QUEM DEFENDE SEUS DADOS?

2025

INTERNETLAB

ELECTRONIC FRONTIER FOUNDATION

SUMÁRIO

I. INTRODUÇÃO

O InternetLab é um centro independente de pesquisa interdisciplinar que promove o debate acadêmico e a produção de conhecimento nas áreas de direito e tecnologia, sobretudo no campo da Internet. Somos uma entidade sem fins lucrativos e atuamos como ponto de articulação entre acadêmicos e representantes dos setores público, privado e da sociedade civil. Em parceria com a Electronic Frontier Foundation (EFF), entidade do terceiro setor dos Estados Unidos, o InternetLab lança, em 2025, a oitava edição do projeto "Quem Defende Seus Dados?", versão brasileira do "Who has your back?".

O nosso objetivo é observar e avaliar o comprometimento público de operadoras de serviços de telecomunicações — em especial, empresas de telefonia móvel e de conexão à internet — com a privacidade e a proteção de dados de seus usuários. **Ao premiar as empresas com estrelas, pretendemos incentivar a adoção de boas práticas e o desenvolvimento de políticas que assumam um compromisso público com a proteção da privacidade e dos dados pessoais.**

O "Who Has Your Back?" é desenvolvido pela EFF desde 2011. Em 2015, o projeto expandiu-se para outros países, especialmente os da América Latina[1]. As edições latino-americanas têm como objetivo avaliar as empresas de telefonia móvel e de conexão à internet quanto às políticas de transparência, privacidade e proteção de dados pessoais. No caso do Brasil, a metodologia de avaliação foi elaborada com base nos princípios e garantias estabelecidos pela Constituição Federal, pelo Marco Civil da Internet, pela Lei Geral de Proteção de Dados e demais normas vigentes.

Neste documento apresentamos a metodologia utilizada para nossa análise final. Em 2025, seguimos aprimorando nossos parâmetros de avaliação com base nas leis e regulamentos vigentes sobre privacidade e proteção de dados. Reforçamos, ainda, que a pesquisa não se limita a monitorar a adequação ou conformidade das empresas à legislação. Ela também visa avaliar boas práticas de privacidade e proteção de dados que vêm emergindo no setor privado, na academia e na sociedade civil com o objetivo de garantir a efetiva defesa dos direitos fundamentais dos cidadãos. Para atingir os objetivos propostos, analisaremos as

[1] Canadá: https://www.eff.org/node/81906; Colômbia: https://www.eff.org/deeplinks/2016/11/who-has-your-back-colombia-new-report-shows-telecom-privacy-slowly-improving Holanda: https://www.eff.org/node/82161; Estados Unidos: https://www.eff.org/who-has-your-back-2017; Alemanha: https://www.eff.org/node/81907; Polônia: https://www.eff.org/node/81901; Irlanda: https://www.eff.org/node/81899; Peru: https://www.eff.org/deeplinks/2015/11/new-report-shows-which-peruvian-isps-care-about-their-users-privacy; México: https://www.eff.org/deeplinks/2015/06/new-report-shows-which-mexican-isps-stand-their-users; Paraguai: https://qdtd.tedic.org; Chile: https://www.derechosdigitales.org/publicaciones/quien-defiende-tus-datos-2017/.

operadoras de serviços de telecomunicações com foco nas empresas de telefonia e de conexão à Internet. Além de contribuir para o aprimoramento das práticas de privacidade e proteção de dados no setor de telecomunicações, esta pesquisa também visa fornecer subsídios para pesquisadores, formuladores de políticas públicas, entidades reguladoras e a sociedade civil. Ao tornar mais visível o comportamento das empresas, buscamos fortalecer a capacidade de escolha, monitoramento e reivindicação por parte dos usuários.

Em nossa análise, selecionamos as cinco empresas de telefonia e banda larga fixa que mantiveram o maior número de usuários ao longo de todo o período da pesquisa (2023-2025), conforme o ranking da Agência Nacional de Telecomunicações (Anatel), são elas):

- Claro (banda larga fixa e telefonia móvel);
- Vivo (banda larga fixa e telefonia móvel);
- Oi (banda larga fixa);
- Brisanet (banda larga fixa); e
- Tim (telefonia móvel).

Para contextualizar as escolhas metodológicas da pesquisa, alguns esclarecimentos. No início da coleta de dados (fevereiro de 2024), duas empresas de banda larga fixa — EB Fibra/Alloha Fibra[2] e Desktop — figuravam entre as cinco maiores em número de assinantes nos serviços de telecomunicações. No entanto, elas não serão analisadas nesta pesquisa, pois no ranking atual da Anatel já não constam entre as cinco com maior número de usuários. Da mesma forma, ao final da coleta de dados para a pesquisa (fevereiro de 2025), outras três empresas — Giga Mais Fibra, Algar (CTBC Telecom) e Datora — também poderiam ter sido incluídas. Contudo, como o critério adotado exige que as empresas estejam dentro desse grupo durante todo o período de análise, elas também foram excluídas da amostra. Essa escolha visa garantir a consistência nos dados e permitir comparações mais robustas ao longo do tempo.

Para a nossa avaliação, valorizamos uma série de critérios, expostos na terceira seção deste documento, que compreendem, por exemplo: a existência e a acessibilidade de informações sobre privacidade em páginas específicas nos sites das empresas (como "portais de privacidade"); a acessibilidade e a disponibilização, em português, de seus relatórios de transparência e segurança; a oferta de meios para o exercício dos direitos dos titulares de dados — como os direitos de acesso, retificação e apagamento dos dados — assim como o respeito a tais solicitações; além da existência de protocolos específicos de

[2] Em 2021, a EBFibra mudou a sua marca para Alloha Fibra. Aqui, adotamos as duas nomenclaturas, pois no registro da Anatel e no CNPJ ainda constam EB Fibra.

entrega de dados a agentes do estado, dentre outros. Os critérios foram mensurados com base em parâmetros objetivos construídos a partir da legislação vigente e de boas práticas consolidadas no setor. Para isso, realizamos a análise de documentos públicos, as interações com as empresas e as solicitações de acesso a dados pessoais feitas por integrantes do InternetLab. Conforme o grau de atendimento a esses parâmetros, as empresas receberam estrelas — inteiras ou fracionadas. Mais detalhes sobre os critérios e a forma de pontuação estão descritos nas próximas seções desta metodologia.

II. METODOLOGIA DA COLETA

Cada empresa foi avaliada a partir de seis categorias, cuja elaboração levou em consideração as exigências da legislação vigente (especialmente da Lei Geral de Proteção de Dados e do Marco Civil da Internet) e boas práticas internacionais em matéria de proteção à privacidade.

A coleta de informações foi realizada em duas etapas complementares:

1. Busca ativa em fontes públicas

Na primeira etapa, conduzida entre janeiro de 2023 e dezembro de 2024, realizamos uma busca ativa em fontes públicas para identificar documentos e informações relevantes disponibilizados pelas próprias empresas, bem como conteúdos veiculados na grande imprensa e na mídia especializada. Foram analisados:

- Portais e políticas de privacidade e proteção de dados;
- Códigos de ética;
- Relatórios de sustentabilidade;
- Contratos de prestação de serviços;
- Informações publicadas nos sites institucionais das empresas;
- Notícias, colunas e outras participações na mídia geral e especializada;

2. Diálogo com as empresas

Em março de 2025, resultados preliminares — i.e. uma versão inicial das pontuações por categoria e suas respectivas justificativas —, foram encaminhados a todas as empresas avaliadas, acompanhados de um convite para revisão e atualização das informações coletadas na primeira etapa. Essa interlocução teve como objetivo garantir a acurácia dos dados analisados, bem como oferecer espaço para que as empresas esclarecessem

eventuais imprecisões, compartilhassem documentos adicionais e atualizassem informações institucionais relevantes.

Das cinco empresas avaliadas, quatro responderam ao contato: Claro, Vivo, Oi e Tim. A Brisanet, embora tenha sido contatada em duas ocasiões — em março e novamente em abril de 2025 —, não apresentou retorno até o encerramento da fase de revisão.

Foram realizadas reuniões com as equipes da Oi, Claro e Tim, nas quais os resultados preliminares foram discutidos e documentos complementares, fornecidos. A Vivo optou por enviar suas contribuições exclusivamente por e-mail.

As contribuições recebidas foram analisadas à luz dos critérios metodológicos previamente definidos e, quando pertinentes, incorporadas à avaliação final. Para as empresas que não apresentaram retorno, foram mantidas as informações apuradas durante a etapa inicial de coleta.

III. PONTUAÇÃO

Com base nas respostas obtidas, atribuímos as seguintes notas:

Estrela cheia	¾ de estrela	½ estrela	¼ de estrela	Nenhuma estrela
★	★	★	★	☆

As empresas iniciam a avaliação sem nenhuma estrela e, à medida que cumprem os parâmetros previstos em cada categoria, vão acumulando frações de estrela. Uma estrela cheia indica o cumprimento total dos critérios estabelecidos, enquanto a ausência de estrelas reflete o não atendimento a qualquer um deles.

IV. CRITÉRIOS ANALISADOS

CATEGORIA 1: Informações sobre a política de proteção de dados

A empresa fornece informações claras e completas sobre suas práticas de proteção de dados?

Todas as pessoas usuárias de internet têm direito a informações claras e completas sobre o tratamento de seus dados, que podem ser utilizados apenas para finalidades específicas (Marco Civil da Internet, art. 7º, incisos VI e VIII). Além disso, informações sobre padrões de segurança devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente nos sites das empresas (Decreto n.º 8.771/2016, art. 16).

A Lei Geral de Proteção de Dados Pessoais (LGPD) reitera o respeito à transparência como princípio norteador da proteção de dados (LGPD, art. 6º, inciso VI) Ela estabelece o direito dos titulares a informações claras, adequadas e ostensivas sobre o tratamento de seus dados pessoais (LGPD, art. 6º, inciso VI, art. 18 e art. 19). Nesse mesmo sentido, a LGPD tem um cuidado especial no que concerne à finalidade específica; à forma e duração do tratamento; à identificação e contato do controlador; ao eventual compartilhamento de dados e aos deveres dos agentes responsáveis pelo tratamento (LGPD, art. 9º). Prevê ainda, a obrigação de informar eventuais mudanças da finalidade do tratamento não compatíveis com o consentimento original, facultando-se, nesse caso, a revogação do consentimento (LGPD, art. 9º, § 2º).

As pessoas titulares de dados também têm direito à exclusão definitiva, ao acesso e à retificação dos dados pessoais, conforme o artigo 43 do Código de Defesa do Consumidor, o artigo 7º do Marco Civil da Internet e diversos dispositivos da Lei Geral de Proteção de Dados.

Nesta categoria, buscamos analisar as práticas de transparência e prestação de informações das empresas perante os titulares de dados e o público em geral. Buscamos, ainda, avaliar as respostas oferecidas pelas empresas a solicitações de titulares, no exercício de seus direitos. Para tal, no decorrer do período analisado por esse relatório, integrantes do InternetLab realizaram pedidos de acesso aos seus dados pessoais, armazenados pelas empresas.

Quais foram os parâmetros de avaliação?

(I) [Informações sobre coleta]

A empresa fornece informações claras e completas sobre:

(a) quais dados são coletados;

(b) em que situações a coleta ocorre;

(c) se há possibilidade de coleta de dados disponíveis publicamente;

(d) listagem por nome, na política ou aviso de privacidade, de quais terceiros fornecem dados à empresa (inclusive fornecedores de dados públicos); e

(e) se há avaliação sobre a conformidade legal de terceiros com a LGPD.

(II) [Informações sobre finalidade]

A empresa fornece informações claras e completas sobre:

(a) a finalidade do tratamento pela própria empresa; e

(b) o tipo ou a forma de tratamento.

(III) [Informações sobre armazenamento, segurança e compartilhamento]

A empresa fornece informações claras e completas sobre a segurança dos dados pessoais, por exemplo:

(a) por quanto tempo e onde são armazenados;

(b) em quais circunstâncias são apagados;

(c) se podem ser retidos e em quais circunstâncias;

(d) quais práticas de segurança administrativa e técnica observa, avaliando, por exemplo, se há uma Política de Segurança Cibernética/TI com informações sobre as proteções contra *malware*, *ransomware*, *worms* e outros vírus;

(e) se há controles de acesso para acesso aos dados, considerando-se diferentes categorias de colaboradores;

(f) com quais terceiros a empresa compartilha os dados (após a coleta);

(g) para quais finalidades os dados podem ser compartilhados (inclusive quando do uso de *softwares*, plataformas online, redes ou nuvens para uso interno da empresa);

(h) quais as hipóteses de transferência internacional de dados;

(IV) [Informações sobre direitos]

(a) A empresa informa aos titulares sobre seus direitos segundo a LGPD;

(b) A empresa informa quais são os meios (por exemplo, e-mails ou portais) para exercício dos direitos dos titulares.

(V) [Respostas a solicitações de direitos]

(a) A empresa fornece informação de guarda ou acesso a dados pessoais mediante requisição de seus titulares. Tais informações são claras e completas, indicando a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, no prazo de até 15 dias; ou em formato simplificado, imediatamente.

(b) A empresa atendeu às requisições sobre direitos dos titulares em até um mês; A verificação deste critério foi feita a partir das solicitações realizadas por integrantes do InternetLab de acesso aos seus dados pessoais, armazenados pelas empresas.

(VI) [**Atualização da política de privacidade]**

A empresa promete enviar notificações (por exemplo, por e-mail ou SMS) aos usuários na hipótese de modificações de suas práticas de tratamento de dados.

(VII) [**Acessibilidade]**

A empresa apresenta informações claras e completas sobre privacidade e proteção de dados de forma acessível em seu site (por exemplo em um "portal da privacidade" ou semelhantes), contanto que tais informações também estejam disponíveis nos contratos de adesão ou políticas de privacidade aplicáveis.

Padrões de desempenho

O provedor de Internet atende	O provedor de Internet atende	O provedor de Internet atende	O provedor de Internet atende a apenas um	O provedor de Internet não atende a

de 6 a 7 parâmetros.	de 4 a 5 parâmetros.	de 2 a 3 parâmetros.	dos parâmetros.	nenhum dos parâmetros.
				

CATEGORIA 2: Protocolos de entrega de dados para investigações

A empresa se compromete a seguir a interpretação da lei mais protetiva do direito à privacidade diante da requisição de dados pessoais por agentes do Estado, e tem políticas específicas para esses casos?

A legislação brasileira prevê diferentes hipóteses em que autoridades públicas podem ter acesso a dados de usuários de serviços de conexão à internet.

Dados cadastrais, isto é, aqueles referentes à qualificação pessoal, filiação e endereço, podem ser disponibilizados diretamente a autoridades administrativas, sem necessidade de ordem judicial, se e quando as autoridades possuírem competência legal para a requisição (Marco Civil da Internet, art. 10, § 3º). Também é necessário que a autoridade administrativa indique, em seu pedido, o fundamento legal de competência expressa e a motivação para o acesso aos dados cadastrais (art. 11, Decreto n.º 8.771/2016, que regulamenta o Marco Civil da Internet).

Atualmente, **autoridades policiais e o Ministério Público possuem competência para a requisição de dados cadastrais em situações específicas.** Estão elas nos seguintes âmbitos de aplicação:

- Lei das Organizações Criminosas (Lei n.º 12.850/2013)
- Lei dos Crimes de Lavagem de Dinheiro (Lei n.º 9.613/1998)
- No caso da investigação dos delitos referidos no artigo 13-A do CPP: crimes de sequestro e cárcere privado, redução a condição análoga à escravidão, tráfico de pessoas, extorsão mediante restrição de liberdade, extorsão mediante sequestro e promoção ou auxílio à efetivação de ato destinado ao envio de criança ou adolescente para o exterior com inobservância das formalidades legais ou com o fito de obter lucro.

Nesse sentido, a interpretação mais protetiva da privacidade dos usuários encara como sendo essas as únicas autoridades administrativas investidas de competência legal para requisitar

dados cadastrais sem ordem judicial, no âmbito de investigações desses crimes. Em outros casos, a ordem judicial ainda seria necessária para a entrega de dados cadastrais.

Apesar disso, algumas autoridades policiais reivindicam autoridade para requisitar informações, independentemente do crime investigado. As autoridades argumentam que a Lei n.º 12.830/2013, que dispõe sobre a investigação criminal conduzida pelo delegado de polícia, permitiria a requisição de informações (art. 2, § 2º). A questão foi levada ao Supremo Tribunal Federal (STF) em ação direta de inconstitucionalidade (ADI 5059) e aguarda julgamento. Até que a controvérsia seja pacificada, o InternetLab cobrará transparência das empresas acerca das autoridades consideradas competentes para a requisição de dados cadastrais e das circunstâncias consideradas aptas a ensejar o acesso aos dados.

Os **registros de conexão**, isto é, "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (art. 5, VI da Lei n.º 12.965/2014), somente podem ser disponibilizados ao requisitante **se a entrega for autorizada por ordem judicial** (art. 10, §1º da Lei n.º 12.965/2014).

Atualmente, entretanto, tem sido observada a ocorrência de pedidos e decisões judiciais que incumbem provedores de conexão do fornecimento de informações que extrapolam a definição do artigo 5º, VI, do Marco Civil da Internet, alcançando, por exemplo, o número da porta lógica de origem dos IPs. O Marco Civil da Internet, no entanto, não prevê a obrigação de guarda de tais dados, ainda que sejam úteis — e, eventualmente, necessários — à identificação de um usuário de Internet. Trata-se de uma interpretação extensiva que tanto pode implicar uma obrigação de fazer excessiva para as empresas, como uma restrição do direito à privacidade dos usuários, considerando a insegurança acerca dos dados sujeitos à retenção e compartilhamento.

Quanto aos **dados de geolocalização**, o Código de Processo Penal dispõe que podem ser requisitados **mediante autorização judicial**, se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, por membro do Ministério Público ou delegado de polícia (Código de Processo Penal, art. 13-B). Exceção é prevista apenas no caso de ausência de manifestação judicial no prazo de 12 horas, caso em que a autoridade competente poderá requisitar dados diretamente às empresas prestadoras de serviço de telecomunicações e/ou telemática (Código de Processo Penal, art. 13-B, §4º).

A constitucionalidade desses dispositivos também foi submetida à avaliação do STF , em decorrência da ação direta de inconstitucionalidade (ADI 5642) proposta em janeiro de 2017 pela a Associação Nacional das Operadoras de Celular (ACEL). A associação argumentava que os dispositivos, ao permitirem a dispensa de ordem judicial para acesso aos dados de localização, violam a privacidade e o sigilo das comunicações, direitos fundamentais previstos no artigo 5º incisos X e XII da Constituição. A ADI 5642, no entanto, foi considerada improcedente pelo STF em decisão proferida em 18 de abril de 2024.

Além disso, há outra controvérsia no que diz respeito à temporalidade dos dados locacionais que podem ser exigidos: a despeito de possível violação à privacidade e às normativas de proteção de dados, segundo algumas interpretações, somente a requisição de dados de localização em tempo real necessitaria ser feita mediante ordem judicial; dados pretéritos, não (vide Habeas Corpus n.º 247331, do Superior Tribunal de Justiça, Rel. Min. Maria Thereza de Assis Moura, DJe 03/09/2014). De qualquer maneira, até que as controvérsias sejam pacificadas, o InternetLab cobrará transparência das empresas acerca de quais práticas adota em relação aos dados de localização.

Também são alvos de questionamentos na Corte Constitucional os **pedidos genéricos** de quebra de sigilo de dados. A Lei das Interceptações Telefônicas (LIT) autoriza a quebra de sigilo e interceptação de comunicações, mas sempre limitando essa quebra/interceptação a "indícios razoáveis de autoria ou participação em infração penal" (LIT, art. 2º, I). Outras determinações jurídicas, tais como o supramencionado art. 13-B do Código de Processo Penal, indicam a necessidade de fundamentos e elementos concretos para a quebra de sigilo de pessoas determinadas e definidas. O ordenamento jurídico brasileiro não suporta, portanto, a autorização judicial para quebra de sigilo com base em pedidos genéricos, sem elementos indicativos de autoria e participação ou sem determinação ou definição dos alvos da quebra.

Há poucos anos, o STF admitiu Repercussão Geral do Recurso Extraordinário 1.301.250 (Tema 1.148), que atravessa o assunto dos pedidos genéricos. No caso, para investigar o assassinato da vereadora Marielle Franco e seu motorista Anderson Gomes, a autoridade investigativa requisitou quebra de sigilo de dados telemáticos de todos aqueles que haviam pesquisado na internet, num período de cinco dias, termos como o nome da vereadora e o local do crime. O caso estabelecerá precedente importante sobre o acesso a dados de pessoas indefinidas através de pedidos genéricos de quebra de sigilo de dados.

Por fim, ressaltamos que além da exposição de tais informações em seus contratos ou outros documentos, **buscamos também valorizar a publicação de protocolos específicos voltados à entrega de dados para agentes do Estado,** que se preocupem em determinar quais as formas e condições do acesso a dados pessoais no âmbito de investigações ou ações equivalentes. A existência de protocolos claros e públicos, como o fazem diversas empresas de tecnologia, é importante medida do comprometimento público da empresa com a privacidade e proteção dos dados de seus usuários.

Nesta categoria, procuramos avaliar se a empresa, em seu contrato ou qualquer outro documento oficial disponível para o público, **informa de maneira clara e completa às/aos usuárias/os quais as circunstâncias em que autoridades judiciais ou administrativas podem obter acesso a seus dados.**

Tratando-se de matéria sob controvérsia jurídica, a questão se desdobra em diferentes parâmetros, que buscam discriminar níveis de proteção, clareza e comprometimento quanto ao

acesso a dados para investigações. Os parâmetros buscam refletir o compromisso da empresa com a transparência quanto às autoridades consideradas competentes, seu comprometimento atento às disputas normativas atuais e às limitações da legislação (em especial quanto aos crimes no âmbito de cuja investigação estaria dispensada a ordem judicial para acesso a dados cadastrais), além do comprometimento expresso em suas diretivas quanto a dados de localização, registros de conexão e a publicação de protocolos voltados à entrega de dados em investigações.

Quais foram os parâmetros de avaliação?

(I) **[Dados cadastrais]**

(a) A empresa promete fornecer dados cadastrais por requisição (sem ordem judicial) apenas a autoridades administrativas competentes, além de identificá-las. Em outros casos, exige ordem judicial.

(b) A empresa promete fornecer dados cadastrais por requisição (sem ordem judicial) apenas no âmbito da apuração dos crimes a que se referem os dispositivos da Lei 12.850/13, da Lei 9.613/98 e o artigo 13-A do CPP. Em outros casos, exige ordem judicial.

(II) **[Dados de geolocalização]**

(a) A empresa oferece informações claras sobre as circunstâncias em que fornece dados de geolocalização, identificando se fornece dados em tempo real ou pretéritos;

(b) A empresa promete entregar dados de geolocalização da vítima ou suspeito apenas mediante ordem judicial, quando necessário à prevenção e à repressão de crimes relacionados ao tráfico de pessoas;

(c) Nos casos de crimes de tráfico de pessoas, promete, apenas na ausência de manifestação judicial, entregar os dados no prazo de 12 (doze) horas, mediante requisição da autoridade competente.

(III) **[Registros de conexão]**

A empresa promete fornecer registros de conexão apenas mediante ordem judicial, estritamente nos termos definidos no Marco Civil da Internet (art. 5, inciso VI).

(IV) **[Vedação a ordens genéricas de acesso a dados]**

A empresa se compromete a não atender e/ou contestar pedidos genéricos de acesso a dados, i.e., que não determinem pessoas específicas cujas informações serão compartilhadas às autoridades.

(V) **[Protocolos específicos e transparência]**

A empresa publica protocolo de resposta a pedidos de entrega de dados pessoais a autoridades públicas, que contenham as informações de maneira estruturada e simplificada.

Padrões de desempenho

O provedor de Internet atende a 4 ou 5 parâmetros.	O provedor de Internet atende a 3 parâmetros.	O provedor de Internet atende a 2 parâmetros.	O provedor de Internet atende a apenas um parâmetro.	O provedor de Internet não atende a nenhum dos parâmetros.
				

CATEGORIA 3: Defesa dos usuários no Judiciário

A empresa contestou, de forma administrativa ou judicial, pedidos abusivos de acesso a dados ou legislação que considera violar a privacidade de usuários?

O Judiciário, seja em disputas de perfil individual ou coletivo, é um importante espaço para a defesa e consolidação de direitos dos usuários contra abusos e ilegalidades.

A legislação estabelece que quaisquer ordens de acesso a dados pessoais — advindas de autoridades judiciais ou administrativas competentes — devem incluir, no mínimo, a indicação do fundamento legal de sua competência e a motivação do pedido (arts. 10, §1º e §3º e 22 do Marco Civil da Internet e art. 11 do Decreto n.º 8.771/2016). Além disso, o Decreto (art. 11, § 3º) também veda pedidos coletivos, genéricos ou inespecíficos. O não cumprimento desses critérios é um forte indicativo de abuso na solicitação de acesso.

Buscamos avaliar o posicionamento das empresas em processos judiciais relacionados à privacidade e proteção de dados. No período de análise, foram considerados dois eixos: (i) A defesa, por vias judiciais, de legislação, ou interpretação da legislação, que seja favorável ao usuário; e (ii) a defesa do próprio usuário perante pedidos considerados abusivos.

(I) [Contestação de legislação]

A empresa contestou judicialmente legislação, ou interpretação da legislação, que considera violar a privacidade de usuários de Internet. A contestação se fundamentou pela legislação ser desproporcional, não definir de modo claro, preciso e detalhado os casos e circunstâncias em que os dados devem ser fornecidos e/ou não prever as salvaguardas adequadas para inibir eventuais abusos (Exemplos de legislações que podem vir a ser contestadas: arts. 15, 17 e 21 da Lei das Organizações Criminosas; art. 2, §2º da Lei 12.630/13; arts. 13-A e 13-B do Código de Processo Penal).

(II) [Contestação de pedidos abusivos]

A empresa contestou, seja judicial ou administrativamente, ao menos uma vez durante o período analisado, pedidos abusivos de acesso a dados de usuários. Tais contestações tiveram por base os pedidos extrapolarem as prerrogativas legais da autoridade solicitante e/ou serem desproporcionais por sua falta de clareza e precisão sobre os dados requeridos e a motivação. Além disso, qualquer outra razão que comprometa o direito à privacidade dos usuários pode ser motivo para as contestações.

Padrões de desempenho

O provedor de Internet atende aos dois parâmetros.	O provedor de Internet atende a um parâmetro.	O provedor de Internet não atende a nenhum dos parâmetros.
		

CATEGORIA 4: Postura pública pró-privacidade

A empresa se posicionou publicamente em defesa da privacidade e da proteção de dados, fortalecendo a cultura de proteção a esses direitos no Brasil?

Esta categoria tem como objetivo avaliar a postura pública das empresas em relação a temas de privacidade e proteção de dados. Para isso, consideramos suas participações em consultas públicas, debates ou eventos acerca de leis, projetos de lei e políticas públicas que impactam os usuários da rede. Também consideramos a maneira como se posicionam na mídia geral e especializada, por exemplo, em resposta a medidas governamentais que possam afetar os usuários.

Consideramos apenas a participação realizada em nome da própria empresa, excluindo contribuições feitas por meio de associações que representam múltiplas empresas, como a Conexis e a Acel. Isso porque entendemos que um posicionamento público institucional é essencial para fortalecer a relação de confiança e compromisso entre a empresa e seus usuários. Na análise do posicionamento geral pró-privacidade, verificamos se a empresa, em nome próprio, participou de consultas públicas, debates ou se manifestou na mídia, seja

geral ou especializada. Além disso, avaliamos se sua posição incluiu a defesa concreta da aprovação de normas ou da adoção de técnicas que ampliem a proteção dos usuários de seus serviços.

Nesta edição, analisamos ainda a possível inércia das operadoras diante de suas vulnerabilidades de seguranças e dos indícios de interceptação ilegal das comunicações de seus usuários por meio de spywares. Nela, avaliamos se as operadoras tomaram todas as medidas cabíveis para i) ter ciência de suas vulnerabilidades de segurança; ii) projetar e comunicar os riscos associados à exploração dessas falhas, incluindo sua notificação aos usuários e agências reguladoras, como a Anatel.

Nosso interesse na temática se deve a um conjunto de acontecimentos que demonstram como governos ao redor do globo têm utilizado tecnologias de vigilância que baseiam seu funcionamento na exploração de vulnerabilidades de segurança de dispositivos de comunicação pessoal.[3] O uso de spywares para vigilância remota, secreta e invasiva tem permitido que governos acessem, armazenem e manipulem grandes volumes de dados pessoais sem o consentimento dos alvos[4]. Denúncias e investigações sobre casos de vigilância ilegal — frequentemente motivados por razões políticas — têm acendido um alerta sobre a proteção de direitos fundamentais, como a privacidade, a inviolabilidade do sigilo das comunicações e dos dados pessoais, a liberdade de expressão e o direito à informação.

---

[3] Em 2019, o Relator Especial das Nações Unidas sobre a promoção e proteção do direito à liberdade de opinião e expressão, David Kaye, apresentou o relatório Surveillance and Human Rights (Vigilância e Direitos Humanos), no qual examina os impactos da vigilância direcionada sobre os direitos fundamentais. O documento destaca como tecnologias de monitoramento, frequentemente desenvolvidas por empresas privadas, têm sido empregadas por governos para espionar jornalistas, ativistas e opositores políticos, resultando em detenções arbitrárias, tortura e até execuções extrajudiciais. Kaye ressalta a ausência de regulamentação e transparência na exportação e comercialização dessas tecnologias, que frequentemente acabam nas mãos de regimes repressivos. Casos emblemáticos incluem a vigilância de jornalistas e opositores na Hungria, Índia, México e Marrocos. KAYE, D; SCHAAKE, M. Global spyware such as Pegasus is a threat to democracy. Here's how to stop it. Washington Post, 19 jul. 2021. Disponível em: https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/ . Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Surveillance and Human Rights. United Nations Human Rights. 28 mai. 2019. Disponível em: https://documents.un.org/doc/undoc/gen/g19/148/76/pdf/g1914876.pdf?token=CveA5Dilbzvyzulw3p&fe=true.

[4] "Tais ferramentas tecnológicas são aptas a interceptar comunicações telefônicas e telemáticas, a partir da 'infecção' de dispositivos eletrônicos por um programa espião (spyware) e, com isso, possibilitar aos intrusos monitorar conversas, escutar o som ambiente pelo microfone do dispositivo; captar imagens por meio das câmeras frontal e traseira; determinar a localização em tempo real, por meio do sistema de GPS; capturar as imagens da tela e acompanhar em tempo real tudo o que é digitado (keylogger) ou visualizado pelo usuário, funcionalidades que podem vir a ser obtidas sem qualquer intervenção do usuário-vítima ('zero click')". Ação Declaratória de Incostitucionalidade por Omissão 84. Petição Inicial. Procuradoria Geral da República, p. 8. Disponível em: https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=6816879.

O Brasil não está alheio a este cenário. No início de 2023, a imprensa denunicou o uso ilegal de ferramentas de geolocalização de dispositivos eletrônicos pela Agência Brasileira de Inteligência (Abin) durante o governo Bolsonaro, sendo a principal delas o spyware First Mile. Em janeiro de 2024, a Polícia Federal deflagrou a Operação Vigilância Aproximada para investigar o uso ilegal de ferramentas de geolocalização de dispositivos eletrônicos pela Agência Brasileira de Inteligência (Abin) durante o governo Bolsonaro, sendo a principal delas, o spyware First Mile. A ação policial tem buscado identificar e apurar ações de organização criminosa que agiu para monitorar ilegalmente pessoas e autoridades públicas, invadindo aparelhos e computadores, além da infraestrutura de telefonia. As medidas dão continuidade à Operação Última Milha, deflagrada em outubro de 2023, que também investiga a instrumentalização da Abin para fins políticos, o que ficou conhecido pelas autoridades como "Abin paralela". Segundo a decisão do ministro Alexandre de Moraes, que autorizou as medidas da operação, o inquérito policial indica a presença de um núcleo político na Abin, sobretudo na gestão de Alexandre Ramagem, que utilizou-se da tecnologia, de forma ilegal, para monitorar autoridades e servidores públicos, dentre outros cidadãos.

O First Mile é um software espião. Desenvolvido pela empresa israelense Cognyte (ex-Verint), foi adquirido pela Abin em dezembro de 2018. Seu funcionamento explora fragilidades em redes de telecomunicações, possibilitando a coleta de informações sobre a movimentação de alvos de interesse ao rastrear a localização de dispositivos móveis . Anualmente a ferramenta permitiria o monitoramento da geolocalização de até 10 mil celulares que utilizam as redes 3G, 4G e 5G, bastando inserir o número de telefone do alvo. Relatos indicam que a tecnologia foi amplamente utilizada na gestão de Alexandre Ramagem, entre maio de 2020 e abril de 2022, para monitorar ilegalmente agentes públicos e outros cidadãos.

A gravidade das denúncias levou a Procuradoria-Geral da República (PGR) a ingressar, em dezembro de 2023, com uma Ação Direta de Inconstitucionalidade por Omissão (ADO 84), posteriormente convertida na Arguição de descumprimento de preceito fundamental (ADPF) 1143 no STF, questionando a ausência de regulamentação para o uso de spywares por órgãos e agentes públicos. No pedido ao STF, a PGR argumentou que a aquisição e o uso dessas tecnologias sem regulamentação comprometem direitos fundamentais, como a proteção à inviolabilidade da vida privada, da intimidade e do sigilo das comunicações e dos dados pessoais. Nesse sentido, solicitou a fixação de um prazo razoável para que o Congresso Nacional aprove uma legislação sobre o tema.

Em junho de 2024, na audiência pública sobre a ADPF 1143 convocada pelo ministro Cristiano Zanin[5], a PF e a Anatel apresentaram evidências detalhadas sobre as falhas

[5] BRASIL. Supremo Tribunal Federal. Despacho de programação da audiência pública na ADPF 1143. Brasília, DF: STF, 2024. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF1143Despachoprogramaoaudincia1.pdf.

estruturais nas redes de telecomunicações brasileiras[6] que possibilitaram o uso do spyware First Mile para monitoramento ilegal de celulares. Segundo as autoridades, o software explorava vulnerabilidades no protocolo SS7 (Signaling System No. 7)[7], utilizado em redes móveis 2G e 3G, que permite a interconexão entre operadoras, mas não verifica a autenticidade das solicitações de acesso a dados de localização. Isso possibilita que agentes não autorizados rastreiem dispositivos apenas inserindo o número de telefone do alvo. Peritos da PF demonstraram ao STF que o First Mile identificava a Estação Rádio Base (ERB) à qual o celular estava conectado, gerando coordenadas geográficas com um raio de precisão considerável. O laudo técnico da PF alertou que, apesar da adoção de tecnologias mais avançadas como 4G e 5G, o SS7 ainda é amplamente utilizado, representando um risco contínuo à segurança das comunicações[8]. Diante disso, a PF e a Anatel reforçaram a necessidade de fortalecer a infraestrutura das redes para evitar novos casos de espionagem e garantir maior proteção à privacidade dos usuários.

Em paralelo, em janeiro de 2024, a Anatel abriu três processos administrativos para investigar o possível envolvimento de empresas de telefonia móvel no monitoramento ilegal de celulares por meio do software First Mile[9]. Conforme nota à imprensa,[10] a Anatel investiga se as operadoras, à época dos fatos, identificaram tentativas de acesso indevido às informações ou se tomaram conhecimento dessas ocorrências apenas posteriormente, por meio da imprensa. Seja qual for o caso, também apura o dever de comunicação à agência. As empresas negaram qualquer comunicação prévia com a Abin ou conhecimento sobre a espionagem ilegal e afirmaram que adotaram medidas de bloqueio contra acessos indevidos via protocolos de interconexão internacional. Os processos seguem sob sigilo, o que dificulta seu acompanhamento detalhado. Há notícias de que a Abin atuou sem interação prévia com as operadoras, mas ainda não se sabe exatamente quando as

---

[6] SUPREMO TRIBUNAL FEDERAL (STF). STF encerra audiência pública com diversidade de visões sobre as ferramentas de monitoramento. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-encerra-audiencia-publica-com-diversidade-de-visoes-sobre-as-ferramentas-de-monitoramento/.

[7] GLOBO. Abin paralela: PF e Anatel explicam vulnerabilidade que permitiu acesso à localização de celulares. O Globo, Rio de Janeiro, 18 jul. 2024. Disponível em: https://oglobo.globo.com/politica/noticia/2024/07/18/abin-paralela-pf-e-anatel-explicam-vulnerabilidade-que-permitiu-acesso-a-localizacao-de-celulares.ghtml.

[8] TELETIME. Sinalização de roaming foi a brecha para monitoramento ilegal da Abin e é investigado pela Polícia Federal. Teletime, 20 out. 2023. Disponível em: https://teletime.com.br/20/10/2023/sinalizacao-de-roaming-foi-a-brecha-para-monitoramento-ilegal-da-abin-e-investigado-pela-policia-federal/.

[9] AGÊNCIA BRASIL. Anatel investiga operadoras de celular por indícios de espionagem**.** Rádioagência Nacional, 6 fev. 2024. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2024-02/anatel-investigas-operadoras-de-celular-por-indicios-de-espionagem.

[10] AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). *Nota à imprensa*. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/nota-a-imprensa-11.

empresas perceberam os ataques. Apesar de terem adotado medidas para corrigir vulnerabilidades[11], não notificaram a agência, o que pode configurar uma irregularidade.[12]

Consideramos, neste contexto, a proliferação global de tecnologias de vigilância remota, secreta e invasiva, amplamente utilizadas por serviços de inteligência e órgãos de repressão estatais para monitorar cidadãos[13], bem como os casos recentes de contratações e tentativas, pelo poder público brasileiro, de ferramentas intrusivas para vigiar e intimidar jornalistas, ativistas, acadêmicos, políticos e funcionários públicos. Em particular, a investigação da contratação e do uso do spyware First Mile pela Abin evidencia os riscos que a exploração das vulnerabilidades dos sistemas de telecomunicações impõe a direitos fundamentais, como a privacidade, a intimidade e a inviolabilidade do sigilo das comunicações e dos dados pessoais. Embora as investigações ainda estejam em curso, os elementos já publicizados permitem questionar as vulnerabilidades, ações e omissões que facilitaram ataques e violações de direitos, além de fornecer subsídios para que esses casos não se repitam. Dado que spywares operam explorando falhas em dispositivos e sistemas operacionais sob responsabilidade das empresas de telecomunicações, analisamos as medidas adotadas por essas empresas para identificar, comunicar e mitigar tais riscos.

A partir do tema, nesta categoria, analisamos a possível inércia das operadoras diante de suas vulnerabilidades de segurança e dos indícios de interceptação ilegal das comunicações de seus usuários por meio de spywares. A avaliação não se limita ao atendimento de exigências formuladas por autoridades públicas, mas observa a conduta e o posicionamento das operadoras no debate público sobre o tema.

A análise considera se essas empresas evidenciam, de forma pública, sua conscientização e atuação em relação às medidas necessárias para: i) identificar e mitigar suas vulnerabilidades de segurança; e ii) projetar e comunicar os riscos associados à exploração dessas falhas, incluindo sua notificação aos usuários e agências reguladoras, como a Anatel.

---

[11] Temos ciência da notícia que indica que as empresas de telefonia consertaram a vulnerabilidade que permitia os ataques desde meados de 2023.

[12] KLEINA, Nilton Kleina. *Tim, Vivo e Claro não alertaram Anatel mesmo sabendo de possível ataque espião, diz jornal* 31 jan. 2024. Disponível em: https://www.tecmundo.com.br/seguranca/279478-tim-vivo-claro-nao-alertaram-anatel-mesmo-sabendo-possivel-ataque-espiao-diz-jornal.htm

[13] A título ilustrativo, são alguns desses casos as tentativas de contratação entre março de 2018 e início de 2019, por parte da força-tarefa que comandava a Operação Lava-Jato da aquisição do Spyware *Pegasus*. Também as tentativas de contratação da mesma tecnologia em licitação do Ministério da Justiça e Segurança Pública, em 2021. O *pegasus* é um dos spywares mais conhecidos e goi responsável por viabilizar o monitoramento ilegal de ao menos 180 jornalistas ao redor do mundo. As tentativas de contratação do Pegasus, que não tiveram êxito devido à pressão da sociedade civil e de autoridades. No entanto, temos outros exemplos de contratações realizadas de softwares espiões como o First Mile, que será abordado a seguir.

Dado o potencial impacto das tecnologias de espionagem a direitos fundamentais, a ausência de transparência quanto às medidas adotadas para mitigar esses riscos configura um fator de especial preocupação. Diante desse cenário, as notas para esse parâmetro foram congeladas até obtermos maiores informações acerca das ações dessas operadoras.

Quais foram os parâmetros de avaliação?

(I) [Posicionamento em geral]

A empresa se posicionou, em nome próprio, em consultas públicas, debates, ou na mídia, geral ou especializada. No posicionamento, ela defendeu concretamente a aprovação de normas ou adoção de técnicas que aumentem a proteção conferida aos usuários dos seus serviços.

(II) [Posicionamento quanto às suas vulnerabilidades de segurança]

A empresa adotou postura proativa para (i) identificar e mitigar suas vulnerabilidades de segurança; e (ii) se posicionou em nome próprio, em consultas públicas, debates ou na mídia, especializada ou não para projetar e comunicar os riscos associados à exploração dessas falhas, incluindo sua notificação aos usuários e agências reguladoras, como a Anatel.

Padrões de desempenho

O provedor de Internet atende aos dois parâmetros.	O provedor de Internet atende a um parâmetro.	O provedor de Internet não atende a nenhum dos parâmetros.
★	⯪	☆

CATEGORIA 5: Relatórios de transparência e de impacto à proteção de dados

A empresa publica, periodicamente, relatórios de transparência, em português e facilmente acessíveis, com informações básicas sobre pedidos de dados por autoridades públicas? A empresa elabora e publica relatórios de impacto à proteção de dados pessoais?

Os relatórios de transparência são informes emitidos por empresas que podem conter, entre outros conteúdos, estatísticas relativas a pedidos de dados. Esses relatórios revelam o quanto e como as empresas cooperam com as autoridades estatais, em geral por exigência legal fornecendo dados para a instrução processual em causas cíveis e criminais. Internacionalmente, a publicação desses relatórios por provedores de aplicações como Google, Facebook, Twitter, e Microsoft, bem como provedores de conexão à Internet e de telefonia móvel como a Vodafone e Verizon, já é uma prática estabelecida. No Brasil, contudo, a publicação dos relatórios de transparência ainda é uma prática pouco comum. Defende-se que a ausência de informações sobre os pedidos de acesso a dados por autoridades estatais, assim como as respostas que as empresas fornecem a tais pedidos, oculta ameaças e ataques a direitos de usuários, como a privacidade, e prejudica o debate público em torno de tais direitos.

Embora as empresas brasileiras não tenham, até o momento, a obrigação legal de produzir relatórios de transparência, também não há proibição para a publicação de estatísticas sobre pedidos e exibições de dados. Existe, portanto, a oportunidade de cultivar uma relação de confiança com usuários, baseada na transparência, além de contribuir para o debate público a respeito das prerrogativas de acesso a dados de usuários por parte das autoridades públicas.

Nesse sentido, o Decreto n.º 8.771/2016 (art. 12) cria a obrigação de órgãos da Administração Pública Federal divulgarem relatórios estatísticos similares aos citados acima. Tais relatórios devem incluir, por exemplo, a quantidade de requerimentos e de usuários afetados pelas solicitações e a relação de pedidos deferidos e indeferidos pelos provedores. Tais obrigações direcionadas a órgãos públicos reforçam o desenvolvimento de uma cultura nacional de transparência sobre pedidos de dados. Acreditamos que o setor privado possa, desde já e proativamente, se apropriar dessa pauta. Afinal, em manifestações a Comissões Parlamentares[14], empresas já mencionaram a vasta quantidade de pedidos que recebem. Além disso, a Associação Nacional de Operadoras Celulares (ACEL) e a **Associação Brasileira de**

[14] A **CPI das Escutas Telefônicas Clandestinas**, instaurada em dezembro de **2007** na **Câmara dos Deputados**, investigou interceptações ilegais no Brasil, após denúncias de grampos contra ministros do STF. A comissão buscou identificar responsáveis, critérios adotados e propor melhorias na legislação. Representantes das operadoras de telefonia foram convocados para esclarecer seus procedimentos. As empresas afirmaram que as interceptações ocorriam apenas mediante ordem judicial, conforme a Lei nº 9.296/96. **Em 2007, a pedido de autoridades para investigações criminais, foram realizadas 235 mil interceptações pela TIM, 92 mil pela Vivo, 33 mil pela Claro e 20 mil pela Oi.** Parlamentares questionaram a alta quantidade de escutas e sugeriram uma banalização do processo de quebra de sigilo telefônico.
CÂMARA DOS DEPUTADOS. **Câmara instala CPI sobre grampos telefônicos ilegais.** Portal da Câmara dos Deputados, Brasília, 19 dez. 2007. Disponível em: https://www.camara.leg.br/noticias/111887-CAMARA-INSTALA-CPI-SOBRE-GRAMPOS-TELEFONICOS-ILEGAIS.
GIRALDI, R. **À CPI, empresas informam que foram feitas 380 mil escutas telefônicas legais em 2007**. Folha de S. Paulo, São Paulo, 06 mar. 2008. Disponível em: https://www1.folha.uol.com.br/folha/brasil/ult96u379346.shtml.
BRASIL. Supremo Tribunal Federal. **Norma que autoriza MP e polícia a requisitar de telefônicas dados cadastrais de investigados é válida, decide STF**. Notícias STF, Brasília, DF, 11 set. 2024.

Concessionárias de Serviço Telefônico Fixo Comutado (Abrafix) , em manifestações feitas nas ADIs 5063 e 4906, respectivamente, afirmaram que há abusos na atuação das autoridades públicas, como pedidos sem fundamentação. Nesse contexto, torna-se cada vez mais importante a criação de canais de acompanhamento periódicos dessas informações por usuários, por exemplo, pela sua publicação em relatórios ou informes de transparência.

A Lei Geral de Proteção de Dados estabelece os Relatórios de Impacto à Proteção de Dados Pessoais (RIDP) como documentos que descrevem os 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, XVII). Embora, em regra,[15] sua divulgação não seja obrigatória, a ANPD destaca tal prática como uma estratégia importante para demonstrar o compromisso privacidade e a segurança dos titulares. A publicação do RIPD reforça a transparência e a responsabilização das organizações, alinhando-se aos princípios da LGPD, como livre acesso, transparência e prestação de contas. Isso significa a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais durante todas as fases de tratamento dessas informações pelos controladores (art. 6º, X). Para tal, a ANPD recomenda que o RIPD seja disponibilizado em meios de fácil acesso pelo titular, especialmente em seus sítios eletrônicos, de forma clara, adequada e ostensiva, contendo informações sobre suas atividades de tratamento de dados pessoais.[16]

Para a presente avaliação, a acessibilidade e publicidade dos relatórios também foram analisadas. Isto é, somente relatórios escritos ou traduzidos para a língua portuguesa foram considerados. Por fim, os relatórios facilmente acessíveis nas páginas principais, de contratação de serviços ou publicizados na mídia foram melhores avaliados.

Quais foram os parâmetros de avaliação?

(I) **[Publicação de relatório]**
A empresa publica relatório de transparência em português sobre privacidade e proteção de dados.

(II) **[Acessibilidade do relatório]**
O relatório de transparência é facilmente acessível ao público em geral.

---

[15] Especificamente em relação a entidades e órgãos públicos, o RIPD deverá ser publicado: (i) por determinação da ANPD, nos termos do art. 32 da LGPD; ou (ii) pelo próprio controlador, quando não identificada hipótese de sigilo aplicável ao caso, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011.

[16] A própria ANPD reconhece que a necessidade de proteção de segredos comerciais e industriais não é, por si só, uma justificativa absoluta para impedir a publicação do RIPD, uma vez que a autoridade prevê a possibilidade de disponibilizar uma versão pública distinta da versão interna.

(III) **[Periodicidade do relatório]**
O relatório de transparência é publicado com periodicidade mínima anual.

(IV) **[Informações sobre pedidos de acesso a dados]**
A empresa apresenta, no relatório de transparência:

a) Informações sobre pedidos de acesso a dados recebidos, atendidos e rejeitados;

b) Informação sobre o tipo de dado solicitado (se as demandas buscavam conteúdo de comunicação, apenas metadados ou ambos);

c) Informações sobre número de contas afetadas.

(V) **[Relatório de impacto à proteção de dados]**
A empresa elabora e publica Relatórios de Impacto à Proteção de Dados Pessoais.

Padrões de desempenho

O provedor de Internet atende a todos os parâmetros.	O provedor de Internet atende a quatro parâmetros.	O provedor de Internet atende a dois ou três parâmetros.	O provedor de Internet atende a um parâmetro.	O provedor de Internet não atende a nenhum dos parâmetros.
				

CATEGORIA 6: Notificação do usuário

A empresa notifica usuários quando recebe pedidos de dados?

A categoria analisa se a empresa notifica os usuários sobre os pedidos de acesso a dados pelas autoridades administrativas ou judiciais competentes. Acreditamos que a prática é fundamental para garantir a ampla defesa, o contraditório e, assim, a proteção contra abusos e irregularidades.

O impacto de notificações para a garantia da efetiva e ampla defesa e contraditório em um Estado de Direito não é novidade. À luz do princípio constitucional do devido processo, a legislação estabelece o dever de notificar atingidos sobre medidas que afetam seus direitos. Pelo Código de Processo Penal brasileiro, por exemplo, quando o juiz recebe um pedido de imposição

de medida cautelar contra alguém, cabe à autoridade avisar o investigado sobre o pedido, para que possa apresentar seus argumentos de defesa (art. 282, § 3º).

No contexto de solicitações de dados, provedores de Internet ganham papel fundamental na proteção de garantias processuais de investigados. Isso porque a notificação do usuário por parte das empresas possibilita que ele conteste pedidos ilegais desde o início da investigação. Os pedidos podem ser ilegais, seja por falta de fundamentação, seja por falta de competência legal da autoridade. Sem a notificação, o usuário depende da contestação feita pelas próprias empresas contra pedidos que elas consideram abusivos. Ao serem notificados pelas empresas, os usuários ganham a chance de se defenderem contra potenciais violações de sua privacidade.

Tendo isso em mente, consideramos importante incentivar a prática de notificação de usuários no QDSD. Vale lembrar que, em casos de pedidos de dados não acompanhados pela obrigação de sigilo, a notificação de empresas ao usuário afetado é **autorizada** pela legislação brasileira, dada a ausência de prescrição legal em sentido contrário. Com efeito, algumas provedoras de aplicações de Internet já assumem esse tipo de compromisso em sua atuação no Brasil. Por exemplo, o Facebook, além de garantir a notificação prévia do usuário, se compromete a fornecer a notificação em atraso, após o término do período de sigilo, judicialmente estabelecido.

A possibilidade de notificação do usuário pode ser vislumbrada, por exemplo, em casos de pedidos de dados de identificação pela justiça cível, bem como por outros órgãos da Administração, como a Receita Federal ou a ANATEL. Até mesmo no âmbito de processos penais, a notificação prévia à entrega de dados é, em geral, permitida, exceto em casos de sigilo. Tal procedimento viabiliza os princípios constitucionais da ampla defesa e do contraditório, reforçando a possibilidade de contestação à produção de provas irrelevantes ou desnecessárias para o caso. Por fim, a notificação é um elemento fundamental no fomento a uma cultura de proteção da privacidade.

Qual foi o parâmetro de avaliação?

(I) **[Notificação]** A empresa promete notificar o usuário antes da entrega, ou assim que permitido, dos dados cadastrais e registros de conexão, exceto se o sigilo da entrega for imposto por lei ou determinado em decisão judicial.

Padrões de desempenho

O provedor de Internet atende ao parâmetro.	O provedor de Internet não atende ao parâmetro.

V. RESULTADOS

BRISANET

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 
Nesta categoria, a BRISANET obteve **3/4 de estrela**, tendo atendido integralmente os parâmetros II, III, IV e V.

Considerando-se que os critérios (a) e (b) foram atendidos e o critério (e) foi parcialmente atendido, o **parâmetro I** foi considerado **parcialmente atendido**.

Sub-parâmetro (a): atendido. Em sua *Política de privacidade*, a empresa elenca extensivamente os dados coletados (vide excerto abaixo):

> O que coletamos:
>
> Nome completo, CPF, RG, e-mail, telefone residencial, celular, endereço, tipo de moradia, data de nascimento, estado civil, tipo de público, biometria facial.
>
> Para que coletamos:
>
> Identificar e autenticar você;
>
> Cumprir as obrigações decorrentes do uso dos nossos serviços e funcionalidades, inclusive para atendimento de disposições legais e regulatórias;
>
> Apresentar nossos serviços e condições comerciais aplicáveis à sua região;
>
> Permitir que Você realize a contratação dos serviços disponíveis em nosso Site;
>
> Adimplir com as obrigações contratuais relativas às contratações efetuadas por Você de nossos serviços;
>
> Conhecer melhor seu perfil e possibilitar nosso contato, caso você deseje se tornar um representante do Grupo Brisanet;
>
> Possibilitar a sua participação e das pessoas a quem você nos indicar, nas ações/campanhas promocionais realizadas por nós;

> Enriquecer sua experiência conosco, gerenciando suas dúvidas e solicitações;- Permitir que Você nos envie uma manifestação através de nosso canal de Ouvidoria disponível em nosso Site;
>
> Garantir a portabilidade dos Dados cadastrais para outro Controlador do mesmo ramo de nossa atuação, caso solicitado por Você, cumprindo com obrigação do artigo 18 da Lei Geral de Proteção de Dados Pessoais;
>
> Proteger Você no que diz respeito à prevenção de fraudes e riscos associados, além do cumprimento de obrigações legais e regulatórias;

Sub-parâmetro (b): atendido. Mesmo que não haja redação específica nesse sentido, nos mesmos trechos apontados acima, informa-se indiretamente quais as situações em que a coleta ocorre. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

Sub-parâmetro (c): não atendido. A empresa não menciona a possibilidade de coleta de dados disponíveis publicamente.

Sub-parâmetro (d): não atendido. A *Política de Privacidade* da Brisanet não faz menção à coleta de dados por meio de terceiros. Tampouco lista as categorias ou, nominalmente, as organizações envolvidas neste tipo de coleta.

Sub-parâmetro (e): parcialmente atendido. A Política de Privacidade da Brisanet afirma que o tratamento de dados por terceiros em seu nome respeitará "as condições estipuladas [na Política] e as normas de segurança da informação, obrigatoriamente". No entanto, não há listagem das formas de avaliação de terceiros empregadas pela operadora.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a finalidade da utilização dos dados e o tipo ou a forma de tratamento, considerou-se **atendido**, pois os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): atendido. Na sua *Política de Privacidade*, na seção 'Sobre os dados que coletamos", a empresa explica, de forma detalhada, quais são as funções para cada dado coletado.

Sub-parâmetro (b): atendido. Desde que as formas de utilização descritas na Política de Privacidade da Brisanet abranjam integralmente todas as suas atividades de tratamento de dados, a listagem apresentada no item "Sobre os dados que coletamos" será considerada suficiente.

Quanto ao **parâmetro III,** referente ao fornecimento de informações claras e completas sobre armazenamento, segurança e compartilhamento, considerou-se **atendido**, pois os subparâmetros (a), (b), e (g) foram atendidos (c), (d), (e) e (f) foram parcialmente presentes

Sub-parâmetro (a): atendido. Em sua *Política de Privacidade*, no item 'Como armazenamos seus dados pessoais e o registro de atividades', a empresa prevê os períodos exatos de armazenamento em conformidade aos fundamentos legais.

Sub-parâmetro (b): atendido. Do trecho acima, infere-se que os dados são apagados após o decurso do prazo apontado.

Sub-parâmetro (c): parcialmente atendido. A Política de Privacidade meramente cita algumas hipóteses de retenção de dados, sem correlacionar tais hipóteses com os tipos de dados detidos pela empresa.

Sub-parâmetro (d): parcialmente atendido. No item "Como protegemos seus dados e como você também poderá protegê-los", a Política de Privacidade exemplifica, de maneira genérica, algumas medidas administrativas e técnicas de proteção dos dados. Não contamos, no entanto, com indicações dos procedimentos e tecnologias empregados em consonância com estas medidas.

Sub-parâmetro (e): parcialmente atendido. Conforme item acima, a empresa menciona somente "acesso a pessoas não autorizadas".

Sub-parâmetro (f): parcialmente atendidos. O item 'Hipóteses de compartilhamento de dados' foi considerado insuficiente para compreender com quais categorias de colaboradores a empresa compartilha seus dados; essa informação está presente apenas de forma genérica:

> Com empresas do mesmo grupo econômico, sempre em observância às diretrizes de segurança e proteção de dados; e
>
> Com empresas parceiras e prestadores de serviços necessários à execução dos nossos serviços e funcionalidades, sempre exigindo de tais organizações o cumprimento das diretrizes de segurança e proteção de dados.

Sub-parâmetro (g): atendido. No item "Compartilhamento de dados", a Política de Privacidade da Brisanet elenca todas as hipóteses de compartilhamento com os terceiros citados.

Sub-parâmetro (h): não atendido. A Política de Privacidade da Brisanet apenas menciona que alguns dados serão armazenados em nuvens localizadas fora do Brasil, sem, no entanto, fornecer detalhes sobre (i) o tipo de dado armazenado nestas circunstâncias; (ii) os países nos quais os dados podem ser armazenados; (iii) os responsáveis pelo fornecimento das nuvens utilizadas pela operadora.

Considerando-se que os critérios (a) e (b) estavam presentes, o **parâmetro IV** foi considerado **atendido**.

Sub-parâmetro (a): atendido. Na política de privacidade, a Brisanet informa sobre direitos de titulares de dados na seção "Seus direitos".

Sub-parâmetro (b): atendido. No mesmo documento, a empresa dispõe sobre os canais de atendimento adequados para o exercício de direitos.

Considerando-se que os critérios (a) e (b) estavam presentes, o **parâmetro V** foi considerado **atendido.**

Subparâmetro (a) e (b): atendidos. A Brisanet disponibiliza um e-mail para o exercício de direitos (ouvidoria@grupobrisanet.com.br) para não clientes. Uma integrante da nossa equipe realizou solicitação e a empresa respondeu em tempo hábil alegando inexistência de dados das requerentes.

O **parâmetro VI**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado **não atendido**. A BRISANET afirma, em sua Política de Privacidade, que não notificará os usuários em casos de alterações da política:

> Você reconhece o nosso direito de alterar o teor desta Política a qualquer momento, conforme a finalidade ou necessidade, tal qual para adequação e conformidade legal de disposição de lei ou norma que tenha força jurídica equivalente, cabendo a Você verificá-la sempre que efetuar o acesso ao nosso Site ou utilizar nossos serviços e funcionalidades.
>
> Ocorrendo atualizações neste documento e que demandem nova coleta de consentimento, Você será notificado por meio dos canais de contato que Você informar.

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado **parcialmente atendido**. A Brisanet disponibiliza informações sobre privacidade e proteção de dados em seu site, como em sua Política de Privacidade. No entanto, o contrato de adesão não possui nenhuma disposição diretamente relacionada ao cumprimento da integralidade das obrigações de controlador de dados segundo a legislação nacional (inclusive a LGPD), e não menciona as Políticas de Privacidade e Proteção de Dados disponibilizadas no site da Brisanet.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a BRISANET **não obteve estrela**, pois não cumpriu nenhum dos parâmetros.

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado não atendido. Em sua *Política de Privacidade*, a empresa apenas menciona genericamente o compartilhamento com autoridades públicas "sempre que houver determinação legal, requerimento, requisição ou ordem judicial." Nenhuma outra política divulgada e relacionada à entrega de dados às autoridades foi identificada no Centro de Privacidade da Brisanet..

O **parâmetro II**, referente ao oferecimento de informações sobre dados de geolocalização, também foi considerado **não atendido**, pois não localizamos as informações nos contratos ou documentos da Brisanet.

O **parâmetro III,** referente a registros de conexão, também foi considerado **não atendido**. Não localizamos essas informações nos contratos ou documentos da Brisanet.

O **parâmetro IV**, referente ao compromisso de não atender e/ou contestar pedidos genéricos, também foi considerado **não atendido**. Não localizamos essas informações nos contratos ou documentos da Brisanet.

Por fim, o **parâmetro V**, relativo à existência de protocolos específicos sobre entrega de dados ao Estado, foi considerado **não atendido**. Não foi encontrada menção ao tema nos documentos analisados.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 
Nesta categoria, a Brisanet obteve **estrela vazia,** pois não atendeu aos parâmetros.

O **parâmetro I**, referente à contestação de legislação, **não foi atendido**. Realizamos buscas em todos os tribunais superiores, como STF e o STJ a partir do nome da empresa (“Brisanet Serviços de Telecomunicações S.A” e “Brisanet”). Além disso, pesquisamos os termos em sites de buscadores de processos. Então, visitamos todos os processos que a Brisanet é parte e não localizamos contestações de legislações violadoras da privacidade. Conforme essa metodologia, nesta etapa da pesquisa, não localizamos contestações, por parte da Brisanet, quer de pedidos abusivos, quer de legislação violadora da privacidade.

O **parâmetro II**, referente à contestação de pedidos abusivos, também **não foi atendido**. Não encontramos contestações da Brisanet a pedidos abusivos nem a legislações que violem a privacidade. Para isso, realizamos buscas nos tribunais superiores, como STF e STJ, utilizando o nome da empresa (“Brisanet Serviços de Telecomunicações S.A.” e “Brisanet”). Além disso, consultamos plataformas de busca de processos e analisamos individualmente todas as ações em que a Brisanet figura como parte. Não identificamos, até o momento, registros de contestações relacionadas a esses temas.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 
Nesta categoria, a BRISANET obteve **1/4 de estrela**, pois cumpriu parcialmente o parâmetro I.

O **parâmetro I** foi **parcialmente atendido**, pois embora não tenhamos identificado manifestações públicas da empresa em nome próprio em fóruns legislativos, consultas públicas ou imprensa especializada sobre políticas de proteção de dados, a Brisanet demonstrou esforços de conscientização por meio de seu blog institucional. **Foram localizados conteúdos educativos sobre ataques cibernéticos, armazenamento seguro em nuvem e boas práticas de segurança digital,** voltados à orientação dos usuários. Essas ações contribuem para a cultura de proteção de dados, ainda que não configurem um posicionamento público formal em defesa de normas ou políticas.

A Brisanet **não obteve pontuação no parâmetro II**, pois **não atendeu aos critérios estabelecidos**. Este parâmetro avalia se a empresa adotou postura proativa na identificação e mitigação de vulnerabilidades de segurança, e se comunicou, em nome próprio, os riscos

associados — especialmente em contextos como o uso indevido de tecnologias de vigilância, conforme descrito no documento metodológico.

Embora o blog da Brisanet contenha conteúdos genéricos sobre cibersegurança e boas práticas digitais, isso não configura posicionamento institucional em consultas públicas, debates especializados ou diálogo com órgãos como a Anatel. Como esses materiais já foram considerados no Parâmetro I, **não há elementos suficientes para justificar pontuação aqui**, que exige ações concretas e visibilidade pública da empresa em resposta a riscos de segurança.

CATEGORIA 5: Relatórios de transparência e de impacto à proteção de dados

Resultado: 

Nesta, a BRISANET **não obteve estrela**, pois não cumpriu nenhum dos parâmetros.

A Brisanet não atende ao **parâmetro I**, pois não identificamos nenhum documento da empresa relacionado a esse critério.

A Brisanet não atende ao **parâmetro II**, pois não identificamos nenhum documento da empresa relacionado a esse critério. Diante da ausência de material, não é possível avaliar sua acessibilidade.

A Brisanet não atende ao **parâmetro III**, pois não identificamos nenhum documento da empresa relacionado a esse critério.

A Brisanet não atende ao **parâmetro IV**, pois não identificamos nenhum documento da empresa relacionado a esse critério - nem informações sobre pedidos de acesso a dados ou contas afetadas em outros documentos.

A Brisanet não atende ao **parâmetro V**, pois não identificamos nenhum documento da empresa relacionado a esse critério.

CATEGORIA 6: Notificação do usuário

Resultado: 

Nesta categoria, a Brisanet obteve **estrela vazia**, pois não atendeu ao parâmetro.

A Brisanet não atende ao **parâmetro I**, pois não identificamos nenhum documento da empresa relacionado a esse critério.

CLARO

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 
Nesta categoria, a Claro obteve **estrela cheia**, tendo atendido a todos os parâmetros.

A Claro atende integralmente ao parâmetro I, fornecendo informações claras e completas sobre os 5 sub-parâmetros.

Sub-parâmetro (a): atendido. Em seu Portal da Privacidade, a empresa elenca extensivamente os dados coletados (vide excerto abaixo):

> Quais dados pessoais coletamos??
> - Dados cadastrais e de qualificação: nome, CPF, RG, CNH, data de nascimento, gênero, profissão, idade, fotos, áudios, vídeos, estado civil, nacionalidade, naturalidade, filiação, usuário/login, telefone, e-mail, endereço.
> - Dados financeiros e de pagamento: dados bancários ou de cartões de crédito e débito (nome do titular, nº do cartão, data de validade, etc.), informações da fatura e de outras formas de pagamento, score de crédito, contestações e atrasos de conta, registro de crédito.
> - Dados de navegação e uso dos produtos e serviços Claro: dados sobre navegadores e dispositivos (IP, atividade do sistema, data, hora e URL), dados sobre ligações e telefonia (destino, duração e envio de mensagens SMS, chamadas realizadas e recebidas, envio de SMS, volume de dados utilizados, antenas que te atendem), registros de conexão à Internet e de acesso às aplicações da Claro, IMEI, MacAddress, histórico e informações de navegação na Internet, dados coletados por cookies.
> - Dados e consumo de preferências: dados de geolocalização e de outros que possibilitam saber a sua localização em tempo real, por meio de coordenadas de latitude e longitude e um raio de precisão.
> - Fotografia e dados biométricos: sua imagem em documentos e em fotos tiradas nas lojas físicas ou no autoatendimento e imagens das câmeras de segurança em lojas físicas.
> - Dados baseados na sua interação com os nossos serviços e consumo de conteúdo: interações entre ID do equipamento utilizado e nossos serviços, como cliques em conteúdos, conteúdos assistidos (plays), favoritos, avaliações, compra e aluguel de filmes, conteúdos assistidos na TV linear, criação de lembretes de programas de TV e conteúdos agendados para gravação.
> - Gravações telefônicas do SAC: chamadas gravadas ao ligar para o Atendimento Claro.

O InternetLab enaltece, ainda, a conduta da Claro de esclarecer quais dados coleta das pessoas que sequer são seus clientes, como se vê no seu Portal da Privacidade:

> Se você entrou em contato com nossa Central de Vendas em busca da contratação de um produto ou serviço, mas interrompeu a contratação, o seu contato fica registrado e podemos entrar em contato para entender melhor como podemos ajudar.

> Da mesma forma, se você entrar em algum de nossos sites e escolher alguns produtos, mas abandonar o carrinho, vamos lembrá-lo a respeito dessa intenção de compra para confirmar se você mantém o interesse.
> Obtemos informações de empresas com bases de dados legítimas e de procedência adequada, para buscar trazer novos clientes para a Claro.
> Temos agentes autorizados, que vendem produtos e serviços da Claro e realizam atendimento conforme previsto na regulamentação. Eles também prospectam clientes e são orientados a seguir as boas práticas relacionadas, inclusive consulta aos cadastros Não Perturbe e Não me Perturbe.

Sub-parâmetro (b): atendido. A Claro indica, também no Portal de Privacidade, como coleta os dados pessoais no item 'Como coletamos os seus dados'.

Sub-parâmetro (c): atendido. Na mesma seção apontada no subparâmetro (a) acima, há o relato de que dados públicos disponíveis são coletados pela empresa.

Sub-parâmetro (d): atendido. A empresa divulga, no Portal de Privacidade, a lista de terceiros com quem compartilha os dados por categorias.

Sub-parâmetro (e): atendido. A Claro esclarece em seu Portal de Privacidade, no item 'Seus dados podem ser compartilhados?', de forma específica sobre privacidade e proteção de dados em que são exigidos dos terceiros pleno cuidado e garantias do tratamento dos dados:

> A Claro exige que esses terceiros deverão observar certos cuidados no tratamento, como a segurança dos seus dados.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a finalidade da utilização dos dados e o tipo ou a forma de tratamento, considerou-se **atendido**, pois os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): atendido. No seu Portal da Privacidade, na seção "Para que precisamos dos seus dados?", a empresa explica, de forma detalhada, quais são as funções para cada tipo de dado coletado. Como no caso da finalidade "Fornecer nossos produtos e serviços e executar nosso contrato com você", em dá exemplos concretos ("cadastrar seu contrato como cliente, cobrar pelos serviços contratados, melhorar nosso serviços, atender ordens de serviço, realizar recargas"), os produtos e serviços em referência ("• Mobilidade: Telefonia móvel e Telefonia fixa; Entretenimento: Claro TV, TV+, Música e Serviços Digitais; Conectividade: Virtua e Wi-fi; e Soluções para Empresas: PME, Claro Empresas e Embratel."e os tipos de dados utilizados (dados cadastrais, dados financeiros e dados de consumo e de preferências).

Sub-parâmetro (b): atendido. No trecho "Fique por dentro dos tratamentos de dados feitos pela Claro", de sua Política de Privacidade, a empresa indiretamente esclarece as maneiras de uso dos dados pessoais coletados. Além disso, aponta no início do seu Portal de Privacidade:

> Aqui, você fica por dentro dos tratamentos de dados feitos pela Claro em:
>
> • Mobilidade, como planos pré-pagos, controle e pós-pagos;

• Entretenimento, como NOW e TV (DTH e cabo);

• Conectividade, como banda larga Vírtua e Wi-fi;

• Empresas, soluções Claro empresas e Embratel.

Quanto ao **parâmetro III,** referente ao fornecimento de informações claras e completas sobre armazenamento, segurança e compartilhamento, considerou-se **atendido**, pois todos os sub-parâmetros foram atendidos.

Sub-parâmetro (a): No seu Portal de Privacidade, na seção "Por quanto tempo armazenamos seus dados e onde?", a empresa indica que que o armazenamento de dados se dá apenas pelo tempo necessário para atingir as finalidades informadas e indica as hipóteses de análise em casos nos quais é preciso reter os dados por mais tempos (isto é, analisam se há uma obrigação legal regulatória, contratual ou imposta por autoridade competente de reter dados pessoais; se são necessários para manter registros históricos, comerciais e financeiros precisos ou para atender determinações internas da Claro, inclusive para exercício regular de seus direitos ou, ainda, se são necessários para cumprir a lei). Alguns exemplos de prazos de retenção pela Claro são:

6 meses: registros de acesso a funcionalidade de internet nos aplicativos da Claro.

1 ano, no mínimo: registros de conexão à internet, mas sem guardar os registros de acesso.

até 6 meses: gravação da interação entre você e atendente no SAC.

5 anos, no mínimo: documentos fiscais que englobam dados das ligações efetuadas e recebidas, data e horário de duração e valor da chamada.

10 anos: dados cadastrais e de faturamento.

A Claro também reforça a segurança do armazenamento dos dados e indica que são armazenados nacionalmente - em seus servidores nos data centers situados nas cidades de São Paulo, Campinas e Rio de Janeiro - e internacionalmente - em nuvem, em servidores localizados no território estrangeiro, como nos Estados Unidos -, atentos às orientações da ANPD, que ainda regulamentará esse tipo de tratamento.

Sub-parâmetro (b): Isso porque, no mesmo trecho apontado acima, infere-se que os dados são apagados após o decurso do prazo apontado.

Sub-parâmetro (c): No Portal de Privacidade, no mesmo item referenciado acima, há as hipóteses de retenção dos dados.

Sub-parâmetro (d): No Portal de Privacidade, a empresa se compromete a seguir padrões de segurança e controle, sem especificar neste documento, no entanto, quais são as práticas adotadas.

A Claro utiliza:

• soluções e medidas técnicas de segurança, visando preservar a inviolabilidade dos dados compatíveis com os padrões internacionais e com as boas práticas do setor;

• medidas de segurança apropriadas na atuação contra os riscos de perda acidental ou ilegal, alteração, divulgação ou acesso não autorizado.

Apesar da informação genérica do Portal de Privacidade, a empresa apresenta mais informações sobre as práticas de segurança adotadas nos Sustainability Report 2022 (p. 53) do grupo América Móvil. De acordo com o relatório, o sistema adotado no Brasil é o Security Operation Center com certificado ISO 45001 Safety Management Systems.

Além disso, a empresa possui um documento integralmente dedicado à questão da segurança, a 'Política de Segurança da Informação e Segurança Cibernética'.

Sub-parâmetro (e): sso porque a empresa divulga, em seu Portal de Privacidade, no item "Quem tem acesso aos seus dados na Claro?", sobre o controle de acesso por meio de uma "Políticas de Acesso às informações".

Sub-parâmetro (f): No item "Seus dados podem ser compartilhados?", a empresa expõe categorias gerais de terceiros com os quais os dados podem ser compartilhados (autoridades administrativas e judiciais; escritórios de advocacia, Setor Público e empresas do mesmo grupo ou afiliadas) e a respectiva finalidade do compartilhamento. Além disso, indica como

A Claro é considerada controladora dos dados pessoais, assim como cada uma das empresas do grupo. São elas:

• **Claro S/A** - prestadora dos serviços de telefonia móvel, telefonia fixa, longa distância nacional, televisão por assinatura a cabo, internet fixa e móvel e serviços de valor adicionado;

• **Embratel TVSAT Telecomunicações** - prestadora dos serviços de televisão por assinatura, por meio da tecnologia DTH;

• **Claro Nxt** - prestadora dos serviços de telefonia móvel e longa distância nacional.

Para realizar todas as suas atividades, a Claro precisa compartilhar seus dados com alguns terceiros. Afinal, são eles que vão prestar serviços para você e deverão observar certos cuidados, como a segurança dos seus dados. Veja quais são esses terceiros:

1. Empresas de Call Center – Realização de atendimento a clientes e clientes prospectivos.

2. Empresas de Serviços Técnicos – Instalação e manutenção de serviços Claro, como TV e Internet.

3. Empresas que comercializam conteúdos via Claro - Comercialização de conteúdos de terceiros nos canais de vendas da Claro e que precisam de algumas informações para ativarem os conteúdos e assinaturas.

4. Empresas de Crédito e Cobrança – Realização de cobranças das faturas em aberto.

> 5. Empresas de Soluções de Crédito - Fornecimento de insumos para o desenvolvimento de produtos voltados à análise e concessão de crédito e soluções antifraude.
>
> 6. Agentes Autorizados – Venda de produtos e serviços com a marca Claro, que muitas vezes são a porta de entrada dos clientes

Além disso, em seu Contrato de Prestação de Serviço SMP pré-pago, afirma:

> 15.6 Todas as informações do cadastro do ASSINANTE são confidenciais e só poderão ser fornecidas: a) ao ASSINANTE; b) ao representante com procuração específica; c) à autoridade judicial; e d) a outras Prestadoras de Serviços de Telecomunicações, para fins específicos para prestação desses serviços.

Sub-parâmetro (g): Em vista dos detalhamentos de cada compartilhamento conforme trecho do Portal da Privacidade apontado acima.

Sub-parâmetro (h): Em seu Portal da Privacidade, a Claro possui um item destinado à transferência internacional de dados:

> Além disso, também são armazenados em nuvem, em servidores localizados no território estrangeiro, como nos Estados Unidos com graus de proteção de dados pessoais adequados ao previsto na Lei. Ainda assim, seguimos atentos às orientações da ANPD, que regulamentará esse tipo de tratamento.

O **parâmetro IV**, que avalia se a empresa disponibiliza informações claras e completas acerca dos direitos dos titulares, foi considerado **atendido**, visto que os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): A Claro atende integralmente o subparâmetro a. No Portal da Privacidade, há a seção "Quais são os seus direitos em relação aos seus dados pessoais?", em que a empresa informa sobre a existência dos direitos do titular previstos na Lei Geral de Proteção de Dados.

Sub-parâmetro (b): A Claro atende integralmente o subparâmetro b. Na mesma seção do item anterior, a empresa indica os meios de exercício desses direitos por meio de portal destinado a tal finalidade ou por meio do endereço de e-mail dpo@claroatendimento.com.br.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado **atendido**, pois todos os sub-parâmetros foram atendidos.

Sub-parâmetro (a) e (b): atendidos. A Claro disponibiliza Portal para exercícios de direitos a clientes e não clientes segundo a LGPD e atendeu integralmente os subparâmetros a e b. Por meio do canal, uma de nossas pesquisadoras fez solicitações de i) confirmação de tratamento de dados/acesso a dados; ii) compartilhamento de dados. A Claro retornou às solicitações com respostas claras, completas e em tempo hábil.

O **parâmetro VI**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado **atendido**. A Claro dispõe, em seu contrato, que "quando [atualizações da Política de Privacidade] ocorrerem, você será informado", além de indicar a data da última modificação. Também dispõe em sua Política de Privacidade que em caso de atualizações o cliente será informado e a empresa indicará na Política, a data da última atualização. Nas contribuições à pesquisa, a empresa também demonstrou que, entre 25/10/2024 e 14/11/2024, comunicou sua base de clientes sobre a atualização da política ocorrida em 26/09/2024, "sendo 22 milhões de mensagens via SMS e 21 milhões de mensagens via e-mail".

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado **atendido**. A Claro disponibiliza informações completas e claras de forma acessível em seu Portal de Privacidade, em diversas páginas e documentos, como a sua Política de privacidade, a sua Página de solicitações, o seu Portal de segurança e no Contrato de prestação de serviço móvel (pré-pago) (item 15.11).

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Claro **obteve estrela cheia**, pois cumpriu todos os parâmetros.

A Claro **atende integralmente** ao **parâmetro I.**

Sub-parâmetro (a): atendido. Em seu Portal de Privacidade, a empresa informa sobre as situações em que compartilha dados com o Setor Público:

> 14. Setor Público - A Claro também compartilha dados pessoais com nosso órgão regulador — ANATEL —, mediante requisições de autoridades administrativas competentes, como Polícia Civil, Polícia Federal, Polícia Militar, Polícia Legislativa, em cumprimento às legislações específicas*; Ministério Público Estadual, Ministério Público Federal, Ministério Público Militar. E nas demais situações, através de cumprimento de decisões judiciais.
>
> Nas demais situações, através de cumprimento de decisões judiciais.
>
> *Lei 12.830 de 20 de junho de 2013 (Lei dos Delegados); Art. 15 da Lei 12.850 de 02 de agosto de 2013 (Lei do Crime Organizado) e Art. 17-B da Lei 9613 de 03 de março de 2018 (Lavagem de Dinheiro) os quais o Delegado de polícia e o Ministério Público terão acesso, independente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito; art. 13-A do Decreto-Lei 3689 de 03 de Outubro de 1941 que

> autoriza o Ministério Público e o Delegado de Polícia a requisitar dados e informações cadastrais da vítima ou de suspeitos e as requisições podem ser dirigidas a qualquer órgão público ou empresa de iniciativa privada e art. 269 do Regimento Interno da Câmara e Resolução 18 da Câmara dos Deputados de 18 dezembro de 2003.

Ainda neste aspecto, vale destacar que a empresa faz referência no contrato a dispositivos da ANATEL que contêm direitos e estabelecem deveres:

> **Contrato de prestação de serviço de comunicação multimídia (SCM)**
>
> 35.02 Os direitos e deveres dos assinantes do serviço de comunicação multimídia estão previstos nos artigos 56, 57 e 58 da Resolução 614/2013 da ANATEL. Os direitos e obrigações da PRESTADORA estão previstos nos artigos 41 a 55 da mesma Resolução.
>
> **Contrato de prestação de serviços SMP pré-pago:**
>
> "16.6 Todas as informações do cadastro do ASSINANTE são confidenciais e só poderão ser fornecidas: a) ao ASSINANTE; b) ao representante com procuração específica; c) à autoridade judicial; e d) a outras Prestadoras de Serviços de Telecomunicações, para fins específicos para prestação desses serviços."

Sub-parâmetro (b): atendido. No mesmo trecho apontado do seu Portal de Privacidade acima, a empresa aponta as leis sob as quais as autoridades apontadas (Polícia Militar, Legislativa etc.) poderão requisitar dados. Além disso, menciona superficialmente os crimes apontados no Art. 13-A do Código de Processo Penal no trecho relativo aos dados de localização.

A Claro também **atende integralmente** ao **parâmetro II**.

Subparâmetros (a), (b) e (c): atendidos. A empresa fornece as informações em seu Portal de Privacidade, ao apontar "Quais dados pessoais a Claro coleta e para quais finalidades eles são utilizados":

> • Dados de Localização:
> • Quais Dados: dados de geolocalização.
> • Finalidades:
> - criação de produtos e serviços não relacionados à publicidade, como o Claro Valida-explicado mais abaixo;
> - medir e realizar melhorias na qualidade dos serviços Claro na sua localidade e cumprir com as determinações previstas pelo órgão regulador e pela legislação. Quando necessário à prevenção e à repressão de crimes relacionados ao tráfico de pessoas, fornecemos

> acesso a esses dados em atendimento a ordens judiciais ou, na ausência de manifestação judicial no prazo de 12 (doze) horas, mediante requisição das autoridades competentes.

A Claro **atende integralmente** ao **parâmetro III**. No Portal de Privacidade da Claro, definem-se os registros de conexão e promete-se que serão entregues somente mediante ordem judicial:

> • Registros de Conexão à Internet:
>
> • Quais Dados: informações relativas à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados.
>
> • Finalidades: Cumprimento de obrigações regulatórias previstas na Lei 13.965/14, o Marco Civil da Internet (MCI). Requisições de acesso aos registros de conexão só são concedidas nos termos do Marco Civil da Internet (MCI), sempre através de determinação judicial.

A Claro também **atende integralmente** ao **parâmetro IV**, visto que passou a prever, em sua Política de Privacidade , que "conforme previsto na legislação vigente não atendemos a solicitações ou pedidos genéricos de acesso a dados ou informações pessoais". A menção expressa à vedação desse tipo de requisição atende ao parâmetro ao indicar que a empresa reconhece e comunica publicamente a impossibilidade de fornecimento de dados quando os pedidos não são individualizados, em linha com o entendimento jurídico predominante sobre a proteção à privacidade em investigações.

Também **atende integralmente** ao **parâmetro V**, porque as informações sobre entrega de dados foram consideradas suficientes como forma de protocolo.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

Nesta categoria, a Claro obteve **estrela cheia**, pois atendeu aos dois parâmetros.

O **parâmetro I**, referente à contestação de legislação, foi **atendido**. A Claro contestou judicialmente a Lei Municipal nº 14.011/2021, que determinava o fornecimento, por operadoras de telecomunicações, de dados cadastrais de clientes residentes no município de Ponta Grossa/PR no contexto do "Programa Salve Celular". A norma previa a entrega de "lista em mídia digital,

contendo nomes, endereços, números de telefones e e-mails de seus clientes", sem base em ordem judicial. Na Ação Civil Pública nº 0024471-36.2022.8.16.0019, a Claro alegou a inconstitucionalidade formal da norma, por usurpar a competência legislativa privativa da União para dispor sobre telecomunicações, e a inconstitucionalidade material, por violar os direitos fundamentais à privacidade e à proteção de dados pessoais, conforme os incisos X e XII do art. 5º da Constituição Federal.

O **parâmetro II**, referente à contestação de pedidos abusivos, também foi **atendido.** A Claro apresentou manifestações formais contrárias a solicitações consideradas abusivas de fornecimento de dados em, ao menos, dois episódios distintos. No primeiro, no âmbito da **Ação Civil Pública nº 0024471-36.2022.8.16.0019**, como já detalhado acima, a empresa recusou-se a fornecer, sem ordem judicial, dados cadastrais como nomes, endereços, telefones e e-mails de clientes residentes em Ponta Grossa/PR, a serem utilizados em programa municipal de segurança pública. A operadora alegou se tratar de "solicitação genérica e indiscriminada, sem detalhamentos", incompatível com os direitos constitucionais à privacidade e à proteção de dados pessoais. No segundo caso, no âmbito administrativo, a empresa respondeu ao **Ofício nº 53500.324483/2022-84 da Anatel**, que transmitia solicitação da **Associação Nacional dos Bureaus de Crédito (ANBC)** para inclusão de dados da base pré-paga no Cadastro Positivo. A Claro se posicionou contrariamente ao pedido, argumentando que essa modalidade não gera faturas nem relatórios financeiros e, portanto, não se enquadra nas exigências legais que fundamentam o Cadastro Positivo, recomendando que a questão fosse previamente debatida no âmbito regulatório.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

A Claro obteve uma **estrela cheia** nesta categoria, pois atendeu aos dois parâmetros.

O **parâmetro I** foi **atendido**. A Claro apresentou manifestações públicas em eventos especializados e consultas públicas que abordam temas relacionados à privacidade e proteção de dados pessoais. Em nome próprio, a empresa participou de painéis e debates como o *"#DPO Program da Deloitte"*, o *"FutureCom 2024"*, e o *"VI Congresso de Segurança Cibernética, Proteção de Dados e Governança de IA*". Na ocasião, representantes da empresa, como sua DPO e seu Diretor de Segurança da Informação, trataram de temas como cultura de privacidade, governança de dados e uso ético da informação. Além disso, a Claro contribuiu formalmente em processos regulatórios conduzidos pela ANPD, incluindo o "*Estudo Preliminar sobre Anonimização e Pseudonimização"* e a "*Tomada de Subsídios sobre Direitos dos Titulares"*. Nesses casos, a empresa defendeu, por exemplo, a transparência nas decisões automatizadas e o entendimento ampliado da pseudonimização como mecanismo de proteção de dados.

O **parâmetro II** também foi **atendido**. Este parâmetro avalia se a empresa adotou postura proativa na identificação e mitigação de vulnerabilidades de segurança, e se comunicou, em nome próprio, os riscos associados — especialmente em contextos como o uso indevido de tecnologias de vigilância, conforme descrito no documento metodológico. A Claro apresentou

esclarecimentos formais sobre os casos de uso ilegal de ferramentas de geolocalização por parte da ABIN, detalhados no documento metodológico. Em resposta à Anatel, no âmbito do **processo administrativo nº 53500.020452/2023-38**, a empresa afirmou que "não teve qualquer conhecimento sobre a utilização, pela ABIN, ou qualquer outro ente, seja público ou privado, de Sistema de Monitoramento de localização de usuários de telecomunicações, até que as notícias se tornassem públicas", declarando ainda que "não possui contrato firmado com empresa de prestação desse tipo de serviço" e "não possui qualquer relação com os eventos".

A Claro também informou que, antes da divulgação dos fatos, implementou medidas técnicas para reforçar a segurança de sua infraestrutura de sinalização. Segundo a empresa, "no final de 2021, com objetivo de reforçar os protocolos de sinalização utilizados, a Claro adquiriu uma nova plataforma ("Mobileum"), cuja ativação completa se deu ao longo de 2022 com o monitoramento e o bloqueio de regras de firewall do protocolo SS7.

Além das medidas técnicas, a Claro relatou ações voltadas à cultura organizacional de segurança, como o programa interno de treinamentos "Conectados com o Certo", voltado à conscientização sobre segurança da informação e privacidade de dados. A empresa também participa regularmente do exercício Guardião Cibernético, promovido pelo Exército Brasileiro, com foco na segurança de infraestruturas críticas. Em 2024, promoveu o evento "Innovation Day", organizado pela sua Diretoria de Segurança da Informação, com painéis sobre prevenção a fraudes, capacitação de colaboradores contra ataques e engajamento dos clientes em práticas de segurança.

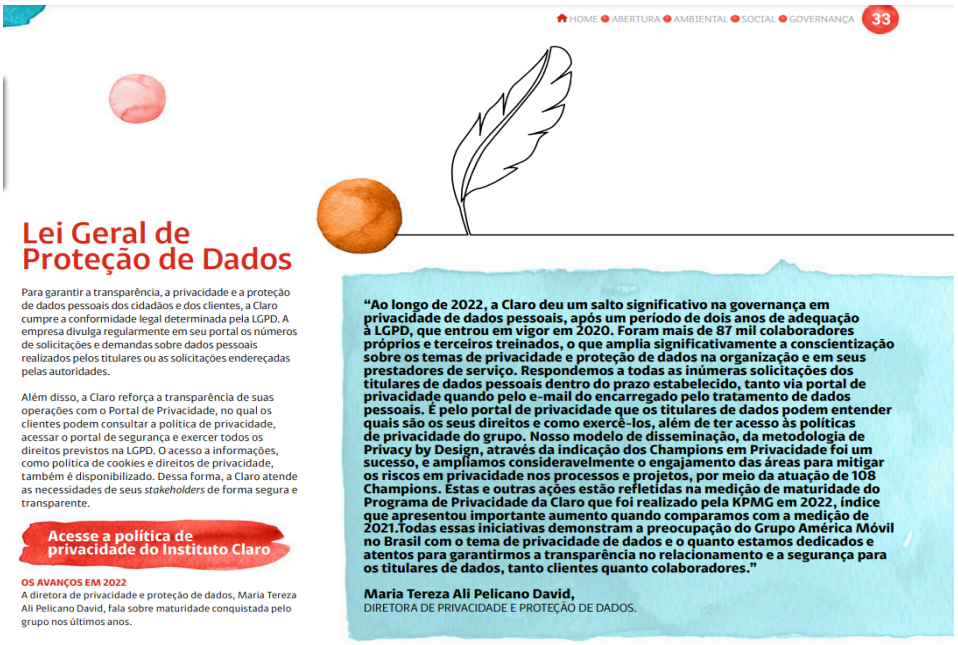
Com base nessas informações, a empresa atendeu ao critério, considerando que a empresa apresentou evidências de atuação proativa na mitigação de vulnerabilidades e ações de comunicação e conscientização em segurança da informação.

CATEGORIA 5: Relatórios de transparência e de impacto à proteção de dados

Resultado: 

Nesta categoria, a Claro **obteve 3/4 de estrela**, pois cumpriu dois parâmetros de forma completa e 2 parâmetros de forma parcial.

A Claro atende integralmente ao **parâmetro I**. A empresa publicou Relatório de Transparência/Social em seu site. A empresa publica, anualmente, desde 2014, relatórios de responsabilidade social corporativa, sendo que o último se refere ao ano de 2022. O relatório de responsabilidade social não tem a privacidade e a proteção de dados como escopo, mas dispõe de uma seção (p. 33-34) sobre a temática, que apesar de ter potencial para melhorias, contém informações relevantes.



HOME ABERTURA AMBIENTAL SOCIAL GOVERNANÇA 33

Lei Geral de Proteção de Dados

Para garantir a transparência, a privacidade e a proteção de dados pessoais dos cidadãos e dos clientes, a Claro cumpre a conformidade legal determinada pela LGPD. A empresa divulga regularmente em seu portal os números de solicitações e demandas sobre dados pessoais realizados pelos titulares ou as solicitações endereçadas pelas autoridades.

Além disso, a Claro reforça a transparência de suas operações com o Portal de Privacidade, no qual os clientes podem consultar a política de privacidade, acessar o portal de segurança e exercer todos os direitos previstos na LGPD. O acesso a informações, como política de cookies e direitos de privacidade, também é disponibilizado. Dessa forma, a Claro atende as necessidades de seus *stakeholders* de forma segura e transparente.

Acesse a política de privacidade do Instituto Claro

OS AVANÇOS EM 2022
A diretora de privacidade e proteção de dados, Maria Tereza Ali Pelicano David, fala sobre maturidade conquistada pelo grupo nos últimos anos.

"Ao longo de 2022, a Claro deu um salto significativo na governança em privacidade de dados pessoais, após um período de dois anos de adequação à LGPD, que entrou em vigor em 2020. Foram mais de 87 mil colaboradores próprios e terceiros treinados, o que amplia significativamente a conscientização sobre os temas de privacidade e proteção de dados na organização e em seus prestadores de serviço. Respondemos a todas as inúmeras solicitações dos titulares de dados pessoais dentro do prazo estabelecido, tanto via portal de privacidade quando pelo e-mail do encarregado pelo tratamento de dados pessoais. É pelo portal de privacidade que os titulares de dados podem entender quais são os seus direitos e como exercê-los, além de ter acesso às políticas de privacidade do grupo. Nosso modelo de disseminação, da metodologia de Privacy by Design, através da indicação dos Champions em Privacidade foi um sucesso, e ampliamos consideravelmente o engajamento das áreas para mitigar os riscos em privacidade nos processos e projetos, por meio da atuação de 108 Champions. Estas e outras ações estão refletidas na medição de maturidade do Programa de Privacidade da Claro que foi realizado pela KPMG em 2022, índice que apresentou importante aumento quando comparamos com a medição de 2021.Todas essas iniciativas demonstram a preocupação do Grupo América Móvil no Brasil com o tema de privacidade de dados e o quanto estamos dedicados e atentos para garantirmos a transparência no relacionamento e a segurança para os titulares de dados, tanto clientes quanto colaboradores."

Maria Tereza Ali Pelicano David,
DIRETORA DE PRIVACIDADE E PROTEÇÃO DE DADOS.

Figura 1, Relatório de Sustentabilidade, p. 33

A Claro atende integralmente ao **parâmetro II**. O Relatório pode ser facilmente acessado no Portal de Privacidade no ícone Relatório de Transparência, sendo direcionado para o Relatório de 2022, publicado em 2023.

A Claro atende integralmente ao **parâmetro III**. O relatório é publicado anualmente, desde 2014.

A Claro apresentou dados relacionados a pedidos de acesso a informações por autoridades públicas no Relatório de Sustentabilidade 2023 da América Móvil, sua controladora. O documento informa que a Claro recebeu 810.965 solicitações de dados por órgãos governamentais, das quais 97,26% foram atendidas e 2,74% não foram atendidas por descumprimento de regulamentações ou outras hipóteses. Embora o relatório forneça dados quantitativos sobre o volume de requisições e a proporção de atendimento, não apresenta informações sobre o tipo de dado solicitado (como conteúdo de comunicação ou metadados), nem sobre o número de contas afetadas. Dessa forma, o **parâmetro IV** não foi integralmente atendido.

A Claro realiza Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), conforme evidenciado em seu fluxo interno de avaliação Privacy by Design e no formulário utilizado para elaboração desses documentos. De acordo com a empresa, os relatórios têm como finalidade demonstrar que o tratamento de dados pessoais ocorre em conformidade com a legislação e com a adoção de medidas voltadas à mitigação de riscos às liberdades civis e aos direitos fundamentais dos titulares. No entanto, não foram localizados RIDPs publicados ou disponibilizados publicamente. Como a metodologia considera não apenas a elaboração, mas

também a publicidade das informações desses documentos, que pode ser feita, por exemplo, por informativos mais simples e acessíveis ao público, o **parâmetro V** é considerado parcialmente atendido.

CATEGORIA 6: Notificação do usuário

Resultado: 

Nesta categoria, a Claro obteve **estrela vazia**, pois não atendeu ao parâmetro.

A Claro não atende ao critério, pois não apresenta, em seus documentos públicos, compromisso de notificar os usuários sobre pedidos de acesso a dados. A empresa afirma que, caso receba solicitações de fornecimento de dados por autoridades, deve atendê-las para não incorrer em crime de desobediência. No entanto, o parâmetro avalia a existência de compromisso de notificação nos casos em que não há imposição legal de sigilo, o que não foi identificado.

OI

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Oi obteve **estrela cheia**, tendo atendido a todos os parâmetros.

A OI atende integralmente ao **parâmetro I**, visto que foram atendidos os sub-parâmetos (a), (b), (d) e (e).

Sub-parâmetro (a): atendido. Em seu Aviso de Privacidade, a empresa elenca extensivamente os dados coletados (vide excerto abaixo):

> Dados de Cadastro
> Nome, CPF, data de nascimento, nome da mãe
> E-mail
> Telefone residencial e móvel
> Endereço
> Dados financeiros
> Histórico de crédito ou de pagamentos
> Datas de pagamento
> Valores em aberto ou pagamentos recebidos
> Informações de fatura
> Informações do cartão de crédito ou débito e conta bancária
> Dados de uso dos produtos e serviços Oi

> Dados de tráfego: Registro das ligações efetuadas e recebidas através do serviço de telefonia fixa (STFC) e o tempo de duração
> Dados de navegação: data e hora de início e término de uma conexão à internet; duração da conexão; endereço IP e cookies
> Dados de perfil: informações sobre consumo/uso de serviços, produto contratado, região de contratação, faixa etária, preferências informadas em pesquisas

Além disso, há o documento 'Quais dados pessoais a Oi tem sobre mim e para quê?', que detalha ainda mais quais são os dados coletados.

Sub-parâmetro (b): atendido. Considerou-se suficientes as informações contidas no Aviso de Privacidade da empresa, na parte 'Como é feita a coleta de dados?':

> Existem algumas formas de coletarmos os seus dados:
>
> Diretamente com você
>
> Na aquisição de serviços e produtos em nossas lojas, sites e parceiros
>
> Na atualização de dados em nossos sites, aplicativos e outros canais de atendimento
>
> Ao responder nossas pesquisas de satisfação
>
> Automaticamente
>
> Lembra quando falamos de cookies? Então, eles são coletados quando você navega em nossos sites e aplicativos. Da mesma maneira, podemos coletar alguns dados de forma automática quando você utiliza nossos serviços. É o que acontece, por exemplo, com os dados de tráfego e dados de navegação, que, como você viu, são importantes para que possamos, dentre outras finalidades, avaliar a performance de nossos produtos/serviços e cumprir obrigações legais.
>
> De forma indireta
>
> Através de empresas parceiras com as quais você tenha um vínculo/cadastro

Sub-parâmetro (c): não atendido. Não há informações sobre dados públicos.

Sub-parâmetro (d): atendido. As informações do Aviso de Privacidade e Programa de Privacidade apresentam listagem das categorias de terceiros que fornecem dados à Oi. O Fluxo apresenta uma descrição das categorias de terceiros que recebem dados da Oi, após coleta independente da operadora.

Sub-parâmetro (e): atendido. A Oi informa, em seu Aviso de Privacidade sobre a avaliação de terceiros em relação à proteção de dados pessoais:

> Importante!
>
> Nossos fornecedores passam por um criterioso processo de seleção, que envolve fiscalização, atendimento de protocolos de segurança e avaliações de conformidade.
>
> A Oi também conta com cláusulas e documentos que asseguram a confidencialidade e o uso dos dados pessoais de acordo com a lei.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a finalidade da utilização dos dados e o tipo ou a forma de tratamento, considerou-se **atendido**, pois os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): atendido. No documento 'Quais dados pessoais a Oi tem sobre mim e para quê?', a empresa explica, de forma detalhada, quais são as funções para cada dado coletado.

Sub-parâmetro (b): atendido. Também no documento 'Quais dados pessoais a Oi tem sobre mim e para quê?', a empresa esclarece as maneiras de uso dos dados pessoais coletados.

Quanto ao **parâmetro III,** referente ao fornecimento de informações claras e completas sobre armazenamento, segurança e compartilhamento, considerou-se **atendido**, pois os sub-parâmetros (c), (d), (e), (f), (g) e (h) estavam presentes, o parâmetro (a) foi parcialmente atendido e o sub-parâmetro (b) não foi atendido.

Sub-parâmetro (a): parcialmente atendido. No seu Aviso de Privacidade, na seção 7 'Por quanto tempo os meus dados ficam armazenados?', a empresa informa os prazos de armazenamento detalhados para cada tipo de dado coletado e o local de seu armazenamento. Porém apenas indica os prazos mínimos de armazenamento.

Sub-parâmetro (b): não atendido. Isso porque, na mesma seção há apenas indicação dos prazos mínimos do armazenamento de dados, mas não há informações sobre prazo máximo de armazenamento, tampouco informações sobre apagamento de dados.

Sub-parâmetro (c): atendido. O item '7. Por quanto tempo os meus dados ficam armazenados?' indica, não exaustivamente, algumas hipóteses de retenção dos dados.

Sub-parâmetro (d): atendido. No item 9 'Os meus dados estão protegidos?', a empresa se compromete a seguir padrões de segurança e controle.

Sub-parâmetro (e): atendido. Isso porque a empresa divulga, no mesmo item acima, sobre o controle de acesso:

> Possuímos regras dispostas em Política que asseguram o controle de acesso aos sistemas e dados armazenados pela Oi. Dessa forma, suas informações, como dados cadastrais, financeiros entre outros, são acessados apenas por colaboradores devidamente autorizados e/ou por fornecedores/terceiros que possuam necessidade de acesso. Lembrando que a contratação de terceiros, além de passar por avaliações prévias de segurança e conformidade, também possuem cláusulas de confidencialidade, segurança e proteção de dados.

Sub-parâmetro (f): atendido. No item 6 'Os meus dados são compartilhados?', a empresa expõe categorias gerais de empresas com as quais podem ser compartilhados os dados.

Sub-parâmetro (g): atendido. O mesmo item acima traz informações sobre as finalidades de compartilhamento com terceiros.

Sub-parâmetro (h): atendido. Em seu Aviso de Privacidade, a Oi possui o item 8 'Onde meus dados são salvos?' que contempla o critério sobre hipóteses de transferência internacional de dados.

O **parâmetro IV**, que avalia se a empresa disponibiliza informações claras e completas acerca dos direitos dos titulares, foi considerado **atendido**, visto que os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): atendido. A Oi dispõe de uma página intitulada Conheça seus direitos na qual se dedica a expor os direitos dos titulares de dados, assim como a forma de exercê-los no âmbito da empresa. Além disso, o item 10 "Quais são os meus direitos?" de seu Aviso de Privacidade compila diversos direitos dos titulares e direciona à página supracitada.

Sub-parâmetro (b): atendido. Na página Conheça seus direitos a Oi direciona os titulares para os formulários de direitos que indica como clientes e ex-clientes podem solicitar os direitos de **(i)** confirmação de tratamento/acesso de dados; **(ii)** correção de dados; **(iii)** exclusão/anonimização de dados; **(iv)** portabilidade e compartilhamento de dados com entidades públicas e privadas; **(v)** oposição a tratamento de dados**; (vi)** revogação e informações sobre consentimento; (vii) revisão de decisões automatizadas.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado **atendido**, visto que os sub-parâmetros (a) e (b) estavam presentes.

Subparâmetro (a) e (b): atendidos. A empresa atendeu as requisições feitas por meio de sua página de Formulário de direitos e disponibilizou, no período previsto no sub-parâmetro, informações claras e completas de quais dados da solicitante são armazenados pela empresa. Além disso, a Oi informou as categorias de terceiros com as quais pode compartilhar os dados. Destaca-se, positivamente, o protocolo de segurança da Oi para a verificação da identidade do solicitante.

O **parâmetro VI**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado **atendido**. A Oi informa que em seu Aviso de privacidade que nos casos de atualização da política notificará todos os seus clientes para publicizar as mudanças. Além disso, a Oi coloca a data da última atualização de modo acessível no início da página.

> Este aviso pode mudar? Como a Oi está sempre melhorando seus serviços e produtos, esta página pode ser atualizada. Quando isso acontecer, todos os clientes serão informados. Em todo caso, sugerimos o acompanhamento periódico desta página.

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado **atendido**. A Oi disponibiliza informações claras e completas sobre privacidade e proteção de dados em diversos documentos e páginas, tais como em seu Portal de Privacidade, Aviso de Privacidade, nas iniciativas expostas na página Transparência em Privacidade e na página sobre direitos e formas de exercê-los. A título exemplificativo mencionamos o Contrato de adesão à banda larga, a Oi dispõe informações relacionadas às obrigações do controlador de dados pessoais, em acordo com a legislação nacional, no item 7, bem como, no

mesmo item, explica sua política de privacidade e proteção de dados. Assim, justifica-se a avaliação, pois a previsão em contratos constitui um dos critérios constitutivos da pontuação integral do parâmetro VII.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Oi obteve **estrela cheia**, pois cumpriu todos os parâmetros.

A Oi **atende integralmente** ao **parâmetro I**, pois ambos os sub-parâmetros foram atendidos.

Subparâmetro (a): atendido. Considerou-se atendido pois a empresa promete essa entrega por requisição no documento 'Protocolo de entrega de dados a autoridades públicas', Item 2: Análise:

> Nessa etapa identificamos quais dados estão sendo solicitados e a fundamentação legal. Na sequência, verificamos a competência do requisitante.

Subparâmetro (b): atendido. Considerou-se atendido por ter item específico sobre o assunto no documento 'Protocolo de entrega de dados a autoridades públicas', Item 'Em quais situações é preciso apresentar ordem judicial?'.

A Oi também atende integralmente ao **parâmetro II**, pois todosos sub-parâmetros foram atendidos.

Subparâmetro (a): atendido. Foi considerado atendido porque o documento 'Protocolo de Entrega de Dados a Autoridades Públicas' da Oi traz, no item 'coordenadas por estação rádio base', a informação acerca da possibilidade de compartilhamento de dados de geolocalização em tempo real:

> Como a Oi não presta mais serviço de telefonia móvel desde 2022, não há compartilhamento ou acesso a Coordenadas ERB em tempo real por autoridades públicas.

Subparâmetro (b): atendido. O Protocolo de Entrega de Dados a Autoridades Públicas da Oi especifica que os dados de geolocalização ("Coordenadas por Estação Rádio base") apenas são enviados às Autoridades Públicas no atendimento de demandas relacionadas aos crimes descritos no artigo 13-B do CPP.

Subparâmetro (c): atendido. Embora não faça referência explícita à decorrência mínima de 12 horas da ausência de manifestação judicial para divulgação dos dados de geolocalização às Autoridades Públicas, o Protocolo cita o artigo 13-B do CPP, que estabelece o prazo em seu parágrafo 4º.

A Oi **atende integralmente** ao **parâmetro III**. No documento 'Protocolo de entrega de dados a autoridades públicas', Item 'Em quais situações é preciso apresentar ordem judicial?', a empresa traz:

> registros de conexão
>
> Podem ser solicitados mediante ordem judicial de juízo competente, conforme disposto no art. 13, §5º do Marco Civil da Internet"

A Oi **atende** ao **parâmetro IV** de forma integral. No documento 'Protocolo de entrega de dados a autoridades públicas', Item 3 'retorno'

> Caso seja verificada alguma inconsistência ou não atendimento de algum requisito legal, como, por exemplo, pedido de dados genérico ou solicitações de dados excessivos, a Oi apresenta uma contestação.

Por fim, a Oi também **atende integralmente** ao **parâmetro V**, porque é possível encontrar, no documento 'Protocolo de entrega de dados a autoridades públicas' informações claras acerca da entrega de dados.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

Nesta categoria, a Oi obteve **estrela cheia**, pois atendeu aos dois parâmetros.

O **parâmetro I**, referente à contestação de legislação, foi considerado **atendido**. Realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte, e A Oi, representada pela Associação Brasileira de Concessionárias de Serviços Telefônicos (Abrafix), propôs a ADI 4906 para questionar dispositivo de Lei de Lavagem de Dinheiro (nº 12.683/2012) acerca do compartilhamento de dados cadastrais, alegando que o trecho questionado viola os direitos constitucionais à privacidade e à intimidade.

O **parâmetro II**, referente à contestação de pedidos abusivos, também foi **atendido**. Realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado de São Paulo e no portal "Jusbrasil", em ambos os casos pelos termos " Oi E sigilo E quebra" e por acórdãos publicados entre 01/01/2023 e 31/12/2023. Por exemplo, encontramos, que a Oi contestou pedido - considerado abusivo pela empresa - de quebra de dados para responsabilização por ações criminais no contexto de ofensas publicas na internet (Acórdão 1109036-53.2020.8.26.0100 - Rel. Des. César Peixoto).

CATEGORIA 4: Postura pública pró-privacidade

Resultado: ★
A Oi obteve uma **estrela cheia** nesta categoria, pois atendeu aos dois parâmetros.

O **parâmetro I** foi **atendido**. Conforme evidências apresentadas pela empresa, a empresa participou, ao longo do período avaliado, de consultas públicas da Autoridade Nacional de Proteção de Dados (ANPD), como no Guia Orientativo sobre Legítimo Interesse, em 2023. Nessa consulta, a empresa destacou a necessidade de maior proteção dos dados de crianças e adolescentes. A Oi também apontou sua contribuição no Estudo Preliminar de Anonimização e Pseudonimização, elaborado também pela ANPD, em 2024. Nesse estudo, a empresa inclusive compartilha o trecho em que contribuiu:

Não há dúvidas de que os agentes de tratamento precisam ter condições de demonstrar que as técnicas de anonimização aplicadas consideram os meios próprios e esforços razoáveis disponíveis à época, mas a exigência de um processo como o proposto pode implicar no dispêndio de recursos, como contratação de consultorias para elaboração dos cálculos, dificultando – senão inviabilizando - a adoção de uma medida que, em última instância, tende a beneficiar os titulares de dados.

1.4. Proibição de anonimização inteiramente automatizada

Dispõe o item "K" do Apêndice I: "*A anonimização não deve ser totalmente automatizada - ferramentas automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano*"

É certo que o envolvimento humano em processos de anonimização pode ser uma medida a ser recomendada para as organizações, todavia, inexiste na LGPD qualquer proibição de que o processo de anonimização seja automatizado.

Não devemos nos esquecer que os guias produzidos pela ANPD, embora sejam de extrema valia para a correta interpretação da lei, constituem ato infra legal, não podendo inovar ou contrariar a lei em razão do princípio da reserva legal.

Senão por isso, com o desenvolvimento tecnológico, podem surgir ferramentas que realizam a anonimização automatizada, o que deve ser visto como algo positivo, já que permitiria a economia de tempo e recursos pelas empresas.

A limitação acima, portanto, é desarrazoada e contraria o fundamento da LGPD de desenvolvimento tecnológico, além de estabelecer uma proibição sem qualquer respaldo legal. Por esse motivo, entendemos que o item deva ser excluído do apêndice, ou, quando muito, reescrito para deixar claro que se trata de uma simples **recomendação**, e não de uma vedação.

Ainda, a empresa apresentou seu posicionamento na mídia, como sua participação no evento Guardião Cibernético de 2023, bem como em entrevista do Chief Compliance and Privacy Officer da Oi para a Teletime, em 2023, na qual ele defende as regras estabelecidas na Lei Geral de Proteção de Dados.

O **parâmetro II** também foi **atendido**. A Oi demonstrou postura proativa na identificação e mitigação de vulnerabilidades de segurança. De acordo com as informações apresentadas pela empresa, foram adotadas diversas iniciativas para fortalecer a proteção dos dados e das comunicações dos usuários. A Oi disponibiliza, em seu portal regulatório, informações sobre suas práticas de segurança e apresenta ações específicas de reforço da proteção cibernética. Dentre as iniciativas, destaca-se o lançamento de uma ferramenta para proteção de senhas, medida que visa minimizar riscos decorrentes de credenciais vulneráveis.

Quanto à comunicação dos riscos, a empresa se posicionou publicamente, em nome próprio, sobre a importância da conduta ética na proteção de dados e participou de debates sobre segurança e proteção de dados. Além disso, foram localizados registros da participação da Oi em eventos públicos e entrevistas na mídia especializada, como a Teletime, abordando a importância de práticas robustas de segurança da informação. Essas ações contribuem para a conscientização sobre riscos relacionados a vulnerabilidades, mesmo que, no momento, não haja comprovação documental de notificações específicas aos usuários ou à Anatel sobre a exploração de falhas concretas.

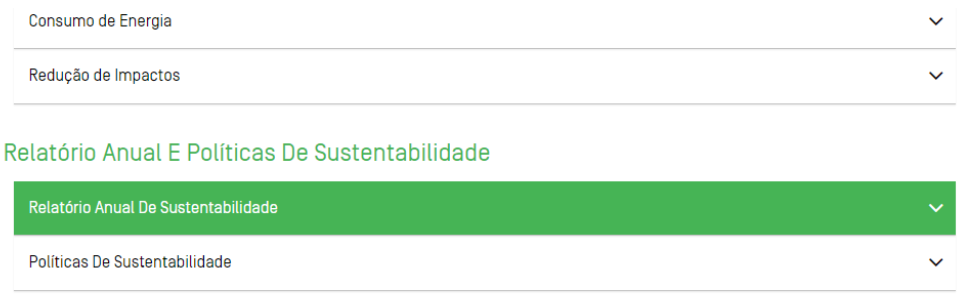
CATEGORIA 5: Relatórios de transparência e de impacto à proteção de dados

Resultado: 

Nesta categoria, a Oi **obteve estrela cheia**, pois cumpriu todos os parâmetros.

A Oi atende integralmente o **parâmetro I**. A empresa publica anualmente, desde 2011, relatórios de sustentabilidade (ESG), segundo os padrões da Global Reporting Initiative. A última edição foi publicada em agosto de 2023 e faz um balanço dos compromissos e políticas adotadas pela Oi no ano de 2022. O relatório de sustentabilidade não tem como escopo as políticas ou estatísticas de privacidade e proteção de dados, no entanto traz informações relevantes acerca da temática, em especial na subseção "Programa Oi de Privacidade" da seção 9 "O jeito Oi de cuidar das pessoas" (p. 80-84). A Oi expõe as frentes de seu Programa, que atuam em "três frentes distintas: na estrutura organizacional (Governança), na conscientização (Educação e Treinamento) e no atendimento à legislação (Processos)." (p. 80). As principais realizações na área, apresentadas no relatório são: 1) lançamento da ferramenta para gestão dos atendimento de direitos dos titulares; 2) operação do Privacy by Design; 3) reestruturação do Portal de Privacidade; 4) ações destinadas à disseminação do conhecimento sobre privacidade e IV) fortalecimento do posicionamento público da empresa pró-privacidade. Além disso, o relatório traz estatísticas sobre pedidos de acesso a dados, que serão detalhados no parâmetro IV.

A Oi atende integralmente ao **parâmetro II.** O Relatório pode ser facilmente acessado no site da empresa, na seção "ESG", subseção "Sustentabilidade" e "Relatório Anual de Sustentabilidade", conforme demonstrado abaixo:



A Oi atende integralmente ao **parâmetro III**. Desde 2011, a empresa publica relatórios de transparência e sustentabilidade.

A Oi atende integralmente ao **parâmetro IV**. A empresa publicou, no Relatório de Sustentabilidade de 2022, que em 2022 recebeu 513.321 requisições feitas por autoridades públicas para acesso a dados, referente aproximadamente 2,5 milhões de contas. A Oi detalha o tipo de dado solicitado na tabela abaixo:

Relatório de Sustentabilidade, 2022, p. 82

Além disso, a empresa informa que "apresentou contestação a aproximadamente 2.700 solicitações, com a impetração de cerca de 18 habeas corpus, em razão da manutenção de pedidos considerados ilegais." (p. 82).

CATEGORIA 6: Notificação do usuário

Resultado: ☆

Nesta categoria, a Oi obteve **estrela vazia**, pois não atendeu ao parâmetro.

A Oi não atende ao **parâmetro I**. Isso pois não localizamos nenhuma menção à possibilidade de notificação do usuário em quaisquer dos documentos analisados.

TIM

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a Tim obteve **estrela cheia**, tendo atendido a todos os parâmetros.

A Claro atende integralmente ao parâmetro I, fornecendo informações claras e completas sobre os sub-parâmetros (a), (b), (d) e (e).

Sub-parâmetro (a): atendido. Em sua Política de Privacidade, a empresa elenca extensivamente os dados coletados no item 'Que tipo de dados e com qual finalidade a TIM trata' através de uma tabela.

Sub-parâmetro (b): atendido. No mesmo item da tabela referenciada acima, a Tim traz a origem dos dados, deixando claro em que circunstâncias é feita a coleta.

Sub-parâmetro (c): não atendido. Não há qualquer referência à obtenção - ou não - de dados públicos por parte da empresa.

Sub-parâmetro (d): atendido. A empresa divulga, em sua Política de Privacidade, a lista de terceiros com quem compartilha os dados por categorias no item 'Com quem a TIM compartilha os seus Dados'.

Sub-parâmetro (e): atendido. No item 'Como a TIM coleta seus Dados Pessoais', da Política de Privacidade, a empresa destaca a necessidade de adequação de terceiros à proteção de dados no seguinte excerto:

> Além disso, quando Você utilizar Produtos operados por terceiros, parceiros da TIM, nós poderemos receber Dados desses Produtos, como seu histórico de uso ou outros Dados, conforme o caso. Ainda, para que possamos ofertar nossos Serviços e Produtos, podemos receber de empresas parceiras seus Dados, sendo certo que sempre nos preocupamos com a licitude de tais Dados. **Assim, exigimos de nossos parceiros que apenas compartilhem Dados legítimos e de procedência adequada.**

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a finalidade da utilização dos dados, considerou-se **atendido**, pois os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): atendido. Na sua *Política de Privacidade*, na seção 'Que tipo de dados e com qual finalidade a TIM trata', a empresa explica, de forma detalhada, quais são as funções para cada dado coletado.

Sub-parâmetro (b): atendido. Na mesma seção, a empresa indiretamente esclarece as maneiras de uso dos dados pessoais coletados

Quanto ao **parâmetro III,** referente ao fornecimento de informações claras e completas sobre armazenamento, segurança e compartilhamento, considerou-se que **atendido**, pois os sub-parâmetros (a), (b), (c), (d), (e), (f), (g) e (h) foram atendidos.

Sub-parâmetro (a): atendido. Na política 'Onde e por quanto tempo a Tim armazena seus dados', a empresa informa os prazos de armazenamento detalhados para cada tipo de dado coletado e o local de seu armazenamento. Ressalta-se que a empresa é categórica quanto ao prazo de

armazenamento, dando a entender que se tratam de prazos exatos - nem máximos, nem mínimos - e quanto ao local também, afirmando haver armazenamento em locais próprios da Tim ou em servidores terceiros definidos.

Sub-parâmetro (b): **atendido.** No mesmo item apontado acima, infere-se que os dados são apagados após o decurso do prazo apontado.

Sub-parâmetro (c): atendido. No mesmo item apontado acima, a empresa elenca as hipóteses de retenção dos dados:

> Para determinar o período de retenção adequado para os Dados Pessoais, além do prazo de prescrição previsto em lei, consideramos outros critérios, como a quantidade, a natureza e a sensibilidade destes Dados, o risco potencial de danos decorrentes do uso não autorizado ou da divulgação de seus Dados Pessoais, a finalidade de tratamento destes dados, e se podemos alcançar os propósitos almejados por outros meios, e os requisitos legais aplicáveis, dentre outros.

Sub-parâmetro (d): atendido. No documento 'Política de Segurança da Informação e Segurança Cibernética', a empresa detalha quais são as práticas de segurança que a Tim adota.

Sub-parâmetro (e): atendido. A empresa divulga em seu 'Contrato de Prestação de Serviço Móvel Pessoal Pré Pago' a cláusula 11.2 que traz o seguinte texto:

> 11.2 A TIM garante que as informações tratadas no âmbito do Contrato, especialmente os dados pessoais, estarão armazenadas em ambiente seguro, em servidores localizados no Brasil ou no exterior, observado o estado da técnica disponível, valendo se de políticas e tecnologias de segurança como criptografia, controles de acesso e certificações de segurança específicos, e somente poderão ser acessadas por pessoas qualificadas e autorizadas pela TIM.

Além disso, em sua *Política de Privacidade*, na seção 'Quais são as nossas responsabilidades e como a TIM protege seus dados', a empresa afirma aplicar o controle de acesso.

Sub-parâmetro (f): atendido. Na seção 'Com quem a TIM compartilha os seus dados', em sua *Política de Privacidade*, a empresa expõe categorias gerais de empresas com as quais podem ser compartilhados os dados.

Sub-parâmetro (g): atendido. Na mesma seção acima, a empresa explica detalhadamente a finalidade do compartilhamento dos dados.

Sub-parâmetro (h): atendido. No documento 'Onde e por quanto tempo a TIM armazena seus dados' possui um item dedicado às Transferências Internacionais, em que também esclarece as hipóteses de transferência.

O **parâmetro IV**, que avalia se a empresa disponibiliza informações claras e completas acerca dos direitos dos titulares, foi considerado **atendido**. Os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): atendido. A Tim atende integralmente o subparâmetro a. No item 7 "Quais são os direitos dos Titulares de Dados e como exercê-los" (p. 16-18) de sua Política de Privacidade, a Tim expõe informações sobre direitos e como exercê-los.

Direito	Conceito
Direito de confirmar a existência de tratamento dos seus dados e de acessá-los	Permissão para que Você possa verificar se Tratamos Dados Pessoais seus e requisitar uma cópia dos Dados Pessoais que nós temos sobre Você.
Direito de retificação	Este direito permite que Você, a qualquer momento, solicite a correção dos seus Dados Pessoais, caso identifique que alguns deles estão incorretos, inexatos ou desatualizados.
Direito de oposição	A lei autoriza o Tratamento de Dados Pessoais mesmo sem o seu consentimento ou um contrato conosco. Nesse caso, é preciso demonstrar que há motivos legítimos para tratar seus Dados, como, por exemplo, prevenir fraudes ou melhorar nossa comunicação com Você. Caso você não concorde com esse Tratamento, poderá se opor a ele, solicitando a interrupção.

Figura 1, Política de Privacidade, p. 16

Direito de solicitar anonimização, bloqueio ou eliminação	Este direito permite que Você nos peça para (a) anonimizar seus dados, de forma a que eles não possam mais ser relacionados a Você e, portanto, deixem de ser Dados Pessoais; (b) bloquear seus Dados, suspendendo temporariamente a possibilidade de Tratarmos seus Dados; (c) eliminar seus Dados, caso em que apagaremos todos os seus Dados sem possibilidade de reversão, salvo os casos previstos em lei.
Direito à portabilidade	Você tem o direito de solicitar, mediante requisição expressa, que a TIM forneça a Você, ou a terceiros que Você escolher, os seus Dados Pessoais em formato estruturado e interoperável. Da mesma forma, Você pode pedir que outras empresas enviem à TIM seus Dados Pessoais para facilitar a contratação dos nossos Serviços, por exemplo.
Direito de retirar o seu consentimento	Você tem o direito de retirar o seu consentimento em relação às atividades de Tratamento que se baseiam no consentimento. No entanto, isso não afetará a legalidade de qualquer Tratamento realizado anteriormente. Se Você retirar o seu consentimento, talvez não possamos fornecer determinados Serviços, mas iremos avisá-lo quando isso ocorrer.
Direito à informação sobre uso compartilhado de Dados	Manteremos esta política e nossa lista de parceiros com que compartilhamos os Dados sempre atualizada. Em todo caso, se Você tiver dúvidas ou quiser maiores detalhes, Você tem o direito de nos solicitar essas informações.
Direito de não fornecer o seu consentimento	O seu consentimento, quando necessário, deve ser livre e informado. Portanto, sempre que pedirmos seu consentimento, Você será livre para negá-lo – ainda que, nesses casos, seja possível que tenhamos que limitar nossos Serviços, caso estes dependam do seu consentimento.

Figura 2, Política de Privacidade, p. 17

Sub-parâmetro (b): atendido. Em sua Central de Privacidade, a Tim disponibiliza, na pergunta "Quais são os Direitos dos Titulares", canal de atendimento para o exercício de direitos.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado **atendido**, pois os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a) e (b): atendidos. A empresa atendeu as requisições feitas por meio de formulário disponível em sua Central de privacidade e disponibilizou, imediatamente, confirmação de

tratamento de dados do solicitante e, no período previsto no subparâmetro, disponibilizou informações claras e completas de quais dados da solicitante são armazenados pela empresa.

O **parâmetro VI**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado **atendido**. No item 11 "Como e quando esta Política pode ser alterada?", de sua Política de Privacidade, a Tim informa que poderá alterar a política, mas limita a notificação aos clientes apenas em caso de alterações relevantes. Em suas palavras:

> Como estamos sempre buscando melhorar nossos Serviços e oferecendo novas funcionalidades, essa Política de Privacidade pode passar por atualizações.Fique tranquilo, caso sejam feitas alterações relevantes, nós informaremos a você, sem prejuízo de você verificar a versão mais atual em nosso Site. (Política de Privacidade, p. 22)

Entendemos que a política estabelece que os usuários serão notificados em caso de alterações relevantes atende ao critério. Considerando que notificar todas as mudanças, independentemente de sua relevância, pode gerar um efeito contrário ao desejado — fazendo com que os usuários deixem de distinguir o que realmente importa —, a exigência de aviso apenas para mudanças significativas parece razoável. No entanto, consideramos uma boa prática que o critério de relevância seja esclarecido dentro da própria política (o que é uma alteração relevante?), evitando qualquer ambiguidade.

Além disso, como reforço de seu compromisso institucional com a transparência no tratamento de dados, destaca-se também o plano de comunicação executado durante o processo de migração de clientes da Oi, submetido à Anatel. Embora não se trate de notificações relativas a pedidos de autoridades, o plano contempla mensagens prévias aos usuários por diferentes canais (SMS, e-mail e portal online), com informações claras sobre os impactos da migração e o tratamento de seus dados pessoais, conforme exigências da LGPD e da regulação setorial. A atuação demonstra um padrão relevante de boas práticas comunicacionais com os titulares, que contribui para qualificar o atendimento ao parâmetro.

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado **atendido**. A Tim disponibiliza informações completas e claras, de forma acessível, em sua Central de privacidade, em diversas páginas e documentos, como as suas Política de privacidade, contendo suas Política de dados, Política de segurança da informação e segurança cibernética e Política de Armazenamento de dados. Além disso, conta com seção de "Dados" (item 11) no seu Contrato de Prestação de Serviço de Telefonia Móvel (Pós pago).

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Tim **obteve estrela cheia**, pois cumpriu todos os parâmetros.

A Tim **atende integralmente** ao **parâmetro I**, pois os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): atendido. Em seu documento 'Como é realizado o compartilhamento de dados pessoais em caso de investigação?', a empresa detalha como o compartilhamento por requisição ocorre:

> Neste sentido, previamente ao fornecimento dos dados pessoais solicitados, verificamos se há competência jurisdicional ou administrativa, visando assim validar se o juízo ou o órgão público requisitante possui competência e legitimidade que justifique o cumprimento da medida.

Sub-parâmetro (b): atendido. No mesmo documento, a empresa fala sobre o compartilhamento por ordem judicial:

> Uma das possibilidades desse compartilhamento é para cumprimento de ordem judicial, cumprimento de pedido extrajudicial (encaminhado pela polícia judiciária ou Ministério Público) e requisição de autoridade administrativa competente (por exemplo, uma delegacia ou uma agência governamental), direcionada à TIM, solicitando o fornecimento de dados pessoais de cliente TIM, em cumprimento à legislação específica e vigente.
>
> (...)
>
> Alguns exemplos mais comuns que observamos aqui na empresa incluem:
>
> I. Solicitação de dados sobre número de telefone para investigações criminais e ações cíveis;
>
> II. Solicitação de dados cadastrais, mediante ordem judicial ou de autoridade administrativa, ou autoridades policiais e Ministério Público;
>
> III. Solicitação de registros de conexão, mediante ordem judicial;
>
> IV. Localização de Estação Rádio Base (antena telefônica, mediante ordem judicial;
>
> V. Conteúdo de comunicações privadas, mediante ordem judicial.

A Tim **atende integralmente** ao **parâmetro II,** pois os sub-parâmetros (a), (b) e (c) foram atendidos.

Subparâmetros (a), (b) e (c): atendidos. A empresa fornece as informações em seu documento 'Como é realizado o compartilhamento de dados pessoais em caso de investigação?', no seguinte excerto:

> Por fim, indicamos que dados sobre geolocalização do aparelho não são compartilhados com terceiros para fins de realização de investigação. Contudo, dados de localização de estações rádio base utilizadas por um aparelho, em tempo real ou pretérito, podem ser fornecidas a partir de ordem judicial, salvo para casos de prevenção e repressão dos crimes relacionados ao tráfico de pessoas, hipótese do artigo 13-B do Código de Processo Penal, em que os dados de localização poderão ser requisitados por membro do Ministério Público ou o delegado de polícia.

A Tim também **atende integralmente** ao **parâmetro III**. No documento 'Como é realizado o compartilhamento de dados pessoais em caso de investigação?' a Tim afirma que os registro de conexão serão entregues apenas mediante ordem judicial:

> III. Solicitação de registros de conexão, mediante ordem judicial;

O **parâmetro IV** também é **integralmente atingido**. No documento 'Como é realizado o compartilhamento de dados pessoais em caso de investigação, cumprimentos de ordens judiciais ou administrativas?' a empresa descreve a análise quanto à proporcionalidade e razoabilidade da medida e explicita diretamente sobre a recusa ou contestação a ordens genéricas:

> Além disso, é feita uma análise da proporcionalidade daquela solicitação, ou seja, se a decisão se encontra dentro dos critérios de proporcionalidade e razoabilidade exigidos pela legislação brasileira, em especial o Código de Processo Civil (art. 8º) e a Constituição Federal, sendo contestados ou recusados quaisquer pedidos ou ordens genéricas.

Por fim, a Tim **atende integralmente** ao **parâmetro V**. É possível encontrar o documento 'Como é realizado o compartilhamento de dados pessoais em caso de investigação?' com facilidade e com informações simples e estruturadas acerca de protocolo de entrega de dados.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

Nesta categoria, a Tim obteve **estrela cheia**, pois atendeu aos dois parâmetros.

O **parâmetro I**, referente à contestação de legislação, foi considerado **atendido**. A TIM contestou judicialmente legislações e a ausência de legislações que considera violar a privacidade de usuários. No âmbito da ADPF 1.143, em trâmite no Supremo Tribunal Federal, participou por meio da Conexis, como amicus curiae, manifestando-se contra a ausência de regulamentação sobre o uso de ferramentas de monitoramento remoto por órgãos estatais. A empresa, por meio da entidade, argumentou que essas práticas são desproporcionais e violam os direitos fundamentais à privacidade, intimidade e sigilo das comunicações, previstos nos incisos X e XII do art. 5º da Constituição.

Além disso, na Ação Civil Pública nº 0024471-36.2022.8.16.0019, a TIM impugnou a Lei Municipal nº 14.011/2021, que previa a entrega, sem ordem judicial, de dados cadastrais de clientes do município de Ponta Grossa/PR. A empresa argumentou que a norma era inconstitucional por violar a competência privativa da União para legislar sobre telecomunicações e por afrontar os direitos fundamentais à privacidade e à proteção de dados pessoais. Sustentou também que a exigência de compartilhamento massivo de dados sem respaldo judicial compromete princípios

como o da legalidade e da proporcionalidade, impondo às operadoras obrigações que extrapolam suas competências legais e operacionais.

O **parâmetro II**, referente à contestação de pedidos abusivos, também foi **atendido**. A TIM atendeu ao parâmetro ao apresentar manifestações formais contrárias a solicitações de acesso a dados que considerou abusivas. No âmbito da Ação Civil Pública nº 0024471-36.2022.8.16.0019, como já explicitado acima, a empresa recusou-se a fornecer, sem ordem judicial, dados cadastrais de clientes do município de Ponta Grossa/PR, exigidos por legislação local com o objetivo de implementar um programa municipal de segurança pública. A empresa argumentou que a norma violava direitos fundamentais à privacidade e proteção de dados, além de extrapolar a competência legislativa municipal. Além disso, no âmbito administrativo, a TIM respondeu ao Ofício nº 53500.324483/2022-84 da Anatel, que veiculava solicitação da Associação Nacional dos Bureaus de Crédito (ANBC) para o compartilhamento de dados de usuários de linhas pré-pagas no Cadastro Positivo. Em sua manifestação, a empresa se posicionou de forma contrária ao pedido, sustentando que o fornecimento desses dados não atendia aos princípios da finalidade, adequação e necessidade previstos na LGPD, tampouco à finalidade legal do Cadastro Positivo, já que não há, na modalidade pré-paga, obrigações de pagamento que caracterizem adimplemento ou inadimplemento. A posição da TIM foi posteriormente respaldada por parecer jurídico da Procuradoria Federal Especializada junto à Anatel, que concluiu pela impossibilidade jurídica do compartilhamento desses dados.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

A Tim obteve **3/4 de estrela** nesta categoria, pois atendeu integralmente somente ao parâmetro I.

O **parâmetro I** foi **atendido**. A empresa tem se posicionado publicamente, em nome próprio, em fóruns técnicos, consultas públicas e tomadas de subsídios, com contribuições diretas que demonstram compromisso com a proteção de dados pessoais e a promoção de boas práticas regulatórias no setor. Destacam-se suas manifestações junto à Anatel sobre governança de dados, anonimização e pseudonimização, proteção em transferências internacionais, papel do encarregado, bem como sua participação ativa em discussões sobre o uso ético e seguro da inteligência artificial. Nessas ocasiões, a TIM defendeu concretamente a adoção de normas e abordagens regulatórias que garantam maior segurança jurídica, transparência e respeito aos direitos dos titulares, alinhando-se às diretrizes da LGPD e às melhores práticas internacionais, como o AI Act europeu e as recomendações da OCDE. Essas iniciativas evidenciam uma postura pública ativa em prol do fortalecimento da cultura de privacidade no Brasil.

O **parâmetro II** foi **parcialmente atendido**. A empresa demonstrou ações relevantes relacionadas à proteção de sua infraestrutura e à discussão pública sobre riscos associados à exploração de vulnerabilidades técnicas no contexto da regulação de ferramentas de intrusão remota por agentes estatais. Por exemplo, em resposta à tomada de subsídios da Anatel sobre o Regulamento de Incidentes de Segurança Cibernética, a TIM defendeu a adoção de critérios objetivos, claros e proporcionais para reporte de incidentes, bem como maior segurança jurídica

na definição de responsabilidades, contribuindo para a construção de um ambiente regulatório mais alinhado à proteção dos usuários.

Apesar disso, não foram identificadas manifestações públicas em nome próprio que demonstrem uma comunicação proativa com os usuários ou autoridades sobre riscos concretos associados à exploração de vulnerabilidades específicas, como aquelas investigadas nos casos citados no documento metodológico, inclusive no contexto de possíveis interceptações ilegais. Diante disso, a nota foi ajustada para refletir o avanço institucional relevante, mas com margem para maior transparência e engajamento direto com o público afetado.

CATEGORIA 5: Relatórios de transparência e de impacto à proteção de dados

Resultado: 

Nesta categoria, a Tim **obteve 3/4 de estrela**, pois cumpriu três parâmetros de forma integral e cumpriu 2 parâmetros de forma parcial.

A Tim atende integralmente o **parâmetro I**. A empresa publica anualmente, desde 2013, relatórios de sustentabilidade, sendo que o último foi publicado em 2022. O relatório de sustentabilidade (ESG) não tem a privacidade e a proteção de dados como escopo, mas dispõe de uma seção (p. 72-77) sobre a temática, que apesar de ter potencial para melhorias, contém informações relevantes para a transparência de suas políticas e atuações.
A Tim atende integralmente ao **parâmetro II**. O Relatório pode ser facilmente acessado a partir da página inicial > quem somos > sustentabilidade > relatórios ESG.

A Tim atende integralmente ao **parâmetro III**. O relatório é publicado anualmente desde 2013 e as suas versões anteriores são facilmente acessíveis. Ressaltamos que o relatório sobre 2023 ainda não foi publicado e salientamos a importância em fazê-lo.

A Tim atende parcialmente ao **parâmetro IV**. A empresa publicou, no seu último relatório ESG, que em 2023 houve “mais de 1,9 milhão de solicitações foram feitas pela Justiça à TIM para quebra de privacidade no último ano. Todas foram concedidas.” (p. 88). A empresa cumpre o subparâmetro “b”, pois discrimina os tipos de pedidos conforme demonstrado na tabela abaixo. No entanto, a empresa não apresenta informações sobre o número de contas afetadas e, portanto, não atende ao critério “c”.

Solicitações judiciais de quebra de privacidade por tipo (milhares)

	2021	2022	2023
Interceptações telefônicas	325	267	265
Dados cadastrais	397	403	541
Extratos telefônicos	839	886	1.137
Total	**1.561**	**1.556**	**1.943**

Figura 3, Relatório ESG 2023, p. 88.

A empresa demonstrou que elabora Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs), conforme previsto na LGPD. Entretanto, os relatórios não são disponibilizados publicamente em sua forma completa. Em vez disso, a TIM adota uma estratégia de comunicação com os titulares por meio de documentos chamados de "Informativas de Privacidade", nos quais são extraídas e publicizadas informações relevantes oriundas dos RIPDs. Essas informativas contêm explicações claras sobre a finalidade do tratamento, os dados pessoais envolvidos, as bases legais utilizadas e o compartilhamento com terceiros, como observado nas parcerias com Zé Delivery e Descomplica.

Apesar do esforço de traduzir os aspectos centrais do RIPD para uma linguagem acessível, o vínculo entre essas informativas e os respectivos relatórios de impacto não está explicitado nesses documentos. Assim, embora haja um avanço importante em termos de transparência e prestação de contas, ainda há espaço para aprimoramento no sentido de deixar claro ao titular que as informações derivam diretamente dos RIPDs. Diante disso, o **parâmetro V** foi considerado parcialmente atendido.

CATEGORIA 6: Notificação do usuário

Resultado: ★

Nesta categoria, a Tim obteve **estrela cheia**, tendo atendido ao parâmetro.

A TIM atende integralmente ao **parâmetro I.** A empresa implementou uma política formal de notificação de titulares de dados em casos de requisição de informações por autoridades públicas, prática inédita entre operadoras avaliadas até o momento. As contribuições enviadas demonstram que, sempre que legalmente possível e em situações não cobertas por sigilo judicial, a TIM comunica os usuários afetados sobre o compartilhamento de seus dados, apresentando inclusive evidências documentais de notificações reais enviadas após o atendimento a ofícios administrativos.

VIVO

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 
Nesta categoria, a Vivo obteve **estrela cheia**, tendo atendido a todos os parâmetros.

A Vivo **atende** ao **parâmetro** I, visto que os sub-parâmetros (a), (b), (d) e (e) foram atendidos.

Sub-parâmetro (a): atendido. Em sua Política de Privacidade, a Vivo traz as informações sobre quais dados são coletados de forma detalhada no item 6 'Como e quais dados coletamos?'.

Sub-parâmetro (b): atendido. No mesmo item acima, a empresa informa as situações de coleta.

Sub-parâmetro (c): não atendido. Não há menção em documentos da Vivo sobre a possibilidade ou não de coleta de dados disponíveis publicamente.

Sub-parâmetro (d): atendido. A empresa divulga, em sua Política de Privacidade, a lista de terceiros com quem compartilha os dados por categorias, no item 9 'Com quem a Vivo compartilha os seus dados?'.

Sub-parâmetro (e): atendido. No mesmo item acima, a empresa especifica o seguinte:

> Fique tranquilo, pois a Vivo atua de forma criteriosa na seleção dos seus parceiros e fornecedores. Além disso, exige contratualmente que esses atuem de forma segura e adotem medidas técnicas de segurança para garantir o cumprimento da legislação aplicável. E não apenas isso, fornecemos instruções e verificamos se o terceiro implementou boas práticas, sempre com o propósito de manter os seus dados pessoais em segurança.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a finalidade da utilização dos dados, considerou-se **atendido**, pois os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetros (a) e (b): atendidos. Ambos os critérios foram contemplados no item 7 'Como tratamos os seus dados e com qual finalidade?' na Política de Privacidade.

Quanto ao **parâmetro III,** referente ao fornecimento de informações claras e completas sobre armazenamento, segurança e compartilhamento, considerou-se que foi **atendido**, pois todos os sub-parâmetros foram atendidos.

Sub-parâmetro (a): atendido. Na Política de Privacidade, no item 14 'Por quanto tempo manteremos os seus dados?', a empresa informa os prazos de armazenamento detalhados para cada tipo de dado coletado e o local de seu armazenamento. Ressalta-se que a empresa é categórica quanto ao prazo de armazenamento, dando a entender que se tratam de prazos exatos - nem máximos, nem mínimos.

Sub-parâmetro (b): **atendido.** Isso porque, no mesmo trecho apontado acima, infere-se que os dados são apagados após o decurso do prazo apontado.

Sub-parâmetro (c): atendido. Na Política de Privacidade, no mesmo item referenciado acima, há as hipóteses de retenção dos dados.

Sub-parâmetro (d): atendido. No mesmo documento, a empresa se compromete a seguir padrões de segurança e controle, no item 8 'Como os meus dados são protegidos?'.

Sub-parâmetro (e): atendido. No mesmo item, há informações sobre controles de acesso.

Sub-parâmetro (f): atendido. No item 9 'Com quem a Vivo compartilha seus dados?', a empresa expõe categorias gerais de empresas com as quais podem ser compartilhados os dados.

Sub-parâmetro (g): atendido. No mesmo item acima, são citadas as finalidades de compartilhamento.

Sub-parâmetro (h): atendido. Em sua Política de Privacidade, a Vivo possui um item destinado à transferência internacional de dados, o item 10 'A transferência internacional dos seus dados'.

O **parâmetro IV**, que avalia se a empresa disponibiliza informações claras e completas acerca dos direitos dos titulares, foi considerado **atendido**. Os sub-parâmetros (a) e (b) foram atendidos.

Subparâmetro (a): atendido. No item 15 "Quais são os meus direitos como Titular e como posso fazer para exercê-los?" de sua Política de Privacidade e Proteção de Dados, (p. 17-19) a Vivo apresenta, de forma didática, os direitos dos titulares de dados conforme a LGPD e como exercê-los.

Subparâmetro (b): atendido . Em seu Centro de Privacidade, a Vivo reúne canais de exercícios para o exercício dos direitos. Para cada direito listado há um meio adequado para o seu exercício, por exemplo: 1) para acesso e consulta de dados pessoais armazenados pela empresa, a Vivo disponibiliza canal de atendimento para clientes e formulários para não clientes; 2) para atualização ou correção de dados pessoais, o titular deve usar o aplicativo Vivo ou o canal de atendimento telefônico; 3) a revogação da permissão de contato da Vivo e de parceiros deve ser feita por SMS. Por fim, para outras dúvidas e/ou dificuldades de contato pelas vias recomendadas, a Vivo disponibiliza um formulário para ser enviado ao e-mail dpo.br@telefonica.com.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado **atendido**. Os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetros (a) e (b): atendidos. A empresa possui portal de acesso a direitos dos titulares para o acesso aos dados armazenados pela Vivo e para o exercício de direitos correlatos.

A empresa atendeu às requisições feitas por meio de sua Central de Privacidade e disponibilizou, imediatamente e sem necessidade de pedido, informações claras e completas de quais dados da solicitante são armazenados pela empresa. Destaca-se, positivamente, o protocolo de segurança da Vivo para a verificação da identidade do solicitante.

O **parâmetro VI**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado **atendido**. A Vivo trata sobre a possibilidade de atualização das suas políticas de privacidade na sua Política de privacidade. A empresa promete notificar seus clientes apenas em casos de "alterações relevantes". Por essa razão, consideramos que o critério foi atendido. Nas palavras da empresa:

> 18. ATUALIZAÇÕES
>
> A Vivo tem o compromisso com a transparência e com o tratamento responsável dos seus dados. Por essa razão, esta Política poderá ser revisada a qualquer tempo e sem prévio aviso, levando-se em consideração a legislação aplicável e as atualizações dos nossos Produtos e Serviços. Mas não se preocupe, Você poderá consultar a versão atualizada em nosso Centro de Transparência e Privacidade. Caso as alterações sejam relevantes, Você será avisado. (Política de privacidade, p. 20)

Entendemos que a política estabelece que os usuários serão notificados em caso de alterações relevantes atende ao critério. Considerando que notificar todas as mudanças, independentemente de sua relevância, pode gerar um efeito contrário ao desejado—fazendo com que os usuários deixem de distinguir o que realmente importa—, a exigência de aviso apenas para mudanças significativas parece razoável. No entanto, consideramos uma boa prática que o critério de relevância seja esclarecido dentro da própria política (o que é uma alteração relevante?), evitando qualquer ambiguidade.

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado **parcialmente atendido**.A Vivo dispõe de informações relevantes, completas e claras sobre privacidade e dados, tais como a Política de Privacidade e Proteção de Dados de Clientes e Titulares, página sobre Segurança da Informação e Confidencialidade de Dados,Tratamento dos dados; canal para exercício dos direitos e página sobre protocolo de resposta a solicitações de autoridade. No entanto, a pesquisa encontrou dificuldades de acessar os contratos de prestação de serviços de banda larga fixa e telefonia móvel na página de contratos e regulamentos do site da empresa. Acreditamos que o acesso ao contrato é condição inafastável para o exercício de direitos do consumidor e é dever das empresas disponibilizá-los de modo acessível ao público. Assim, considerando que não tivemos acesso ao contrato avaliamos que a empresa não cumpre os parâmetros em sua integralidade.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 
Nesta categoria, a Vivo obteve **3/4 de estrela**, tendo atendido integralmente os parâmetros I, III, e V.

A Vivo atende **integralmente** ao **parâmetro I**.

Subparâmetro (a): atendido. Em seu documento 'Protocolo de entrega de dados à Autoridades', a empresa informa sobre as situações em que compartilha dados com o Setor Público. Especifica no item 'Informações fornecidas' sobre os compartilhamentos através de requisição, se comprometendo a verificar os requisitos legais para a entrega.

Sub-parâmetro (b): atendido. No mesmo documento, a empresa especifica no item 'Leis que amparam' uma lista de leis para a entrega de dados, o que foi considerado bastante informativo e claro.

O **parâmetro II não é atendido**, uma vez que não foi encontrado qualquer documento sobre o assunto referente a dados de geolocalização.

A Vivo **atende** ao **parâmetro III**. Em sua Política de privacidade, Item 14 'Por quanto tempo manteremos os seus dados?'

> Os registros de conexão somente serão disponibilizados pela Vivo associados a dados pessoais, mediante ordem judicial, nos termos da lei

O **parâmetro IV** é **parcialmente atendido**, uma vez que a Vivo não fala diretamente dos pedidos genéricos, porém afirma que a entrega de dados não ocorre se o pedido não cumprir os requisitos legais.

Por fim, a Vivo **atende integralmente** ao **parâmetro V**, porque é possível encontrar o documento '=Protocolo de entrega de dados a Autoridades' com facilidade.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 
Nesta categoria, a Vivo obteve **estrela cheia**, pois atendeu aos dois parâmetros.

O **parâmetro I**, referente à contestação de legislação, foi **atendido**. Realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte, e a Vivo, representada pela Associação Brasileira de Concessionárias de Serviços Telefônicos (Abrafix), propôs a ADI 4906 para questionar dispositivo de Lei de Lavagem de Dinheiro (nº 12.683/2012) acerca do compartilhamento de dados

cadastrais, alegando que o trecho questionado viola os direitos constitucionais à privacidade e à intimidade.

O **parâmetro II**, referente à contestação de pedidos abusivos, também foi considerado **atendido**. Realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado de São Paulo e no portal "Jusbrasil", em ambos os casos pelos termos "Vivo E sigilo E quebra" e por acórdãos publicados entre 01/01/2023 e 31/12/2023. Encontramos processo no qual a Vivo contestou pedido em que a autora exigia a gravação de uma chamada telefônica na qual teria sofrido golpe financeiro (Acórdão Apelação Cível nº 1006531-95.2021.8.26.0278 Rel. Caio Marcelo Mendes de Oliveira)

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

A Vivo obteve **3/4 de estrela** nesta categoria, pois atendeu integralmente somente ao parâmetro I.

O **parâmetro I** foi **atendido**. Conforme evidências trazidas pela empresa, considerou-se que a empresa atingiu plenamente o parâmetro. A Vivo destacou diversas consultas públicas nas quais contribuiu, seja por meio individuas participações ocorreram através da plataforma "Participa Mais Brasil", ao longo de 2023 e de 2024. Como na Tomada de Subsídio sobre Inteligência Artificial e Revisão de Decisões Automatizadas da Autoridade Nacional de Proteção de Dados, em 2024. Além disso, a empresa destacou a fala do CEO da Vivo, em agosto de 2024, à Rádio CBN, em que cita as preocupações sobre a cibersegurança na era da digitalização.
A empresa, inclusive, mandou na íntegra sua contribuição para a Autoridade Nacional de Proteção de Dados, na Tomada de Subsídios sobre Inteligência Artificial e Revisão de Decisões Automatizadas.

O **parâmetro II** foi considerado **parcialmente atendido**. Em relação ao item (i) identificar e mitigar suas vulnerabilidades de segurança, a empresa demonstrou ações relevantes e contínuas. A justificativa apresentada cita sua participação no Exercício Guardião Cibernético 6.0, coordenado pelo Comando de Defesa Cibernética do Exército Brasileiro, além de envolvimento em eventos especializados como o Cyber Security Summit Brasil. A Vivo também afirmou realizar testes periódicos, com certificações externas, voltados à detecção e correção de falhas. Esses elementos indicam a existência de práticas estruturadas para prevenção e resposta a riscos de segurança, configurando o atendimento a esse subitem.

Quanto ao item (ii) projeção e comunicação dos riscos associados à exploração de vulnerabilidades, incluindo notificações a usuários e órgãos reguladores, a empresa apresentou evidências de participação em consultas públicas e interações formais com a Anatel. No entanto, declara, no processo regulatório, não ter conhecimento de que suas vulnerabilidades tenham sido exploradas por terceiros, apesar de haver indícios amplamente divulgados e de conhecimento público sobre o uso de spywares no Brasil, conforme descrito em nosso documento metodológico. Essa contradição levanta dúvidas sobre a efetividade dos seus mecanismos internos de monitoramento e sobre sua disposição para projetar riscos relevantes

de forma transparente. Assim, este subitem não foi atendido. Dessa forma, a avaliação foi classificada como parcialmente atendido.

CATEGORIA 5: Relatórios de transparência e de impacto à proteção de dados

Resultado: 

Nesta categoria, a Vivo obteve **3/4 de estrela**, tendo atendido integralmente os parâmetros I, II e III.

A Vivo atende integralmente o **parâmetro I**. A empresa publica, anualmente, relatórios de sustentabilidade. Apesar de o relatório de sustentabilidade não ter a privacidade e proteção de dados como escopo, tais documentos apresentam ações e estatísticas relevantes para as temáticas. Por exemplo, no relatório de 2022, cita iniciativas na área de privacidade e proteção de dados (p. 71-77), tais como: 1) criação da Política de Privacidade para Colaboradores; 2) implementação do Comitê de Privacidade; 3) adaptação da Política de Privacidade; 4) participação na elaboração do Código de Melhores Práticas de Proteção de Dados para o Setor de Telecomunicações no Brasil; 5) participação na agenda pública de discussões (contribuições à ANPD etc); 6) Workshops.

Relatório de Sustentabilidade de 2022, p. 75.

A Vivo atende integralmente ao parâmetro II. Os seus relatório podem ser facilmente acessados no Centro de Privacidade, como apresentado abaixo:

A Vivo atende integralmente ao **parâmetro III**. A empresa publica desde 2016 relatórios de transparência e sustentabilidade. Ressaltamos que o relatório sobre 2023 ainda não foi publicado e salientamos a importância em fazê-lo.

A Vivo atende ao **parâmetro IV**, uma vez que seu "Informe de transparência" mais atualizado, de 2023, traz informações sobre o número de pedidos de acesso aos dados, atendidos e rechaçados. Bem como, no informe, a empresa detalha os contextos legais com base nos quais os pedidos foram feitos e por quais autoridades competentes. No entanto, não identificamos informações sobre o número de contas afetadas. Sendo assim, houve atendimento parcial do parâmetro.

A Vivo realiza Relatórios de Impacto à Proteção de Dados Pessoais (RIPD). No entanto, não foram localizados RIDPs publicados ou disponibilizados publicamente. Como a metodologia considera não apenas a elaboração, mas também a publicidade das informações desses documentos, que pode ser feita, por exemplo, por informativos mais simples e acessíveis ao público, o **parâmetro V** é considerado parcialmente atendido.

CATEGORIA 6: Notificação do usuário

Resultado: ☆

Nesta categoria, a Vivo obteve **estrela vazia**, pois não atendeu ao parâmetro.

A Vivo não atende ao **parâmetro I**, pois não apresenta, em seus documentos públicos, compromisso de notificar os usuários sobre pedidos de acesso a dados. Caso receba solicitações de fornecimento de dados por autoridades, a empresa deve atendê-las para não incorrer em crime de desobediência. No entanto, o parâmetro avalia a existência de compromisso de notificação nos casos em que não há imposição legal de sigilo, o que não foi identificado.