciais dos países, como em recursos de apelação que tramitam nos tribunais irlandeses, outros Membros da UE e mesmo na Corte de Justiça da União Europeia.

As organizações e grandes empresas tenderão a analisar cenários de maior ou menor risco de litigiosidade, necessidade de ampliar os quadros técnicos em privacidade e proteção de dados, adaptação de estratégias de defesa nos contenciosos judiciais vs. eficiência operacional dos agentes de tratamento.

# Conclusão

A partir de nossa análise anual com Indicadores Globais, fica evidente que o dinamismo do direito à privacidade e à proteção de dados pessoais continua a desafiar empresas, legisladores e a sociedade. O ano de 2023 foi repleto de avanços significativos, com as autoridades de proteção de dados intensificando esforços para garantir conformidade, enquanto a judicialização de casos revela o amadurecimento e a complexidade dessa área. O crescente papel da Inteligência Artificial como ferramenta e objeto de regulamentação destaca a urgência de inovações normativas e estratégias jurídicas adaptativas.

Através desta 3ª edição dos Indicadores Globais, esperamos ter proporcionado contribuições valiosas que equipem os tomadores de decisões nas organizações, formuladores de políticas públicas e profissionais do Direito para melhor conhecimento das práticas comparadas. A experiência brasileira, portanto, necessita não apenas de um repertório rico e robusto de relatos, números e estatísticas relativas à proteção de dados no mundo, mas também de amadurecimento sobre a importância do tema e cultura da privacidade.

## Quer saber mais?

As edições anteriores dos Indicadores Globais estão disponíveis em [nosso site](#), acesse e confira os materiais publicados pela nossa equipe. Será uma alegria compartilhar experiências e conhecimento.

Juntos, estamos construindo um cenário mais seguro e justo para dados pessoais em todas as fronteiras.

# Equipe

Este material foi produzido pelo **time de Privacidade e Proteção de Dados de L.O.Baptista Advogados**, liderado pelos sócios **Esther Jerussalmy Cunha** e **Fabrizio Polido**.



**Esther Jerussalmy Cunha | Sócia**

✉ [ejc@baptista.com.br](mailto:ejc@baptista.com.br)



**Fabrício Polido | Sócio**

✉ [fbp@baptista.com.br](mailto:fbp@baptista.com.br)



**Denise de Araujo Berzin Reupke**

✉ [dbr@baptista.com.br](mailto:dbr@baptista.com.br)



**Carolina Britski Puga**

✉ [cbp@baptista.com.br](mailto:cbp@baptista.com.br)

## L.O. Baptista Advogados

Avenida Paulista, 1294 - 8º andar  
São Paulo - SP | Brasil  
+55 3147 0800

[www.baptista.com.br](http://www.baptista.com.br) 

L.O. Baptista 

@l.o.baptista 

L.O.Baptista Advogados 

L.O.Baptista Advogados 

Falando em Direito 