QUEM DEFENDE SEUS DADOS?

2022

INTERNETLAB
pesquisa em direito e tecnologia

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 2022 a sétima edição do projeto "Quem Defende Seus Dados?", versão brasileira do ***"Who has your back?"***.

Em 2015, o projeto "*Who Has Your Back?*", desenvolvido pela EFF há nove anos nos Estados Unidos, expandiu-se para outros países ao redor do mundo, especialmente os da América Latina[1]. As edições latino-americanas têm adotado como objetivo avaliar as empresas provedoras 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 as demais leis vigentes, e **busca avaliar o comprometimento público da empresa com a privacidade e a proteção de dados de seus usuários**. **Ao premiar as empresas com estrelas, nosso objetivo é 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 dos usuários.**

Neste ano, continuamos afinando nossos parâmetros de avaliação em vista da aprovação da Lei Geral de Proteção de Dados, de novas modificações nos entendimentos e práticas sobre privacidade e proteção de dados, e de notícias referentes ao uso de reconhecimento facial por parte das operadoras de telefonia. As empresas avaliadas permanecem as mesmas de 2021: Algar, Brisanet, Claro, Oi, Tim e Vivo.

Tentamos valorizar, além do compromisso das empresas expresso em seus contratos e políticas, também seu comprometimento e dedicação à implementação de importantes boas práticas de privacidade e proteção de dados. Valorizamos, 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, o fornecimento de meios para exercício dos direitos dos titulares de dados, como os direitos de acesso e apagamento dos dados, assim como o respeito a tais solicitações, a existência de protocolos específicos de entrega de dados a agentes do estado, dentre outros.

[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/.

Vale ressaltar que os resultados são amplamente divulgados na imprensa nacional[2] e internacional[3].

II. METODOLOGIA E RESULTADO GERAL

Cada empresa foi avaliada a partir de 6 categorias, cuja elaboração leva em consideração as exigências da legislação vigente e boas práticas internacionais em matéria de proteção à privacidade. **Para esta avaliação, foram analisados os contratos de prestação de serviço, relatórios de sustentabilidade e demais documentos que estavam disponíveis nos websites das empresas até 14/10/2022.** Buscamos ainda notícias que circularam na grande imprensa e mídia especializada. Foram considerados, para essa versão do Quem Defende Seus Dados, documentos, ações, posicionamentos etc. compreendidos entre junho de 2021 e outubro de 2022.

Com base nas respostas obtidas, atribuímos as seguintes notas: **A**. 1 estrela cheia; **B**. ¾ de estrela; **C**. ½ estrela; **D**. ¼ de estrela; **E**. Nenhuma estrela. Uma estrela cheia significa que a empresa atende a todos os parâmetros em determinada categoria, enquanto a atribuição de nenhuma estrela significa que a companhia não atendeu a nenhum parâmetro.

Destacamos que, com o intuito de incentivar as empresas com avaliações que elevem sua nota geral, parâmetros e sub-parâmetros parcialmente atendidos **foram sempre arredondados para cima no momento da soma e averiguação do cumprimento de uma categoria ou parâmetro**. Por exemplo, caso a empresa cumpra com 1 parâmetro integralmente e com outro parcialmente, e o atendimento a dois parâmetros seja necessário para a concessão de uma estrela cheia na categoria, o cumprimento, no caso, ao correspondente a "1,5" parâmetro foi considerado suficiente para a obtenção da estrela cheia. O mesmo ocorre entre sub-parâmetros e parâmetros: caso metade ou mais da metade dos sub-parâmetros tenham sido atendidos, o parâmetro correspondente foi considerado integralmente atendido.

Em 2022, as empresas obtiveram as seguintes notas:

[2] Os resultados do ano 2020 foram divulgados em diversos veículos nacionais de grande circulação: https://www1.folha.uol.com.br/mercado/2020/11/tim-e-mais-bem-avaliada-em-protecao-de-dados-algar-e-nextel-as-piores.shtml; https://www.minhaoperadora.com.br/2020/11/tim-e-a-empresa-que-melhor-protege-os-dados-de-seus-clientes.html; https://teletime.com.br/16/11/2020/vivo-e-tim-avancam-em-privacidade-de-dados-diz-pesquisa-do-internetlab/; https://www.telesintese.com.br/relatorio-indica-avanco-na-transparencia-de-politica-de-dados-de-provedoras/; https://www.convergenciadigital.com.br/Telecom/LGPD-ja-influencia-medidas-das-teles-para-protecao-de-dados-55480.html?UserActiveTemplate=mobile%2Csite&from%255Finfo%255Findex=241; https://esportes.yahoo.com/noticias/tim-%C3%A9-mais-bem-avaliada-221100343.html.

[3] A *Electronic Frontier Foundation*, maior e mais antiga organização civil dedicada à defesa de direitos digitais, também divulgou os resultados em seu website. EFF. InternetLab's Report Sets Direction for Telecom Privacy in Brazil. 16 de novembro de 2020. Disponível em: https://www.eff.org/deeplinks/2020/11/internetlabs-report-sets-direction-telecom-privacy-brazil.

QDSD?		Informações sobre a política de proteção de dados	Protocolos de entrega de dados para investigações	Defesa dos usuários no Judiciário	Postura pública pró-privacidade	Relatórios de transparência e de impacto à proteção de dados	Notificação do usuário
Claro		★	★	★	⯪	★	☆
NET		★	★	★	⯪	★	☆
oi		★	★	★	★	★	☆
oi		★	★	★	★	★	☆
TIM		★	★	★	★	★	☆
TIM		★	★	★	★	★	☆
vivo		⯪	★	★	⯪	★	☆
vivo		⯪	★	★	⯪	★	☆
Algar		★	★	⯪	⯪	☆	☆
brisanet		★	☆	★	☆	☆	☆
brisanet		★	☆	★	☆	☆	☆

III. CATEGORIAS

CATEGORIA 1: Informações sobre a política de proteção de dados

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

A legislação brasileira (Marco Civil da Internet, artigo 7º, incisos VI e VIII) garante a usuários o direito a informações claras e completas sobre o tratamento de seus dados, que somente podem ser utilizados para finalidades especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet. Além disso, o art. 16 do Decreto no 8.771/2016 (decreto que regulamenta o Marco Civil da Internet) determina que informações sobre padrões de segurança sejam divulgadas de forma clara e acessível a qualquer interessado, preferencialmente nos sites das empresas.

Mais recentemente, a Lei Geral de Proteção de Dados Pessoais reiterou e aprofundou estes marcos normativos e o respeito à transparência como princípio norteador da proteção de dados. Previu, assim, o direito do titular de dados pessoais a informações claras, adequadas e ostensivas sobre o tratamento de seus dados, especialmente no que diz respeito à finalidade específica, forma e duração do tratamento, à identificação e contato do controlador, ao eventual compartilhamento de dados e a respectiva finalidade, às responsabilidades dos agentes que realizarão o tratamento (LGPD, art. 9º e incisos) e aos direitos que lhe cabem. Previu ainda, para as hipóteses em que o consentimento é requerido, a nulidade do consentimento não precedido de informações transparentes, claras e inequívocas e a obrigação de informar eventuais mudanças da finalidade do tratamento não compatíveis com o consentimento original, facultando-se neste caso a revogação.

Além disso, nesta avaliação, consideramos o art. 43 do Código de Defesa do Consumidor, o Art. 7º do Marco Civil da Internet e diversos dispositivos da Lei Geral de Proteção de Dados, que conferem aos titulares o direito à exclusão definitiva, ao acesso e à retificação dos dados pessoais.

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

É importante ressaltar que o termo "dados" é utilizado em sentido amplo, englobando quaisquer dados pessoais conforme definido pela legislação (incluindo, portanto, tanto dados cadastrais como registros de conexão).

<u>Quais foram os parâmetros de avaliação?</u>

(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, na política ou aviso de privacidade, de categorias de terceiros que 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) a forma como se dá a utilização ou tipo de tratamento.

(III) **[Informações sobre armazenamento, segurança e compartilhamento]** A empresa fornece informações claras e completas sobre como protege dados pessoais, i.e.: (a) por quanto tempo e onde são armazenados; (b) em quais circunstâncias são apagados; (c) se e em quais circunstâncias são retidos; (d) quais práticas de segurança administrativa e técnica observa; (e) se há Política de Segurança Cibernética / TI publicada com informações sobre as proteções específicas contra malware, ransomware, worms e outros vírus; (f) quais categorias de colaborador podem ter acesso aos dados (controles de acesso); (g) com quais terceiros a empresa compartilha os dados (após a coleta); (h) para quais finalidades os dados são compartilhados (inclusive quando do uso de softwares, plataformas online, redes ou nuvens para uso interno da empresa); (i) quais as hipóteses de transferência internacional de dados;

(IV) **[Informações sobre direitos]** (a) Informar sobre quais são e os meios (e.g. e-mails ou links) para exercício dos direitos dos titulares sobre seus dados; (b) informar os titulares de seus direitos.

(V) **[Respostas a solicitações de direitos] (**a) A empresa forneceu confirmação de existência ou o acesso a dados pessoais mediante requisição de seus titulares, integrantes do InternetLab, por meio de declaração clara e completa, indicando a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, no prazo de até 15 (quinze) dias; ou em formato simplificado, imediatamente. (b) A empresa atendeu às requisições sobre direitos dos titulares, integrantes do InternetLab, em até um mês;

(VI) **[Atualização da política de privacidade]** A empresa promete enviar notificações (e.g. por e-mail ou SMS) ao usuário 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 de 6 a 7 parâmetros.

★ O provedor de Internet atende de 4 a 5 parâmetros.

★ O provedor de Internet atende de 2 a 3 parâmetros.

★ O provedor de Internet atende a apenas um dos parâmetros.

☆ O provedor de Internet não atende a 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?

O Marco Civil da Internet, em seu artigo 10, diferencia as hipóteses nas quais autoridades públicas podem ter acesso a dados cadastrais e a registros de conexão.

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 nº 12.965/2014), somente podem ser disponibilizados ao requisitante se a entrega for autorizada por ordem judicial (art. 10, §1º da Lei nº 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 art. 5, 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, dada a insegurança acerca dos dados sujeitos à retenção e compartilhamento.

Já os **dados cadastrais** podem ser disponibilizados diretamente a autoridades administrativas, sem necessidade de ordem judicial, se e quando possuem competência legal para a requisição (art. 10, § 3º). Além disso, o art. 11 do Decreto nº 8.771/2016, que regulamenta alguns aspectos do Marco Civil da Internet, determina que a autoridade administrativa deve indicar no pedido o fundamento legal de competência expressa para o acesso e a motivação para o acesso aos dados cadastrais. **Atualmente, autoridades policiais e do Ministério Público possuem competência para a requisição de dados cadastrais em situações específicas.** Estão elas no âmbito de aplicação da Lei das Organizações Criminosas, da Lei dos Crimes de Lavagem de Dinheiro e 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, em razão da Lei nº 12.830/2013, que dispõe sobre a investigação criminal conduzida pelo delegado de polícia, reivindicam autoridade para requisitar informações, independentemente do crime investigado (art. 2, §2º). A questão foi levada ao Supremo

Tribunal Federal (ADI 5059). 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.

Quanto aos dados de geolocalização, o art. 13-B do Código de Processo Penal dispõe que "se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso". O § 4º do referido artigo dispõe que, "não havendo manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará" diretamente "às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz". Também estes dispositivos estão submetidos à avaliação do Supremo Tribunal Federal, em decorrência da ação direta de inconstitucionalidade (ADI 5642) proposta em janeiro de 2017 pela Associação Nacional das Operadoras de Celular (ACEL), por violarem os art. 5º, incisos X e XII da Constituição, ao permitirem uma interpretação, segundo a qual em alguns casos seria dispensável a ordem judicial para acesso aos dados de localização. 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 nº 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.

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, assim, por se tratar de matéria sob controvérsia jurídica, a questão se desdobra em diferentes parâmetros, que buscam discriminar diferentes 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 constantes 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.

Assim, procuramos avaliar aqui 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.

<u>Quais foram os parâmetros de avaliação?</u>

(I) **[Dados cadastrais: autoridades competentes identificadas]** 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.

(II) **[Dados cadastrais: autoridades e crimes identificados]** A empresa promete fornecer dados cadastrais por requisição (sem ordem judicial) apenas a autoridades administrativas competentes, identificando-as, e 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.

(III) **[Dados de geolocalização]** A empresa (a) oferece informações claras sobre as circunstâncias em que fornece dados de geolocalização, identificando se fornece dados em tempo real ou pretéritos e (b) 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 ou, (c) ainda nestes casos, promete, apenas na ausência de manifestação judicial, entregar os dados no prazo de 12 (doze) horas, mediante requisição da autoridade competente.

(IV) **[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).

(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 quatro ou cinco parâmetros.

★ O provedor de Internet atende a três parâmetros.

★ O provedor de Internet atende a dois parâmetros.

★ O provedor de Internet atende a um parâmetro.

☆ O provedor de Internet não atende a nenhum dos parâmetros.

CATEGORIA 3: Defesa dos usuários no Judiciário

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

O Judiciário, tanto nas disputas de perfil individual quanto coletivo, é um importante espaço para a defesa e consolidação de direitos de usuários contra abusos e ilegalidades. Com isto em vista, buscamos avaliar o posicionamento das empresas em processos judiciais em matéria de privacidade e proteção de dados.

Para tal, foram considerados, dentro do período analisado, dois eixos de análise: (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. Neste último caso, consideramos o disposto no Decreto nº 8.771/2016, que estabelece a necessidade de indicação do fundamento legal de sua competência, a motivação do pedido de dados e veda pedidos coletivos, genéricos ou inespecíficos. A desatenção a tais critérios é forte indício da abusividade da solicitação de acesso.

Quais foram os parâmetros de avaliação?

(I) **[Contestação de legislação]** A empresa contestou judicialmente legislação, ou interpretação da legislação, que considera violar a privacidade de usuários de Internet, por ser desproporcional e/ou por não estabelecer de modo claro, preciso e detalhado os casos e circunstâncias em que dados devam ser entregues ou as salvaguardas adequadas para inibir eventuais abusos (Exemplos: 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 judicial ou administrativamente, ao menos uma vez dentro do período analisado, pedidos abusivos de acesso a dados de usuários que extrapolaram as prerrogativas legais da autoridade solicitante e/ou eram desproporcionais, em razão de sua falta de clareza e precisão sobre dados requeridos e motivação, ou por qualquer outra razão que comprometa o direito à privacidade de usuários.

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 esse direito no Brasil?

Esta categoria pretende avaliar a postura pública das empresas em relação a temas de privacidade e proteção de dados. Para isso, consideramos sua participação em consultas públicas, debates ou eventos acerca de leis, projetos de lei e políticas públicas que impactam usuários da rede, assim como seu posicionamento na mídia comum e especializada, por exemplo, em resposta a medidas governamentais que possam impactá-los.

Neste ano, observamos ainda a postura pública das empresas em relação ao uso de tecnologias de reconhecimento facial. Nosso interesse na temática é devido (i) às recentes ações judiciais e iniciativas da sociedade civil relacionadas a essa temática, (ii) à controvérsia existente na Lei Geral de Proteção de Dados sobre uso de dados biométricos para prevenção a fraudes sem necessidade de obtenção do consentimento do titular de dados, (iii) as questões de discriminação algorítimica e vieses potencialmente envolvidos no uso dessas ferramentas, e (iv) relatos, por parte de clientes, de que empresas de telecomunicações têm solicitado o reconhecimento facial de maneira obrigatória como um requisito para conclusão de cadastro.

Avaliamos, nesse contexto, o comprometimento das empresas com a defesa dos dados pessoais de seus usuários, manifesto em seu posicionamento em consultas públicas, debates ou na mídia, a respeito de tais iniciativas. Para fins de pontuação, não levaremos em consideração se as empresas simplesmente responderam às exigências feitas pelas autoridades públicas, mas sim a conduta e posicionamento adotados publicamente pelas empresas nessas situações.

Consideramos apenas a participação feita em nome da própria empresa e não por associações compostas por várias empresas – como o SindiTeleBrasil – pois acreditamos que o posicionamento público institucional da empresa é essencial para gerar o vínculo de confiança e compromisso com os seus usuários.

Quais foram os parâmetros de avaliação?

(I) **[Posicionamento em geral]** A empresa se posicionou em nome próprio, em quaisquer consultas públicas, debates, ou na mídia, especializada ou não, e defendeu concretamente a aprovação de normas ou adoção de técnicas que aumentem a proteção conferida aos usuários dos seus serviços?

(II) **[Posicionamento sobre reconhecimento facial]** A empresa se posicionou em nome próprio, em consultas públicas, debates, ou na mídia, especializada ou não, contra a obrigatoriedade de procedimentos de reconhecimento facial para fins de cadastro ou acesso aos serviços de telefonia móvel?

Padrões de desempenho

★ O provedor de Internet atende aos dois parâmetros.

⯪ O provedor de Internet atende a 1 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?

Relatórios de transparência são informes emitidos por empresas que podem conter, entre outros conteúdos, estatísticas relacionadas a pedidos de dados. Relatórios com esse tipo de informação tornam público o quanto e como as empresas cooperam com as autoridades do Estado, em geral por força de lei, entregando dados para a instrução processual em causas cíveis e criminais. No exterior, a publicação desses relatórios por provedores de aplicações como Google, Facebook, Twitter, e Microsoft, e provedores de conexão à Internet como Vodafone e Verizon já é uma prática comum. No Brasil, essa ainda é uma prática pouco comum, o que prejudica o debate público sobre privacidade e oculta a afetação desse direito por práticas estatais e privadas.

É verdade que as empresas brasileiras não são ainda legalmente obrigadas a produzir relatórios de transparência. Por outro lado, a publicação de estatísticas sobre pedidos e exibições de dados, de forma agregada, tampouco é proibida. Existe, portanto, a oportunidade de cultivar uma relação de confiança com usuários, baseada na transparência, e contribuir para o debate público a respeito das prerrogativas de acesso a dados de usuários por parte das autoridades públicas.

O art. 12 do Decreto nº 8.771/2016, nesse sentido, cria a obrigação de divulgar estatísticas similares a essas citadas acima (quantidade de requerimentos, autoridades requerentes etc.) para órgãos da Administração Pública federal, o que reforça o desenvolvimento de uma cultura de transparência sobre pedidos de dados no país. Acreditamos que o setor privado possa, desde já, voluntariamente se apropriar dessa pauta. Afinal, em manifestações a Comissões Parlamentares, empresas já mencionaram a grandeza do número de pedidos que recebem e a Associação Nacional de Operadoras Celulares (ACEL), em manifestação na ADI 5063, afirmou que há abusos na atuação das autoridades públicas, como pedidos não fundamentados. Nesse contexto, torna-se cada vez mais importante a criação de canais de acompanhamento periódicos dessas informações por usuários, como seria o caso com a publicação dessas informações em relatórios de transparência.

A Lei Geral de Proteção de Dados Pessoais prevê, ademais, a publicação de relatórios de impacto à proteção de dados pessoais, que devem conter informações sobre processos de tratamento de dados pessoais que possam gerar riscos aos direitos dos usuários, assim como as medidas adotadas para mitigar esses riscos. De acordo com a lei, a publicação desses relatórios poderá ser determinada pela Autoridade Nacional de Proteção de Dados Pessoais (art. 10, §3º; art. 32 e art. 38), nos termos de seu regulamento. A elaboração e publicação de relatórios de impacto à proteção de dados, portanto, foi considerada nessa edição do Quem Defende seus Dados.

Por fim, ressalta-se que também foi analisada a facilidade de acesso pelo público aos relatórios de transparência, assim como a publicidade a eles dada. Assim, somente relatórios escritos ou traduzidos para língua portuguesa foram considerados. Além disso, são melhor avaliados os relatórios facilmente acessíveis nas páginas principais das empresas brasileiras, ou nas páginas de contratação de serviços, e/ou que tenham sido publicizados, pela própria empresa, em propagandas ou na mídia.

Quais foram os parâmetros de avaliação?

(I) **[Publica relatório]** Publica relatório de transparência em português sobre privacidade e proteção de dados.

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

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

(IV) **[Informações sobre pedidos de acesso a dados]** Apresenta, no relatório de transparência:a) Informações sobre pedidos de acesso a dados recebidos, atendidos e rechaçado; 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]** 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?

Quando usuários são notificados de que seus dados cadastrais ou registros de conexão à Internet foram requisitados por autoridades administrativas ou judiciais, ampliam-se suas condições de exercício da ampla defesa contra abusos e irregularidades.

O impacto de notificações para a garantia da efetiva e ampla defesa em um Estado de Direito não é novidade. À luz do princípio constitucional do devido processo, muitas leis estabelecem 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 a ele avisar o atingido sobre o pedido, para que possa apresentar seus argumentos (art. 282, §3º).

No contexto de solicitações de dados, provedores de Internet ganham papel fundamental na proteção de garantias processuais de usuários afetados. Isso porque a notificação de empresas ao usuário permite, na primeira oportunidade, que o usuário conteste pedidos ilegais – tanto na forma de ordens judiciais não fundamentadas, quanto de requisições de autoridades administrativas sem competência e embasamento suficiente. Sem a notificação, o usuário depende da contestação feita pelas próprias empresas contra pedidos considerados por elas abusivos. Se notificados pelas empresas, usuários ganham a possibilidade de se defenderem contra potenciais violações de sua privacidade.

A prática é obrigação legal em diversas jurisdições. Nos Estados Unidos, por exemplo, a Lei 8 USC § 2705(B) prevê a necessidade de um aviso prévio ao cliente quando a requisição aos dados se der por intimação administrativa autorizada por júri federal ou estadual ou por ordem judicial. A ordem judicial, contudo, poderá exigir que a notificação seja adiada por um período máximo de 90 dias, caso haja motivos para acreditar que a notificação possa interferir na investigação.

Tendo isso em mente, consideramos importante incentivar a prática de notificação de usuários no QDSD. 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 Twitter assegura que notifica o usuário caso exista uma solicitação legal relacionado à conta, exceto quando alguma proibição ou quando a solicitação se enquadrar entre as exceções previstas na política de notificações de usuários (casos relacionados a ameaças à vida, exploração sexual de menores ou terrorismo). No mesmo sentido, o Facebook, além de garantir a notificação prévia do usuário, se compromete a fornecer a notificação em atraso, após o término do período de não divulgação, judicialmente estabelecido.

A possibilidade de notificação do usuário pode ser vislumbrada, por exemplo, em casos de pedidos de dados de identificação na justiça cível e no âmbito de pedidos realizados 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 pode ser vista como em regra permitida, caso não haja exigência de sigilo, em respeito aos princípios constitucionais da ampla defesa e ao contraditório, ao reforçar a possibilidade de contestação à produção de provas irrelevantes ou desnecessárias aos fatos do processo.

A notificação não é uma prática difundida no país, nem é dever legal das empresas. É uma medida vista como inovadora e, por exigir pessoal responsável pelas notificações, possivelmente custosa. Por outro lado, a notificação do usuário, no primeiro momento em que for legalmente possível, e preferencialmente prévio à entrega de dados, colabora com o princípio da ampla defesa, além de fomentar uma cultura de proteção à privacidade.

<u>Qual foi o parâmetro de avaliação?</u>

[Notificação] Promete notificar usuário antes da entrega de dados cadastrais e registros de conexão, sempre que o sigilo da entrega não for imposto por lei ou determinado em decisão judicial, ou no primeiro momento em que a notificação for permitida.

Padrões de desempenho

★ O provedor de Internet atende ao parâmetro.

☆ O provedor de Internet não atende ao parâmetro.

IV. RESULTADOS

CLARO / NET

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a Claro-NET obteve **estrela cheia**, tendo atendido aos **parâmetros I, II, III, IV, V, VI e VII**.

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

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

> Quais dados pessoais a Claro coleta e para quais finalidades eles são utilizados?
> • Dados Cadastrais:
> • Quais Dados: nome, e-mail, endereço, telefone, CPF, RG, data de nascimento e gênero.
> • Finalidades: são importantes para algumas ações, como preenchimento do seu contrato de serviço, emissão de nota fiscal e, também para nos comunicarmos com você.
>
> • Dados de Navegação e Uso dos Produtos e Serviços Claro:
> • Quais Dados: informações sobre navegadores e dispositivos, incluindo endereço de IP, relatórios de erros, atividade do sistema, data, hora e URL, dados sobre ligações e telefonia incluindo destino, duração e envio de mensagens SMS. Além disso, informações sobre chamadas realizadas e recebidas, envio de SMS, volume de dados utilizados e antenas que atendem você.
> • Finalidades: mensurar a qualidade dos nossos serviços para que você possa entender a fatura, ter seu próprio controle e para que a Claro possa cumprir com as determinações previstas pelo nosso órgão regulador e pela legislação.
>
> (...)

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): referente às situações em que a coleta ocorre, também foi considerado atendido. Isso porque, mesmo que não haja redação específica nesse sentido, nos mesmos trechos apontados acima, informa-se indiretamente quais as situações em que a coleta ocorre (e.g. na navegação e no uso dos produtos, no preenchimento do contrato de serviço etc.) Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

Sub-parâmetro (c): referente à possibilidade de coleta de dados disponíveis publicamente, foi considerado atendido. Na mesma seção apontada no **Sub-parâmetro (a)** acima, há o relato de que dados públicos disponíveis são coletados pela empresa.

Sub-parâmetro (d): referente à listagem de quais terceiros fornecem dados à empresa, foi considerado atendido. A empresa divulgue, no Portal de Privacidade, a lista de terceiros com quem compartilha os dados por categorias.

Sub-parâmetro (e): relativo à avaliação sobre a conformidade legal de terceiros com a LGPD, foi considerado atendido. Isso porque a Claro estipula cláusula específica sobre privacidade e proteção de dados em que são exigidos dos terceiros pleno cuidado e garantias do tratamento dos dados

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

Sub-parâmetro (a): referente à finalidade do tratamento dos dados, foi considerado atendido. No seu Portal da Privacidade, na seção "Quais dados pessoais a Claro coleta e para quais finalidades eles são utilizados?", a empresa explica, de forma detalhada, quais são as funções para cada dado coletado. Como no caso dos Dados Cadastrais:

> • Quais Dados: nome, e-mail, endereço, telefone, CPF, RG, data de nascimento e gênero.
>
> • Finalidades: são importantes para algumas ações, como preenchimento do seu contrato de serviço, emissão de nota fiscal, cadastramento e acesso aos aplicativos e atendimento por Internet da Claro e também para nos comunicarmos com você.

Sub-parâmetro (b): referente à forma como se dá a utilização ou tipo de tratamento, foi considerado 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 a proteção de dados pessoais, considerou-se que foi atendido, pois os sub-parâmetros (a), (b), (c), (d), (e), (f), (g), (h) e (i) foram atendidos.

Sub-parâmetro (a): referente ao tempo e local de armazenamento dos dados, foi considerado atendido. No seu Portal de Privacidade, na seção "Por quanto tempo a Claro trata seus dados e onde?", 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, não afirmando haver armazenamento em terceiros ou servidores em locais indefinidos.

> A Claro trata seus dados pelo tempo que durar a prestação dos seus serviços, mas também precisa manter seus dados após o término da sua relação com a Claro para cumprir com a lei, como nos casos em que seja necessário fornecer dados às autoridades públicas ou mesmo realização de defesa em processos judiciais.
>
> Alguns exemplos de prazos de retenção pela Claro são:
>
> • seis meses - registros de acesso a Funcionalidades de internet nos aplicativos próprios da Claro;
>
> • um ano - registros de conexão à internet, sendo que não guardará os registros de acesso a funcionalidades de internet;
>
> • um ano e três meses - gravação da interação entre consumidor e atendente no SAC;
>
> • seis anos - documentos fiscais que englobam dados das ligações efetuadas e recebidas, data e horário de duração e valor da chamada.
>
> • dez anos - dados cadastrais e de faturamento;
>
> A Claro armazena os dados de forma segura e com rígido controle de acesso. Esses dados encontram-se armazenados em seus servidores nos data centers situados nas cidades de São Paulo, Campinas e Rio de Janeiro.

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

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

Sub-parâmetro (d): relativo às práticas de segurança da empresa, foi considerado atendido. 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 2021 (p. 48) do grupo América Móvil. De acordo com o relatório, o sistema adotado no Brasil é o Security Operation Center com certificado ISO 27001 Safety Management Systems.

Sub-parâmetro (e): referente à existência ou não de Política de Segurança Cibernética/TI, foi considerado atendido. Na mesma parte do documento, a referência ao certificado ISO 27001 Safety Management Systems demonstra a preocupação da empresa com uma política específica no tema.

Sub-parâmetro (f): relativo a quais categorias de colaborador podem ter acesso aos dados, considerou-se atendido. Isso 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 (g): relativo a quais terceiros a empresa compartilha os dados após a coleta, considerou-se que foi atendido. No item "Com quem a Claro compartilha dados?", a empresa expõe categorias gerais de empresas com as quais podem ser compartilhados os dados:

> 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 (h): relativo às finalidades do compartilhamento de dados com terceiros, foi atendido, em vista dos detalhamentos de cada compartilhamento conforme trecho do Portal da Privacidade apontado acima.

Sub-parâmetro (i): relativo à transferência internacional de dados, foi considerado atendido. Em seu Portal da Privacidade, a Claro possui um item destinado à transferência internacional de dados:

> A Claro também contrata armazenamento em nuvem de fornecedores e parceiros localizados em outros países, o que é uma prática comum e segura de mercado. Esse tipo de tratamento é fundamental para a prestação dos serviços contratados com a Claro e poderá ser realizado fora do território nacional, por exemplo, em servidores localizados em outros países com grau de proteção de dados pessoais adequados ao previsto na Lei. Ainda assim, a Claro segue atenta às orientações da ANPD, que futuramente 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. Os sub-parâmetros (a) e (b) foram atendidos.

Sub-parâmetro (a): relativo aos quais são e os meios para exercício dos direitos dos titulares sobre seus dados, considerou-se atendido. 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. A empresa informa, também, em cada caso, os

meios para o exercício destes direitos - ou através do próprio Portal da Privacidade, ou mediante e-mail ao DPO da Claro.

Sub-parâmetro (b): relativo às informações sobre quais são os direitos do titular, foi considerado atendido, de acordo com o mesmo item exposto acima.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados, foi considerado atendido. A empresa possui portal de acesso a direitos dos titulares com extrato dos dados utilizados. Embora um membro da equipe tenha tido problemas técnicos para acessar o portal, a situação foi resolvida 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. A Claro realiza campanhas de comunicação de atualização da sua Política de Privacidade.
Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado atendido. No rodapé da página inicial do site da Claro, há o link para a Política de Privacidade. Ao acessar esse link, o usuário é redirecionado para o Portal de Privacidade da Claro[4], em que constam a "Política de privacidade", a "Política de cookies" e "Direitos de privacidade". As informações que constam no Portal de Privacidade são bastante claras e de fácil acesso ao cliente.

captura de tela de 17.10.2022

Assim como, as informações que constam na Política de Privacidade são apresentadas nos contratos da Claro.

[4] https://www.claro.com.br/politica-de-privacidade

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ★

Nesta categoria, a Claro obteve **estrela cheia,** tendo cumprido os parâmetros de I a IV ecumprido parcialmente o parâmetro V.

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado cumprido. Em seu Portal de Privacidade, a empresa informa sobre as situações em que compartilha dados com o Setor Público:

> 12. 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.
>
> 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."

O **parâmetro II**, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, foi considerado 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, conforme trecho transcrito abaixo.

O **parâmetro III**, referente ao oferecimento de informações sobre dados de geolocalização, foi considerado atendido. 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.

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, foi considerado atendido. 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.

Por fim, o **parâmetro V**, relativo à existência de protocolos específicos sobre entrega de dados ao Estado, foi considerado parcialmente atendido. Isso porque, é possível encontrar, na página 51 do Relatório de Sustentabilidade AMX, os números de entrega de dados ao Estado, contudo, o relatório encontra-se apenas em espanhol, sem uma versão em português.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: ★

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

Quanto ao **parâmetro I**, referente à contestação de legislação, realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte, e não localizamos quaisquer ações em que a Claro contesta a legislação relacionada aos procedimentos de entrega de dados ao judiciário. Ressaltamos que nossa busca, por questões de escopo e tempo, não buscou por ações do tipo nos tribunais estaduais, relativas, portanto, a legislações ou interpretação de legislações de âmbito estadual. As empresas têm a possibilidade de, durante a fase de discussão dos parâmetros e troca de documentos, comprovar sua atuação nesse sentido.

Em 29/03/2022, o STF publicou o julgamento da Ação Direta de Inconstitucionalidade número 4924/DF[5], em que a Associação Nacional das Operadoras Celulares - ACEL, da qual a Claro faz parte, pediu pela declaração de inconstitucionalidade da Lei 17.107/12, do Estado do Paraná, que dispõe sobre penalidades ao responsável pelo acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres (trote telefônico). A lei visava estabelecer obrigação às operadoras de telefonia de fornecer os dados dos proprietários de linhas telefônicas que acionem indevidamente os serviços de atendimento diante de mero ofício por qualquer órgão ou instutuição pública envolvida. A ACEL argumentou em favor da inviolabilidade da intimidade, vida privada horna e do sigilo das comunicações telefônicas (segundo estabelecido no artigo 5º, incisos X e XII da Constituição Federal), mencionando a indisponibilidade do direito à proteção de dados pessoais em sua argumentação.

Além disso, a ACEL havia ajuizado a ADI 5040/PI[6], publicada em 2021 (não incluída em nosso relatório anterior), em que questionava a legalidade da Lei Nº 6.336/2013 do Estado do Piauí, que obrigava as empresas prestadoras de serviço de telefonia móvel pessoal a fornecerem, aos órgãos de segurança pública, dados relativos à localização de telefones celulares e cartões "SIM" que tivessem sido objeto de furto, roubo e latrocínio ou utilizados na prática de delitos. Entre seus argumentos, a ACEL também alegou grave ofensa à privacidade de seus clientes na hipótese de divulgação das informações pessoais, citando a Constituição e o direito fundamental à privacidade, além da inviolabilidade dosigilo telefônico.

Por fim, para averiguação do **parâmetro II**, referente à contestação de pedidos abusivos, 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 "Claro E sigilo E quebra" e por acórdãos publicados entre 21/06/2021 e 19/10/2022. Encontramos diversas ações nas quais Claro contestou pedidos de dados de seus clientes pela falta de ordem judicial determinando a entrega dos dados[7].

Por exemplo, encontramos, no relatório do acórdão referente ao Processo 1042581-72.2021.8.26.0100:

---

[5] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183

[6] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4461936

[7] É o caso do Processo 1058034-44.2020.8.26.0100, acesso em: http://www.dje.tjsp.jus.br/cdje/consultaSimples.do?cdVolume=15&nuDiario=3242&cdCaderno=15&nuSeqpagina=1

> *"Citada, a corré Claro S/A apresentou contestação às fls. 72/80. Em preliminar, suscitou falta de interesse de agir pela perda do objeto da ação, uma vez que o autor requereu IPs de março de 2020 e anteriores a esta data. Que, o art. 13 do Marco Civil determina a obrigatoriedade das empresas provedoras de conexão em manter a guarda pelo período de até um ano. Se analisar o acesso mais antigo, de março de 2020, o dever de guarda cessou em março de 2021, além do Marco Civil determinar a exclusão do acesso após o período de guarda. A ordem foi recebida em junho de 2021. No mérito, alegou que não se nega a prestar as informações pleiteadas, desde que precedias de ordem judicial, visto que a prestação de tais informações envolve quebra de sigilo, cuja proteção dos dados cadastrais é assegurada pela Constituição Federal."*

Também, no julgamento do Processo, 1058034-44.2020.8.26.0100 deste ano, encontramos:

> *"A Corré Claro S/A requer a reforma da sentença. Alega, em breve síntese, que, no caso em comento, falta interesse de agir para o Autor, bem como que o pedido é impossível, haja vista que o suposto acesso ao sistema de telecomunicações pelos ofensores ocorreu em período anterior ao prazo de 1 (um) ano de resguardo dos dados determinado pelo art. 13 da Lei. 12.965/14 (Marco Civil da Internet), tornando a obrigação de fornecer tais informações de acesso, inexequível."*

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, a Ação Direta de Inconstitucionalidade (ADI) 5642[8], da ACEL, não foram consideradas, já que não registraram movimentações relevantes em vista da suspensão do julgamento e pedido de vista pelo Ministro Nunes Marques (em 17/06/2021).

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Claro obteve **meia estrela,** pois atendeu a um dos parâmetros.

O **parâmetro I**, relativo ao posicionamento em geral da empresa, foi considerado atendido. Em algumas oportunidades ao longo do ano, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários.

---

[8] A Associação Nacional das Operadoras Celulares (Acel), da qual algumas operadoras fazem parte, ajuizou a Ação Direta de Inconstitucionalidade (ADI) 5642, no Supremo Tribunal Federal (STF), para impugnar dispositivo da Lei 13.344/2016, que confere a delegados de polícia e membros do Ministério Público a prerrogativa de requisitar informações e dados necessários à investigação criminal nos casos de tráfico de pessoas, independentemente de autorização judicial. A ACEL pede a concessão de liminar para que o STF dê à Lei 13.344/2016 interpretação conforme a Constituição Federal de modo a impedir entendimento que leve a medidas como interceptação telemática e de voz, localização de terminal ou IMEI (Identificação Internacional de Equipamento Móvel) de cidadão em tempo real por meio de ERB, extrato de ERB, dados cadastrais de usuários de IP, extratos de chamadas telefônicas e SMS, entre outros dados de caráter sigiloso. No mérito, pede a declaração de inconstitucionalidade parcial do dispositivo questionado.

Além disso, a Claro participou, por meio da Conexis do lançamento do Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações, apresentado à Autoridade Nacional de Proteção de Dados[9].

Além disso, a empresa se manifestou publicamente nos seguintes casos:

- Contribuições à minuta de resolução que regulamenta a aplicação da Lei nº 13.709, para agentes de tratamento de pequeno porte, submetida à Consulta Pública;
- Workshop sobre o Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações;
- Debate da Conexis sobre debate código de boas práticas de proteção de dados para telecom https://teletime.com.br/01/11/2022/conexis-debatecodigo-de-boas-praticas-de-protecao-de-dados-para-telecom/
- Notícia: É impossível delegar a ANPD toda a proteção de dados no Brasil https://www.convergenciadigital.com.br/Telecom/E-impossiveldelegar-a-ANPD-toda-a-protecao-de-dados-no-Brasil-61845.html
- Notícia: Claro celebra iniciativa do setor telecom para proteção de dados https://dplnews.com/brasil-claro-celebra-iniciativa-dosetor-telecom-para-definicao-de-boas-praticas-para-protecao-dedados/

O **parâmetro II** foi considerado não atendido. A empresa não se manifestou publicamente contra o uso de reconhecimento facial ou comprometeu-se a não o utilizar para fins de identificação.

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

Resultado: 

Nesta categoria, a Claro obteve **¾ de estrela,** pois atendeu integralmente a 3 parâmetros, I, II e III e parcialmente ao parâmetro IV.

O **parâmetro I** foi considerado atendido. A empresa publicou Relatório de Transparência/Social em seu site.

O **parâmetro II** foi considerado atendido. O Relatório pode ser facilmente acessado no Portal de Privacidade no ícone "Relatório de Transparência", sendo direcionado para o Relatório de 2021, publicado em 2022.

O **parâmetro III** foi considerado atendido. A empresa publicou por dois anos seguidos os Relatórios de Transparência, em 2021 e em 2022.

[9]Acesso em: https://www.telesintese.com.br/operadoras-criam-codigo-de-boas-praticas-de-protecao-de-dados/

O **parâmetro IV** foi considerado parcialmente atendido. A empresa publicou, no Relatório de Transparência, que em 2021 houve 32.949 pedidos de quebra de sigilo. Todavia, não publicou quantos desses pedidos foram atendidos e quantos foram rechaçados.

O **parâmetro V**, por sua vez, relativo à publicação de Relatórios de Impacto à Proteção de Dados, também não foi considerado atendido. Não foram localizados quaisquer documentos nesse sentido em nossas buscas.

CATEGORIA 6: Notificação do usuário

Resultado: ☆

A Claro-NET não obteve estrela, pois não há menção à possibilidade de notificação do usuário em qualquer um dos documentos analisados.

OI

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Na Categoria 1, a Oi obteve **estrela cheia**, pois atendeu integralmente aos parâmetros I, II, IV, VI e VII e parcialmente aos parâmetros III e V.

Em relação ao **parâmetro I**, relacionado aos procedimentos de coleta de dados pessoais, consideramos o seguinte:

Sub-parâmetro (a): integralmente atendido, por meio da disponibilização, no Aviso de Privacidade[10] da Oi, seção 3 ("Quais dados são coletados?") de um descritivo de todos os tipos de dados pessoais coletados discriminados por categoria de titular ("Clientes e Ex-Clientes" ou "Não Clientes"); Com relação aos Clientes, a Oi alega coletar:

- **Dados de Cadastro:** Nome, CPF, RG, data de nascimento, nacionalidade, filiação, E-mail, Telefone residencial e móvel, Endereço residencial e comercial, Profissão e/ou ocupação;
- **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.

Com relação aos Não Clientes (segundo o Fluxo, referentes a *prospects*, terceiros e colaboradores), a Oi alega coletar:

- **Dados de Cadastro:** Nome, CPF, RG, data de nascimento, E-mail, Telefone residencial e/ou móvel, Endereço residencial e/ou comercial;
- **Dados financeiros:** Informações do cartão de crédito ou débito e conta bancária, Score de crédito;
- **Dados de navegação:** Endereço de IP, Local de conexão, Cookies.

Sub-parâmetro (b): integralmente atendido, por meio do Fluxo de Dados disponibilizado no Programa Oi de Privacidade[11] (também acessível pelo Aviso de Privacidade[12], seção 2), com detalhamento das situações em que a coleta ocorre (tanto direta quanto indiretamente);

---

[10] https://www.oi.com.br/aviso-de-privacidade/

[11] https://internetlab.org.br/wp-content/uploads/2022/10/programa-oi-de-privacidade.pdf

[12] https://www.oi.com.br/aviso-de-privacidade/

O item 5 do Aviso de Privacidade "Como é feita a coleta de dados" também fornece um detalhamento das diferentes formas de coleta empregadas pela Oi. A coleta automática por meio de sites e aplicativos é feita por meio de cookies, para os quais o Aviso de Cookies disponibilizado pela Oi fornece mais informações como (i) tipos de cookies e (ii) como gerenciar as preferências de cookies. Não há especificação, no entanto, de quais finalidades são atribuídas a cada tipo de dado coletado por cookies. Também não há especificação de quais dados são coletados automaticamente durante a utilização dos serviços da Oi, nem as finalidades para as quais são tratados.

"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
Quando você navega em nossos sites e aplicativos (através de cookies) ou utiliza nossos serviços.

De forma indireta
Através de empresas parceiras com as quais você tenha um vínculo/cadastro"

Sub-parâmetro (c): integralmente atendido. Há possibilidade de coleta de dados públicos por meio de websites - tal como apresentado no Fluxo de Dados disponibilizado no Programa Oi de Privacidade[13].

Sub-parâmetro (d): integralmente 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 geral das categorias de terceiros que recebem dados da Oi, após coleta independente da operadora.

[13] https://internetlab.org.br/wp-content/uploads/2022/10/programa-oi-de-privacidade.pdf

Sub-parâmetro (e): integralmente atendido. No Programa de Privacidade, a Oi afirma que avalia a conformidade legal de terceiros com a LGPD nos aspectos de "*segurança, controles de acesso, cláusulas e procedimentos de gestão e acompanhamento que assegurem a proteção de dados*". Não somos informados, no entanto, sobre quais os procedimentos específicos empregados pela Oi para assegurar que os terceiros mantenham um nível adequado de proteção de dados pessoais (ex.: fiscalizações e auditorias, seguimento de protocolos de segurança específicos, aderência a cláusulas especificadas pela Oi e disponibilizadas ao público, etc.). No Programa de Privacidade, encontramos:

"[...] Devemos assegurar em cada uma das interações realizadas em nosso ambiente de dados:
[...]
Com nossos terceiros: (i) a existência de ***controles de acesso*** *dos dados disponibilizados ou acessados; (ii) que apenas os* ***dados necessários*** *para as finalidades do compartilhamento sejam de fato disponibilizados; (iii) que as transferências de informações sejam efetuadas* ***de modo seguro****; (iv) a existência de* ***cláusulas*** *contratuais que respaldem a relação; (v) a existência de diligências necessárias de acordo com a criticidade da relação; (vi) a devida gestão e acompanhamento do terceiro."*

O Relatório de Sustentabilidade 2021[14] da Oi também afirma que:

"Por meio do canal de atendimento de direitos, em especial os pedidos de não recebimento de ofertas, a Companhia pôde melhorar a fiscalização da atuação de parceiros comerciais (riscos de terceiros) contra violações de privacidade, tais como desrespeito a listas restritivas de contato e Não me Perturbe, o que culminou inclusive na aplicação de penalidades como descredenciamento de parceiros."

Entendemos, portanto, que a Oi tem procedimentos de monitoramento e gestão de terceiros com quem compartilha dados pessoais.

Em relação ao **parâmetro II**, relacionado ao respeito à finalidade do tratamento dos dados pessoais, consideramos o seguinte:

Sub-parâmetro (a): integralmente atendido. Há descrição das finalidades de tratamento no item "4. Para quais finalidades meus dados são tratados?" do Aviso de Privacidade, que traz uma indicação

[14] https://internetlab.org.br/wp-content/uploads/2022/10/Relatorio-Anual-de-Sustentabilidade-2021.pdf

genérica dos tipos de dados utilizados para cada finalidade. No entanto, a informação não permite ao usuário da Oi identificar se cada tipo de dado coletado é empregado para uma finalidade legítima, observados os princípios da necessidade e minimização. Uma descrição mais detalhada a respeito de quais tipos de dados são destinados a cada finalidade permitiria ao titular de dados compreender seus direitos com maior clareza.

Sub-parâmetro (b): integralmente atendido. O item "4. Para quais finalidades meus dados são tratados?" do Aviso de Privacidade também fornece noções gerais sobre a forma como a Oi utiliza e trata os dados conforme sua macrocategoria (ex.: "dados financeiros") e finalidade.

Em relação ao **parâmetro III**, relacionado ao respeito à finalidade do tratamento dos dados pessoais, consideramos o seguinte:

Sub-parâmetro (a): parcialmente atendido. O item "7. Por quanto tempo os meus dados ficam armazenados?" indica alguns dos prazos legais utilizados pela Oi para a retenção com base no cumprimento de obrigação legal ou regulatória (previstas na Resolução 632/2014 do Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações, Resolução 632/2014 do Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações e Marco Civil da Internet). Não há maior detalhamento, no entanto, a respeito dos prazos regularmente observados pela Oi para retenção de dados fundamentada em outras bases legais (ex.: legítimo interesse, para exercício de direito, etc.). Não sabemos se, nesses casos, a Oi mantém os dados pessoais retidos indefinidamente. Quando à localidade dos dados, o item "8. Onde meus dados são salvos?" nos informa que, "via de regra", os dados são armazenados na União Europeia e Estados Unidos.

Sub-parâmetro (b): não atendido. Os itens do Aviso de Privacidade referentes à retenção não especificam as hipóteses de exclusão de dados pela Oi. No entanto, há opção de *opt-out* disponibilizada ao longo de todo o documento por meio da página "Não Me Perturbe"[15].

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): parcialmente atendido. O item "9. Os meus dados estão protegidos?" do Aviso de Privacidade traz informações gerais sobre os procedimentos de segurança digital e conformidade legal da Oi.

Sub-parâmetro (e): integralmente atendido. A Oi disponibiliza sua Política de Segurança da Informação online[16] com detalhamento dos procedimentos técnicos empregados para a garantia da segurança cibernética (ex.: protocolos de segurança e controle de acesso aos dados).

Sub-parâmetro (f): não atendido. A informação sobre controle de acessos não consta em nenhum documento público.

Sub-parâmetro (g): atendido. O item "6. Os meus dados são compartilhados?" apresenta categorias gerais de terceiros com quem a Oi poderá compartilhar dados do titular.

---

[15] https://www.naomeperturbe.com.br/

[16] Acessível em: https://www.oi.com.br/static/sobre-a-oi/politica-de-seguranca-informacao/politica-da-seguranca-da-informacao.pdf

Sub-parâmetro (h): integralmente atendido. O item "6.Os meus dados são compartilhados?" apresenta as finalidades de compartilhamento com terceiros, especificadas conforme as categorias gerais de terceiro.

Sub-parâmetro (i): parcialmente atendido. O item "8. Onde meus dados são salvos?" nos informa que há transferências internacionais para fins de retenção de dados pela Oi. Não há descritivo de todas as hipóteses de transferência internacional e suas finalidades em nenhum documento público. Também não encontramos informações sobre a localidade de armazenamento destes dados.

Em relação ao **parâmetro IV**, relacionado às informações sobre direitos de titular, consideramos o seguinte:

Sub-parâmetro (a): atendido. A Oi possui uma página de Direitos de Privacidade[17] com todas as informações de contato necessárias para exercício dos direitos.
Os Contratos para adesão aos planos de Banda Larga da Oi também trazem redação com garantia de não-discriminação:

"Direitos do assinante: [...] 8.1 Receber tratamento não discriminatório quanto às condições de acesso e fruição do SERVIÇO BANDA LARGA COM FIBRA DA OI;"

Sub-parâmetro (b): atendido.

Em relação ao **parâmetro IV**, relacionado às respostas da Oi a respeito dos direitos de titular, consideramos o seguinte:

Sub-parâmetro (a): parcialmente atendido. A Oi possui uma página de Formulário de Direitos[18], onde Clientes e Ex-Clientes podem solicitar os direitos de (i) não recebimento de ofertas; (ii) direito de exclusão/anonimização; ou (iii) direito de acesso. No entanto, os não clientes podem apenas exercer o direito de não recebimento de ofertas - sem possibilidade de exercer seus outros direitos assegurados pela LGPD.

Embora o Aviso de Privacidade da Oi redirecione o usuário ao Formulário para exercício dos direitos de confirmação da existência de tratamento e acesso (art. 18, I da LGPD) e portabilidade dos dados (art. 18, V) não é possível exercer estes direitos por meio da página indicada.

O pedido feito por meio do chatbot "Joice" (via Whatsapp) (no dia 13 de outubro de 2022) apenas resulta no redirecionamento ao Portal da Privacidade, sem possibilidade do efetivo exercício do direito de titular de confirmação de existência de tratamento ou acesso. Tentamos contato com o Encarregado de Dados da Oi por e-mail (pp-privacidade@oi.net.br) mas, novamente, fomos redirecionados ao Portal de Privacidade - não havendo satisfação do pedido de informações.

Sub-parâmetro (b): atendido integralmente. A página de Direitos de Privacidade fornece claramente um descritivo dos direitos do titular de dados.

---

[17] https://www.oi.com.br/direitos-privacidade/?_gl=1*ntvb1p*_gcl_dc*R0NMLjE2NjUxNjY4MzYuQ0xpRi0temR6dm9DRlI2cmxRSWRtZ2tPZXc.
[18] https://privacyportal-br.onetrust.com/webform/baeb1383-62f2-491c-b2e4-f232ee6ddd1e/b827d324-036c-4969-9e8e-72f0a0d8a7c5

Em relação ao **parâmetro VI**, relacionado à atualização da política de privacidade, consideramos o seguinte: **atendido integralmente**. O Aviso de Privacidade da Oi estabelece que os clientes da Oi serão informados diante de qualquer alteração na página..

Além disso, os Contratos para adesão aos planos de Banda Larga da Oi trazem a seguinte redação:

"Direitos do assinante: [...] 8.3 Ter conhecimento de qualquer alteração nas condições de prestação do SERVIÇO BANDA LARGA COM FIBRA DA OI que lhe atinja direta ou indiretamente, mediante acesso ao site www.oi.com.br."

Em relação ao **parâmetro VII**, relacionado à acessibilidade, consideramos o seguinte: **integralmente atendido**. O Portal da Privacidade[19] possui diversos documentos em linguagem clara e acessível para compreensão do titular a respeito do tratamento de seus dados e seus direitos. O Regulamento da Oferta que integra o Contrato de Adesão à Banda Larga da Oi possui cláusula de proteção de dados pessoais, definindo responsabilidades para a Oi na qualidade de controladora de dados e mencionando as Políticas de Privacidade e Proteção de Dados disponibilizadas no site da Oi.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ★

Nesta categoria, a Oi obteve **estrela cheia**, pois atendeu a quatro dos possíveis cinco parâmetros estabelecidos pela Categoria 2.

Em relação ao **parâmetro I**, consideramos o seguinte: parcialmente atendido. O Protocolo de Entrega de Dados a Autoridades Públicas da Oi especifica o procedimento de recebimento de pedidos de acesso a dados, análise de competência do requisitante e atendimento da solicitação ou contestação do pedido. Nele, podemos ver que a empresa fornece dados cadastrais sem necessidade de ordem judicial a Delegacias de Polícia, Ministério Público, Advocacia Geral da União e Autarquias (as chamadas "Autoridades Públicas") "conforme autorizado em lei". Porém, não há descritivo das hipóteses legais específicas que permitem o compartilhamento de dados cadastrais com cada uma das autoridades mencionadas (ou seja, não há meios de avaliar a legalidade das hipóteses em que a Oi compartilha dados sem ordem judicial).

Em relação ao **parâmetro II**, consideramos o seguinte: não atendido. A empresa descreve a possibilidade de fornecimento de dados cadastrais sem ordem judicial às Autoridades Públicas, não exclusivamente no atendimento de demandas relacionadas aos crimes descritos nos dispositivos da Lei 12.850/13, da Lei 9.613/98 e o artigo 13-B do CPP.

Em relação ao **parâmetro III**, consideramos o seguinte:

Sub-parâmetro (a): parcialmente atendido. Não há informação sobre a divulgação de dados de geolocalização em tempo real às Autoridades.

[19] https://www.oi.com.br/aviso-de-privacidade/

Sub-parâmetro (b): integralmente 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.

Sub-parâmetro (c): integralmente 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.

Em relação ao **parâmetro IV**, consideramos o seguinte: integralmente atendido. Segundo o Protocolo de Entrega de Dados a Autoridades Públicas da Oi, os registros de conexão são fornecidos apenas diante ordem judicial, segundo o Marco Civil da Internet.

Em relação ao **parâmetro V**, consideramos o seguinte: integralmente atendido. O Protocolo de Entrega de Dados a Autoridades Públicas da Oi especifica, de maneira clara e acessível, o procedimento de recebimento de pedidos de acesso a dados, análise de competência do requisitante e atendimento da solicitação ou contestação do pedido.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: ★

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

Quanto ao **parâmetro I**, referente à contestação de legislação, realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte.

Em 29/03/2022, o STF publicou o julgamento da Ação Direta de Inconstitucionalidade número 4924/DF[20], onde a Associação Nacional das Operadoras Celulares - ACEL, da qual a Oi faz parte, pediu pela declaração de inconstitucionalidade da Lei 17.107/12, do Estado do Paraná, que dispõe sobre penalidades ao responsável pelo acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres (trote telefônico). A lei visava estabelecer obrigação às operadoras de telefonia de fornecer os dados dos proprietários de linhas telefônicas que acionem indevidamente os serviços de atendimento diante de mero ofício por qualquer órgão ou instutuição pública envolvida. A ACEL argumentou em falor da inviolabilidade da intimidade, vida privada horna e do sigilo das comunicações telefônicas (segundo estabelecido no artigo 5º, incisos X e XII da Constituição Federal), mencionando a indisponibilidade do direito à proteção de dados pessoais em sua argumentação.

[20] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183

Além disso, a ACEL havia ajuizado a ADI 5040/PI[21], publicada em 2021 (não incluída em nosso relatório anterior), onde questionava a legalidade da Lei Nº 6.336/2013 do Estado do Piauí, que obrigava as empresas prestadoras de serviço de telefonia móvel pessoal a fornecerem, aos órgãos de segurança pública, dados relativos à localização de telefones celulares e cartões "SIM" que tivessem sido objeto de furto, roubo e latrocínio ou utilizados na prática de delitos. Entre seus argumentos, a ACEL também alegou grave ofensa à privacidade de seus clientes na hipótese de divulgação das informações pessoais, citando a Constituição e o direito fundamental à privacidade, além da inviolabilidade dosigilo telefônico.

Por fim, para averiguação do **parâmetro II**, referente à contestação de pedidos abusivos, 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 21/06/2021 e 19/10/2022. Encontramos diversas ações onde a Oi contestou pedidos de dados de seus clientes pela falta de ordem judicial determinando a entrega dos dados[22].

Por exemplo, encontramos, no relatório do acórdão referente ao Processo 1058034-44.2020.8.26.0100:

"A corré OI Movel S.A habilitou-se nos autos e trouxe juntou documentos (fls. 370/417). Apresentou contestação (fls. 430/440) alegando que não se nega a prestar informações, ***observada a determinação judicial necessária para a quebra do sigilo de dados, garantido constitucionalmente****, pelo que pugna pelo afastamento da condenação sucumbencial. "*

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, a Ação Direta de Inconstitucionalidade (ADI) 5642[23], da ACEL, não foram consideradas, já que não registraram movimentações relevantes em vista da suspensão do julgamento e pedido de vista pelo Ministro Nunes Marques (em 17/06/2021).

Além disso, a Oi nos forneceu mais ações judiciais onde contesta os pedidos de acesso a dados por autoridades legais na fase de discussão dos relatórios preliminares deste projeto.

CATEGORIA 4: Postura pública pró-privacidade

---

[21] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4461936

[22] É o caso do Processo 1058034-44.2020.8.26.0100, acesso em: http://www.dje.tjsp.jus.br/cdje/consultaSimples.do?cdVolume=15&nuDiario=3242&cdCaderno=15&nuSeqpagina=1

[23] A Associação Nacional das Operadoras Celulares (Acel), da qual algumas operadoras fazem parte, ajuizou a Ação Direta de Inconstitucionalidade (ADI) 5642, no Supremo Tribunal Federal (STF), para impugnar dispositivo da Lei 13.344/2016, que confere a delegados de polícia e membros do Ministério Público a prerrogativa de requisitar informações e dados necessários à investigação criminal nos casos de tráfico de pessoas, independentemente de autorização judicial. A ACEL pede a concessão de liminar para que o STF dê à Lei 13.344/2016 interpretação conforme a Constituição Federal de modo a impedir entendimento que leve a medidas como interceptação telemática e de voz, localização de terminal ou IMEI (Identificação Internacional de Equipamento Móvel) de cidadão em tempo real por meio de ERB, extrato de ERB, dados cadastrais de usuários de IP, extratos de chamadas telefônicas e SMS, entre outros dados de caráter sigiloso. No mérito, pede a declaração de inconstitucionalidade parcial do dispositivo questionado.

Resultado: ★

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

O **parâmetro I**, relativo ao posicionamento em geral da empresa, foi considerado atendido.

Identificamos algumas ações públicas da Oi voltadas à promoção da proteção de dados pessoais no Brasil. Por exemplo, a Oi lançou a Oi Soluções, que presta serviços de consultoria de adequação LGPD às empresas[24].

A Oi lançou, em 2021, seu Programa Privacidade e o Programa de Conformidade, que, segundo o Relatório de Sustentabilidade, resultou em pelo menos quatro eventos para liderança e 15 peças de comunicação para a empresa, "*impactando mais de 10 mil colaboradores, a fim de disseminar ainda mais o tema de privacidade".*

Além disso, a Oi participou, por meio da Conexis, do lançamento do Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações, apresentado à Autoridade Nacional de Proteção de Dados[25].

Como parte do Programa de Educação e Comunicação "Pessoas vêm antes de dados", o time de Privacidade da Oi, em parceria com o Oi Futuro, também realizou 3 oficinas de Privacidade para jovens da Rede Pública Estadual de Pernambuco, cerca de 200 estudantes das Escolas Técnicas Estaduais Cícero Dias, Nave Recife e Porto Digital[26].

Além disso, a Encarregada de Dados e o time de privacidade da Oi realizaram um evento com alunos da escola NAVE para a discussão de tópicos de proteção de dados pessoais.[27]

Consideramos o **parâmetro II** integralmente atendido.

Segundo diversas reportagens, a Oi tem tido participação ativa na promoção da tecnologia de reconhecimento facial nos últimos anos. Em 2018, por exemplo, a Oi constituiu uma parceria com a Huawei voltada à comercialização de câmeras de reconhecimento facial[28]. Em 2019, a Oi anunciou sua tecnologia de videomonitoramento inteligente aplicado à prevenção de fraudes bancárias e "situações de risco"[29]. Segundo a matéria, a ferramenta contra fraude bancária "usa um banco de imagens com dezenas de milhões de usuários únicos para garantir que a mesma pessoa não tem mais de uma conta ou CPF. O recurso pode ser usado pelos bancos no momento de abertura de contas, para completar transações e autorizar pagamentos". No mesmo ano, a Oi em parceria com a Secretaria de Segurança

---

[24] Acesso em: https://www.oi.com.br/grandes-empresas/seguranca/consultoria-lgpd/

[25]Acesso em: https://www.telesintese.com.br/operadoras-criam-codigo-de-boas-praticas-de-protecao-de-dados/

[26] Acesso em: https://www.linkedin.com/posts/oioficial_pessoasvemantesdedados-cidadaniadigital-nave-activity-6975897567792381952-UL5I?utm_source=share&utm_medium=member_desktop

[27] Acesso em: https://www.oi.com.br/transparencia-em-privacidade/

[28] Acesso em: https://www1.folha.uol.com.br/tec/2018/10/chinesa-huawei-faz-parceria-com-oi-para-cameras-de-reconhecimento-facial.shtml

[29] Acesso em:https://canaltech.com.br/ciab/ciab-2019-oi-lanca-recursos-de-reconhecimento-facial-contra-fraudes-bancarias-141591/

Pública do Estado do Rio de Janeiro, anunciou a expansão do videomonitoramento urbano com reconhecimento facial, testada durante o Carnaval, para o Estádio Jornalista Mário Filho, o Maracanã[30].

Mais recentemente, em 2022, a Oi Soluções entregou à Secretaria de Segurança Pública da Bahia (SSP-BA) um projeto de videomonitoramento inteligente (novamente com a possibilidade de reconhecimento facial), voltado à transmissão de imagens em tempo real entre os centros integrados, policiais e viaturas[31]. Na fase de discussão do relatório, a Oi nos informou que o papel da empresa nessas situações limita-se ao oferecimento de conectividade à internet – não sendo a empresa em si operadora da tecnologia de videomonitoramento.

Ainda, na fase de discussão dos relatórios preliminares, **a Oi nos informou que não realiza reconhecimento facial para fins de cadastro ou acesso aos serviços de telefonia móvel** - o que consideramos como um diferencial.

A Oi também enviou alguns exemplos de manifestações públicas relacionadas à importância de elaboração de Relatórios de Impacto pelas entidades públicas contratantes de serviços de reconhecimento facial - que, contudo, não foram identificadas em processos publicamente acessíveis pela internet.

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

Resultado: 

Nesta categoria, a Oi obteve **três quartos de estrela**, pois atendeu a três dos cinco parâmetros analisados.

Em relação aos **parâmetros I, II e III**, consideramos o seguinte: integralmente atendido. A Oi possui um Canal de Transparência em Privacidade[32] facilmente acessível e em linguagem clara, onde detalha a jornada de adequação à LGPD e os passos dados para a garantia de direitos dos titulares de dados. O Relatório de Sustentabilidade traz a informação de que:

"No que diz respeito aos direitos dos titulares, em 2021, a Oi recebeu e respondeu mais de 500 pedidos, destacando-se: solicitação de não recebimento de ofertas (37%), pedido de exclusão de dados (33%), confirmação de tratamento (14%), bem como acesso e portabilidade (8%)."

.

O Relatório também traz informações sobre o número de pedidos relacionados a violações de direitos:

[30] Acesso em: https://www.telesintese.com.br/oi-implanta-videomonitoramento-com-reconhecimento-facial-no-maracana/

[31] Acesso em: https://www.minhaoperadora.com.br/2022/06/oi-entrega-12-mil-cameras-de-reconhecimento-facial-e-leitura-de-placas-a-ssp-ba.html

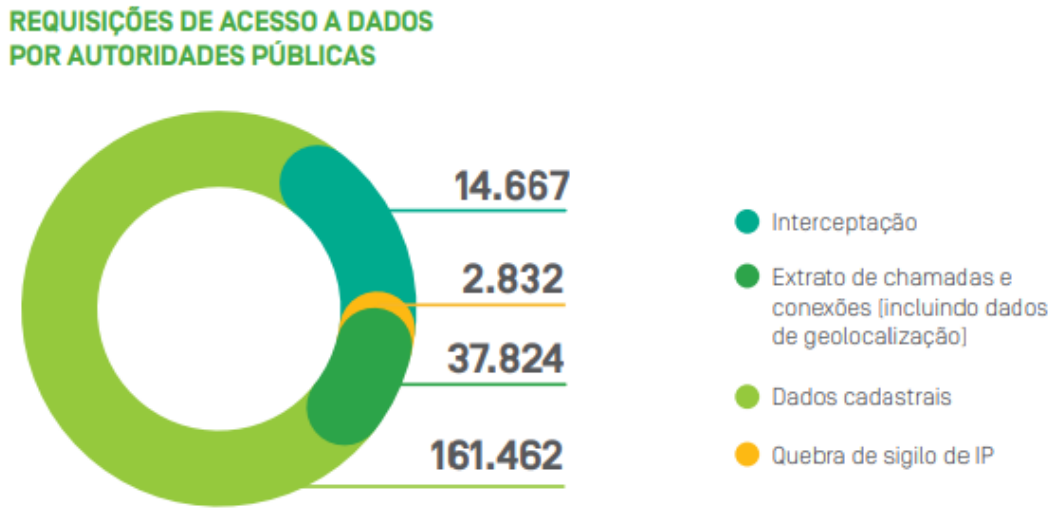
[32] https://www.oi.com.br/transparencia-em-privacidade/

"Para além do Programa Oi de Privacidade, no que concerne o recebimento de ofícios, procedimentos administrativos e judiciais, em 2021, constatou-se uma queda significativa (26%) do número de reclamações pelos canais da Anatel sobre utilização indevida de dados cadastrais, em comparação com o ano de 2020, reduzindo de 2.438 para 1.804 conforme detalhado no quadro a seguir."

"Em relação a ofícios, a Oi recebeu ao todo 8 procedimentos em 2021 de autoridades públicas, dos quais dois encontram-se arquivados, sendo os principais questionamentos: •Suposto compartilhamento de dados para outras empresas; •suposto vazamento de dados de clientes; •esclarecimentos sobre medidas/ recomendação para contenção de vazamento de dados e cumprimento da LGPD; e •esclarecimentos sobre solicitação de dados pessoais para verificação de viabilidade de serviço."

Em relação ao **parâmetro IV** consideramos que foi parcialmente atendido. A Oi cumpriu os sub-parâmetros (a) e (b) e não cumpriu o sub-parâmetro (c).

Sub-parâmetro (a): atendido. A Oi publicou, no Relatório de Sustentabilidade 2021, que recebeu 216.785 requisições de autoridades públicas para acesso a dados, tendo recusado 1% dos pedidos, ou seja, por volta de 21 mil pedidos:



"Com o intuito de respeitar a privacidade de nossos clientes e preservar os sigilos das comunicações, a companhia possui protocolos para análise de pedidos de acesso a dados, que inclui avaliação da autoridade solicitante, tipo de solicitação, competência do juízo em casos de ordem judicial, data da emissão e adequação a requisitos legais, ***sendo contestadas cerca de 1% das requisições.*** *Especificamente em relação aos pedidos de interceptação, em 2021, foram apresentados 18 Habeas Corpus em 2021 em razão da manutenção de pedidos considerados ilegais, dentre os quais 06 ordens foram concedidas, 10 negadas e 02 encontram-se pendentes de julgamento."*

Sub-parâmetro (b): atendido. A Oi publica a discriminação de pedidos de dados para as categorias de "interceptação telefônica", "dados cadastrais", "extratos de chamadas e conexões (incluindo dados de geolocalização" e "quebra de sigilo de IP".

Sub-parâmetro (c): não atendido. Não há informações sobre o número de contas afetadas pelos pedidos de acesso por ordem judicial.

Em relação ao **parâmetro V** consideramos o seguinte: não atendido. Não obtivemos acesso aos Relatórios de Impacto produzidos pela Oi. O Relatório de Sustentabilidade, no entanto, traz a informação de que a Oi já formalizou um modelo de RIPD com o qual trabalha para avaliações internas de risco de proteção de dados.

"Cabe destacar que em 2021 foi formalizado nosso primeiro Relatório de Impacto à Proteção de Dados Pessoais, através do qual foram identificados riscos em relação aos direitos dos titulares atrelados aos princípios da LGPD (finalidade, adequação e retenção) e o direito fundamental à privacidade. Após serem avaliados os riscos, foram propostas e implementadas diversas medidas mitigatórias visando a conformidade e maior controle dos titulares sobre seus dados. Ao considerar aspectos de privacidade desde a concepção de novos produtos, mais do que o atendimento à legislação, a Oi busca contribuir com o despertar da sociedade para o cuidado com dados pessoais, bem como para o empoderamento das pessoas."

CATEGORIA 6: Notificação do usuário

Resultado: ☆

A Oi não obteve estrela, pois não há menção à possibilidade de notificação do usuário em qualquer um dos documentos analisados.

TIM

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

A Tim Banda Larga atende integralmente ao **parâmetro I:**

Sub-parâmetro (a): atendido. Em sua Política de Privacidade, na seção "Que tipo de Dados e com qual finalidade a TIM trata", a empresa apresenta uma tabela em que especifica a origem, o tipo de dado coletado, a finalidade e a base legal de tratamento de diversos dados pessoais processados por ela:

Origem	Tipo de dados coletados	Finalidade	Base legal coletados
Navegação no Site e no aplicativo Meu TIM	Dados de Navegação (IP, data e hora) e Dados do Dispositivo de Acesso (e.g. IMEI, modelo do dispositivo, etc)	**Funcionamento do Site:** ativar funcionalidades essenciais, como software antivírus, adaptar o conteúdo ao formado da tela, entre outras funções.	Legítimo Interesse
		Obrigação Legal: cumprir com as obrigações legais de guarda de IP, data e hora de acesso ao nosso Site.	Cumprimento de Obrigação Legal
		guarda de IP, data e hora de acesso ao nosso Site.	
		Analytics: compreender o seu comportamento de navegação e como o Site e App está sendo usado, para	

Captura de tela em: 13/10/2022

Dentre outros, a empresa informa, na tabela, que coleta:

> Dados de Navegação (IP, data e hora) e Dados do Dispositivo de Acesso (e.g. IMEI, modelo do dispositivo, etc); Dados de Cadastro: email, nome, telefone e modelo do dispositivo móvel; Dados de Navegação e Dados do Dispositivo de Acesso; Dados biométricos faciais (como fotografia fornecida pelo usuário e foto de seu documento); Dados locacionais (país, cidade e estado) de onde ocorreu o acesso ou onde a ligação está ocorrendo; registros de telefonia e de envio de SMS e MMS; desempenho da rede e da infraestrutura de telecomunicações; Dados sobre pagamento: números e dados de cartão de crédito, transações de recargas, informações bancárias necessárias para

> prestação de serviços; informações de crédito para os sistemas de tarifação e emissão de faturas. Informações sobre atendimentos na central de atendimento, chat de atendimento ou outros canais de atendimento; Dados do perfil (tais como gênero, idade, geolocalização aproximada, plano contratado, recargas realizadas, se aplicável, uso de aplicativos (via SDK), modelo do aparelho); Dados de cadastro (como nome, telefone, data de nascimento, e-mail, nome da mãe, CPF, gênero, documentos de identificação, telefone de contato e endereço).

Sub-parâmetro (b): atendido. No mesmo item referenciado acima, a empresa especifica a origem dos dados coletados. Aponta, por exemplo, quais dados são coletados na "Navegação no Site e no aplicativo Meu TIM", nos "Formulários do Site e dos aplicativos Meu TIM", no "Uso dos Serviços e do Aplicativo Meu TIM", no "Uso dos Serviços", nos "Formulários de Cadastro nos Pontos de Venda", dentre outros.

Sub-parâmetro (c): atendido. Em sua Política de Privacidade, no item "Como a TIM coleta os seus Dados Pessoais", a empresa informa que os dados podem ser coletados publicamente através do Site.

Sub-parâmetro (d): atendido. A empresa divulga em sua Política de Privacidade, bem como em sua informativa "Como a TIM compartilha dados pessoais com terceiros", algumas categorias de terceiros que compartilham dados com a empresa, o que foi considerado suficiente para atender o sub-parâmetro.

Sub-parâmetro (e): atendido. A empresa informa no documento "Quem tem acesso aos seus dados pessoais" que:

> nossos parceiros e fornecedores assinam contratos com cláusulas de confidencialidade e de Privacidade e Proteção dos Dados Pessoais que venham a ter acesso, além de participarem, em conjunto com os colaboradores TIM, de treinamentos de conscientização sobre a Lei Geral de Proteção de Dados.

Além disso, a empresa também informa, no documento "Como a TIM compartilha seus dados pessoais com terceiros", de forma detalhada as exigências para com os terceiros relativamente ao tratamento de dados pessoais.

Quanto ao parâmetro II, referente à informação sobre finalidade, foi considerado cumprido:

Sub-parâmetro (a): atendido. No item "Que tipo de Dados e com qual finalidade a TIM trata", a empresa tabela que especifica as finalidades para o tratamento de dados efetuado por ela.

Sub-parâmetro (b): atendido. No mesmo item acima referenciado, há explicação detalhada acerca da forma da utilização dos dados, como no item sobre dados cadastrais, em que se explicita a utilização desses dados para, por exemplo, "recuperar senha do Meu TIM Empresas".

Quanto ao **parâmetro III**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais foi considerado cumprido. Neste parâmetro, foram considerados atendidos os sub-parâmetros (a), (b), (c), (d), (e), (f), (g), (h) e (i).

Sub-parâmetro (a): atendido. Em sua Política de Privacidade, no item "Por quanto tempo os Dados serão armazenados", a empresa estabelece:

> Nós manteremos seus Dados Pessoais somente pelo tempo que for necessário para cumprir com as finalidades para as quais os coletamos, inclusive para fins de cumprimento de quaisquer obrigações legais, contratuais, de prestação de contas ou requisição de autoridades competentes.
> Para determinar o período de retenção adequado para os Dados Pessoais, além do prazo prescricional, consideramos 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 tais propósitos por outros meios, e os requisitos legais aplicáveis. Por exemplo, por obrigação imposta pelo Marco Civil da Internet, os Dados relacionados a IP, data e hora das suas conexões à internet, quando a TIM for responsável por prover este acesso, serão mantidos por, no mínimo, 12 meses e referente aos aplicativos criados pela Tim, por, no mínimo, 6 meses.

Neste documento, a empresa estabelece tempos mínimo e máximo de armazenamento dos dados, bem como maiores esclarecimentos quanto a necessidade de armazenamento de dados pessoais para cumprimento de obrigações legais, regulatórias, contratuais, de prestação de contas, requisição de autoridades competentes ou outras previstas na legislação vigente, inclusive com exemplos concretos de períodos de armazenamento e suas respectivas obrigações legais.

Quanto ao local de armazenamento, a empresa informa em sua Política de Privacidade, no documento "Onde e por quanto tempo a TIM armazena seus dados", onde os dados são armazenados: (i) datacenters da TIM localizados em São Paulo e Rio de Janeiro; (ii) armazenamento por terceiros, contando com medidas de segurança para tal. A empresa, por fim, indica que na hipótese de transferência internacional, os dados serão armazenados na AEE (Área Econômica Europeia) e na Califórnia (EUA).

Sub-parâmetro (b): atendido. Na seção "Onde e por quanto tempo a TIM armazena seus Dados" a empresa informa que mantém os dados pelo prazo máximo de 11 anos, a contar do término da relação contratual entre a empresa e o titular.

Sub-parâmetro (c): atendido. No documento "Onde e por quanto tempo a Tim armazena seus dados", a empresa indica, não exaustivamente, algumas hipóteses de retenção dos dados.

Sub-parâmetro (d): atendido. No Contrato de Prestação de Serviços Live TIM, a empresa se compromete a observar práticas de segurança:

> 19.2 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, no Contrato de Prestação do Serviço Móvel Pessoal Pós-Pago, a empresa também se compromete a observar práticas de segurança:

> 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.

Ao prestar algumas informações em relação aos colaboradores e fornecedores que têm acesso aos dados, considerou-se que as informações dadas eram suficientes.

Sub-parâmetro (e): atendido. Em seu Relatório de Sustentabilidade 2021, p. 316, a empresa esclarece:

A TIM também tem aprimorado a governança nesse processo, com novos procedimentos, controles e investimentos na prevenção, tratamento de incidentes e equipes de monitoramento. A Companhia conduz suas atividades com base na ISO 27001 – norma internacional que descreve as melhores práticas para a gestão de segurança da informação – e NIST (Cyber Security Framework) que apoia a gestão e redução do risco de segurança cibernética. Em 2020, foi realizada uma avaliação dos requisitos de certificação, identificando um nível de conformidade superior a 90% dos requisitos, e os ajustes necessários para obter a certificação serão feitos até 2022.

Sub-parâmetro (f): atendido, já que a empresa afirma que somente pessoas autorizadas, e fornecedores sob cláusulas de confidencialidade, podem ter acesso aos dados. Mesmo que informações mais detalhadas sobre quais funcionários podem acessar os dados poderiam ter sido fornecidas, a menção específica às informações de cadastro e aos dados de comunicação, e a menção aos fornecedores, indicam para a existência de padrões mais claros em relação a tais acessos, razão pela qual o sub-parâmetro foi considerado cumprido.

Sub-parâmetro (g): atendido. Em sua Política de Privacidade, no item "Com quem a TIM compartilha os seus Dados", a empresa especifica com que terceiros fará o compartilhamento, apontando, por exemplo, empresas de "serviços de tecnologia", "análise de desempenho", "pesquisas de mercado", dentre outros.

Em seu Portal de Transparência, a empresa disponibiliza um documento intitulado "Como a TIM usa dados pessoais para direcionar materiais publicitários de terceiros?" a empresa informa que compartilha apenas informações anonimizadas com parceiros comerciais:

> Em alguns casos, a TIM pode utilizar certas informações relacionadas às suas preferências e hábitos com a TIM, para entender que tipo de produto ou serviço de nossos parceiros comerciais podem ser de maior interesse a você. Quando fazemos isso, nós buscamos entender os seus gostos e o seu perfil e, com isso, selecionamos produtos e serviços de alguns de nossos parceiros que imaginamos que possam ser do seu interesse, para direcionar certos materiais publicitários.

Ainda, no documento "Como a TIM compartilha dados pessoais com terceiros?", a TIM informa, genericamente, o procedimentos adotados no compartilhamento de dados:

> Os materiais publicitários podem se referir a produtos e/ou serviços oferecidos pelos parceiros em conjunto com a TIM, ou, ainda, de produtos e/ou serviços próprios dos parceiros. No primeiro caso, não precisamos revelar a sua identidade aos nossos parceiros, ou seja, em regra, não compartilhamos seus dados com eles nessas situações. No segundo caso, pode ser que seja necessário o compartilhamento de seus dados pessoais; contudo, nessa hipótese, sempre que exigido pela legislação aplicável, coletaremos o seu consentimento.
> Sempre nos limitamos a usar o mínimo de informações possível e queremos, acima de tudo, manter você informado sobre os melhores produtos e serviços que podem ser úteis para você. Mesmo assim, se você não quiser receber esse tipo de comunicação publicitária, acesse a nossa Central de Privacidade para requerer a interrupção desse serviço.

Tais informações foram consideradas suficientes para informar sobre o compartilhamento.

Sub-parâmetro (h): atendido. Isso porque, no mesmo trecho da Política de Privacidade, no item "Com quem a TIM compartilha os seus Dados", a empresa especifica as finalidades dos compartilhamentos, apontando, dentre outros:

> "Serviços de Tecnologia: Temos uma série de fornecedores que precisamos contratar para operar os Produtos e oferecer os Serviços, e alguns deles podem tratar em nosso nome os Dados Pessoais que coletamos. Por exemplo, usamos serviços de hospedagem de dados para armazenar a nossa base de dados, usamos também serviços de meios de pagamento para poder processar os dados de faturamento dos nossos Serviços.
> (...)
> Análise de desempenho: Os dados armazenados pela TIM podem vir a ser coletados por tecnologia de terceiros e utilizados para fins de estatísticas (analytics), com a finalidade de a TIM compreender quem são as pessoas que utilizam seus Serviços, visitam seu Site e o Aplicativo Meu TIM ou de qualquer forma interagem com a TIM.
> (...)
> Pesquisas de mercado: Caso você responda a uma pesquisa de mercado enviada pela TIM, é possível que os resultados sejam compartilhados com nosso parceiro responsável por tal pesquisa."

Sub-parâmetro (i): atendido. No documento "Onde e por quanto tempo a TIM armazena seus dados", a empresa dedica um item, "Transferências internacionais", em que explica as hipóteses de transferência internacional:

> Para a prestação de serviços de roaming internacional;
> • Para a utilização de ferramentas gerenciadas e de propriedade

> de fornecedores, em atividades de execução de atos societários ou relações com investidores, por exemplo;
> • Quando há a contratação de serviços de hospedagem, em que os servidores do fornecedor contratado estão localizados no exterior; e
> • Quando a TIM contrata algum fornecedor relevante para a prestação dos seus serviços, que necessita tratar os seus dados pessoais no exterior.

O **parâmetro IV,** que avalia se a empresa divulga informações acerca dos direitos dos titulares, foi considerado atendido.

Sub-parâmetro (a): atendido. A empresa disponibiliza e-mails, em sua Política de Privacidade, para que o titular possa exercer seus direitos.

Sub-parâmetro (b): atendido. A empresa dedica um item em sua Política de Privacidade, "Quais são os direitos dos Titulares de Dados", em que explica, na forma de uma tabela, quais são os direitos do titular. Nessa tabela, há uma coluna em que se explica qual o conceito por trás de cada direito.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, não foi considerado atendido. A empresa não respondeu dentro do prazo ao pedido feito pelo titular de dados.

O **parâmetro VI**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado atendido. Em sua Política de Privacidade, a empresa afirma:

> 10. Como e quando esta Política pode ser alterada
> 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.

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado atendido. A empresa tem um Portal de Privacidade[33] com as principais informações de privacidade e proteção de dados:

[33] https://www.tim.com.br/sp/sobre-a-tim/institucional/seguranca/politica-de-privacidade

Captura de tela: 13/10/2022

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ★

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

Quanto ao **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado cumprido. No documento "Como a Tim compartilha dados pessoais com terceiros?",

> Além disso, a TIM está sujeita a diversas obrigações legais e regulatórias que fazem com que certos compartilhamentos de dados com terceiros, inclusive autoridades, seja necessário. Em muito casos, a TIM também é obrigada a atender a ordens expedidas por autoridades para fornecer certos dados, especialmente em investigações. Sempre protegeremos os seus direitos e apenas forneceremos os dados que sejam legalmente requisitados com fundamentos jurídicos válidos.

No documento "Como é realizado o compartilhamento de dados pessoais em caso de investigação?", disponibilizado no Portal de Privacidade da empresa, oferece um rol exemplificativo de autoridades administrativas que podem requisitar dados, além das hipóteses fundamentadas em ordens judiciais:

> 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 de autoridades administrativas dotadas de competência para requisições incluem Promotores dos Ministérios Público Militar, Estadual e Federal; Delegacias de Polícias Civil, Federal e Legislativa, presidência de CPI (Comissão Parlamentar de Inquérito), além das hipóteses fundamentadas em ordem judiciais.

As informações que constam no referido foram consideradas suficientes para informar aos usuários sobre as hipóteses de compartilhamento de dados com o Estado; por isso, o parâmetro foi considerado atendido.

O **parâmetro II**, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, foi considerado atendido. No documento "Como é realizado o compartilhamento de dados pessoais em caso de investigação?" informa os critérios analisados para a atender à solicitação de acesso a dados; os casos mais comuns de solicitação de dados; e apresenta um rol exemplificativo de hipóteses legais no âmbito dos quais a requisição pode ocorrer:

> 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.
>
> (...)
>
> Não é possivel a apresentação de todas as hipóteses que podem fundamentar ordem judicial, pedido extrajudicial ou solicitação, bem como as autoridades competentes, que podem requerer tais dados pessoais, visto que tais ordens devem fundamentar-se em leis que estabeleçam essa possibilidade.
>
> 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.
>
> Destacamos, no entanto, que o compartilhamento de dados e as finalidades exemplificadas não são um rol taxativo, sendo analisado cada pedido concreto, seguindo os procedimentos mencionados nessa Informativa.

> Também à título de exemplo, apresentamos alguns desses fundamentos legais mais comuns:
> • Constituição Federal Brasileira, sobretudo seu artigo 5º, X a XII.
> • Lei nº 9296/1996 – Lei que regula a interceptação legal
> • Lei nº 9472/1997 – Lei Geral de Telecomunicações
> • Resolução nº 477/2007 – Regulamentação do Serviço Móvel Pessoal – SMP
> • Lei nº 12.830/2013 - Sobre a investigação criminal por delegado de polícia
> • Lei nº 12.850/2013 – Lei de Organizações Criminosas
> • Lei nº 12.965/2014 - Marco Civil da Internet
> • Decreto nº 8.771/2016 - Regulamentador do Marco Civil da Internet
> • Lei nº 12.683/2012 – Lei Lavagem de Dinheiro
> • Lei nº 13.344/2016 – Tráfico de Pessoas
> • Lei nº 15.292/2014 – Lei de Busca de Pessoas Desaparecidas

Tais informações foram consideradas suficientes para esclarecer aos titulares

Ainda, no Contrato de Prestação de Serviços Live, a empresa informa que nos casos de crimes contra crianças e adolescentes, previstos no ECA, a TIM poderá oferecer todos os dados cadastrais do cliente às autoridades judiciais, nos termos do Marco Civil da Internet. A empresa identifica, portanto, tanto o crime, quanto a autoridade competente. Tal informação foi considerada suficiente para fins de avaliação.

> **Contrato de Prestação de Serviços Live**
> 14.1 (g) unilateralmente pela TIM, caso seja constatada a utilização do serviço para prática de atos criminosos, notadamente crimes contra crianças e adolescentes previstos no Estatuto da Criança e do adolescente e demais legislações aplicável a espécie, resguardando o direito de a TIM buscar a eventual reparação por perdas e danos em face do CLIENTE caso tenha sido acionada por terceiros prejudicado, no âmbito de demandas cíveis ou criminais que suscitem a responsabilidade pela pratica de tais atos ofensivos, através do TIM LIVE, sendo, inclusive, facultado à TIM fornecer todos os dados cadastrais do CLIENTE as autoridades judiciais na forma da lei 12.965/2014 para apuração do ilícito e devida responsabilização do autor das ofensas.

O **parâmetro III**, referente ao oferecimento de informações sobre dados de geolocalização, foi considerado atendido. No documento "Como é realizado o compartilhamento de dados pessoais em caso de investigação?", a empresa informa que, em regra, os dados de geolocalização só podem ser requisitados por meio de ordem judicial e esclarece sobre as hipóteses restritas em que o Ministério Público e pelo delegado de polícia podem realizar a requisição:

> 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.

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, foi considerado atendido. A empresa informa, no documento "Como é realizado o compartilhamento de dados pessoais em caso de investigação?", que a solicitação de registros de conexão só ocorre mediante ordem judicial (vide trecho acima).

Por fim, o **parâmetro V**, relativo à existência de protocolos específicos sobre entrega de dados ao estado, foi considerado atendido. Neste ano, a empresa incluiu em seu Portal de Privacidade o documento intitulado "Como é realizado o compartilhamento de dados pessoais em caso de investigação?", que fornece informações sobre os protocolos, requisitos e hipóteses de entregas de dados para investigações.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: ★

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

Quanto ao **parâmetro I**, referente à contestação de legislação, realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte, e não localizamos quaisquer ações onde a Tim contesta a legislação relacionada aos procedimentos de entrega de dados ao judiciário. Ressaltamos que nossa busca, por questões de escopo e tempo, não buscou por ações do tipo nos tribunais estaduais, relativas, portanto, a legislações ou interpretação de legislações de âmbito estadual. As empresas têm a possibilidade de, durante a fase de discussão dos parâmetros e troca de documentos, comprovar sua atuação nesse sentido.

Em 29/03/2022, o STF publicou o julgamento da Ação Direta de Inconstitucionalidade número 4924/DF[34], onde a Associação Nacional das Operadoras Celulares - ACEL, da qual a Tim faz parte, pediu pela declaração de inconstitucionalidade da Lei 17.107/12, do Estado do Paraná, que dispõe sobre penalidades ao responsável pelo acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres (trote telefônico). A lei visava estabelecer obrigação às operadoras de telefonia de fornecer os dados dos proprietários de linhas telefônicas que acionem indevidamente os serviços de atendimento diante de mero ofício por qualquer órgão ou instutuição pública envolvida. A ACEL argumentou em falor da inviolabilidade da intimidade, vida privada horna e do sigilo das comunicações telefônicas (segundo estabelecido no artigo 5º, incisos X e XII da Constituição Federal), mencionando a indisponibilidade do direito à proteção de dados pessoais em sua argumentação.

[34] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183

Além disso, a ACEL havia ajuizado a ADI 5040/PI[35], publicada em 2021 (não incluída em nosso relatório anterior), onde questionava a legalidade da Lei Nº 6.336/2013 do Estado do Piauí, que obrigava as empresas prestadoras de serviço de telefonia móvel pessoal a fornecerem, aos órgãos de segurança pública, dados relativos à localização de telefones celulares e cartões "SIM" que tivessem sido objeto de furto, roubo e latrocínio ou utilizados na prática de delitos. Entre seus argumentos, a ACEL também alegou grave ofensa à privacidade de seus clientes na hipótese de divulgação das informações pessoais, citando a Constituição e o direito fundamental à privacidade, além da inviolabilidade dosigilo telefônico.

Por fim, para averiguação do **parâmetro II**, referente à contestação de pedidos abusivos, 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 "Tim E sigilo E quebra" e por acórdãos publicados entre 21/06/2021 e 19/10/2022. Encontramos diversas ações onde a Tim contestou pedidos de dados de seus clientes pela falta de ordem judicial determinando a entrega dos dados[36].

Por exemplo, encontramos, no relatório do acórdão referente ao Processo 1042581-72.2021.8.26.0100:

> *"Citada, a corré TIM S/A apresentou contestação às fls. 204/214. No mérito, esclareceu que s**omente por ordem judicial a ré pode quebrar o sigilo de dados cadastrais de seus usuários.** Informou que está obrigada legalmente a armazenar informações atreladas a registros de conexões pelo prazo de 01 ano, a contar da data da utilização do IP, conforme preconiza o art. 13 da Lei nº 12.965/2014. [...] Aguarda a procedência da ação em relação a ela, para determinar que forneça os dados cadastrais dos usuários eventualmente identificados como vinculados aos endereços de IPs de sua responsabilidade, isentando-a de qualquer responsabilidade caso não seja possível identificar o usuário, pois esgotado o prazo legal de armazenamento das informações pleiteadas. Sobreveio réplica (fls. 300/301). É o relatório."*

Na Apelação Cível nº 1073466-74.2018.8.26.0100, encontramos a exigência de que os pedidos de informação devem ser acompanhados da indicação das portas lógicas específicas ao IPs solicitados:

Recorre a TIM S/A. Sustenta ter fornecido os resultados das pesquisas relacionadas há 03 conexões, acompanhada dos dados cadastrais do usuário identificado, sinalizando que, em relação há um dos endereços de IP, não havia sido localizado registro de utilização no horário indicado pelo Apelado, fl. 1032. Aduz que, em relação ao IP 189.40.70.118 a Apelante somente teria condições de identificar o real usuário, mediante o prévio fornecimento da porta lógica de origem. Rebela-se contra o valor da multa diária. Pretende a reforma da sentença para que seja reconhecido o cumprimento da liminar e a exclusão da multa diária ou, subsidiariamente a sua redução pelo cumprimento parcial da liminar, com afastamento da sucumbência

> *"A Tim S/A sustenta a impossibilidade de cumprimento da decisão em relação ao IP 189.40.70.118 e a Telefônica em relação aos IPs iniciados em "177.79", ambas sob a alegação de se tratarem de IPs nalteados, ou seja, compartilhados por mais de um usuário, razão pela*

---

[35] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4461936

[36] É o caso do Processo 1058034-44.2020.8.26.0100, acesso em: http://www.dje.tjsp.jus.br/cdje/consultaSimples.do?cdVolume=15&nuDiario=3242&cdCaderno=15&nuSeqpagina=1

qual seria necessário o autor indicasse a respectiva porta lógica, informação que segundo as requeridas seria de conhecimento apenas do provedor de aplicação, in casu, o Facebook."

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, a Ação Direta de Inconstitucionalidade (ADI) 5642[37], da ACEL, não foram consideradas, já que não registraram movimentações relevantes em vista da suspensão do julgamento e pedido de vista pelo Ministro Nunes Marques (em 17/06/2021).

Nessa categoria, convidamos as empresas, nessa fase de envio e discussão dos resultados preliminares do relatório, a compartilharem conosco ações judiciais e administrativas em que tenham participado e que possam ser consideradas para essa categoria. Ressaltamos, também, que processos que ocorram sob segredo de justiça ou cujas informações possam violar a privacidade de seus usuários poderão ser compartilhados com seus números, nomes, autoridades solicitantes e outros dados potencialmente pessoais ou sensíveis suprimidos, de forma somente a comprovar, para nós, a atuação da empresa na defesa judicial ou administrativa de seus clientes, durante o período analisado.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: ★

Nesta categoria, a Tim obteve **estrela cheia,** pois atendeu a ambos os parâmetros.

O **parâmetro I**, relativo ao posicionamento em geral da empresa, foi considerado atendido. Em algumas oportunidades ao longo do ano, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários.

Não foi encontrada nenhuma participação da empresa em quaisquer consultas públicas ou como *amicus curiae* em processos relativos à aprovação de normas ou adoção de técnicas que aumentem a proteção conferida aos usuários dos seus serviços.

[37] A Associação Nacional das Operadoras Celulares (Acel), da qual algumas operadoras fazem parte, ajuizou a Ação Direta de Inconstitucionalidade (ADI) 5642, no Supremo Tribunal Federal (STF), para impugnar dispositivo da Lei 13.344/2016, que confere a delegados de polícia e membros do Ministério Público a prerrogativa de requisitar informações e dados necessários à investigação criminal nos casos de tráfico de pessoas, independentemente de autorização judicial. A ACEL pede a concessão de liminar para que o STF dê à Lei 13.344/2016 interpretação conforme a Constituição Federal de modo a impedir entendimento que leve a medidas como interceptação telemática e de voz, localização de terminal ou IMEI (Identificação Internacional de Equipamento Móvel) de cidadão em tempo real por meio de ERB, extrato de ERB, dados cadastrais de usuários de IP, extratos de chamadas telefônicas e SMS, entre outros dados de caráter sigiloso. No mérito, pede a declaração de inconstitucionalidade parcial do dispositivo questionado.

No entanto, a TIM participou, por meio da Conexis do lançamento do Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações, apresentado à Autoridade Nacional de Proteção de Dados[38].

Consideramos o **parâmetro II** atendido. Na fase de interação com a empresa, a Tim nos informou que o reconhecimento facial é utilizado como medida de segurança pela empresa para fins de prevenção à fraude. **No entanto, o titular tem a opção de consentir com a coleta da biometria facial, não sendo esta uma coleta mandatória para criação de novas contas.**

Ademais, a empresa se manifestou em contribuição para Construção do Projeto de Lei Substitutivo ao n.º 21/2020, que diz respeito aos princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil, no sentido de que "Pode-se identificar algumas utilizações da IA que tendem a comportar mais risco, devendo, portanto, ser objeto de maiores salvaguardas e restrições. A título exemplificativo, temos análise de dados na esfera judicial e reconhecimento facial em ações de segurança pública, bem como outras que necessariamente não permeiam tais riscos como, por exemplo, tecnologias voltadas ao agronegócio."

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

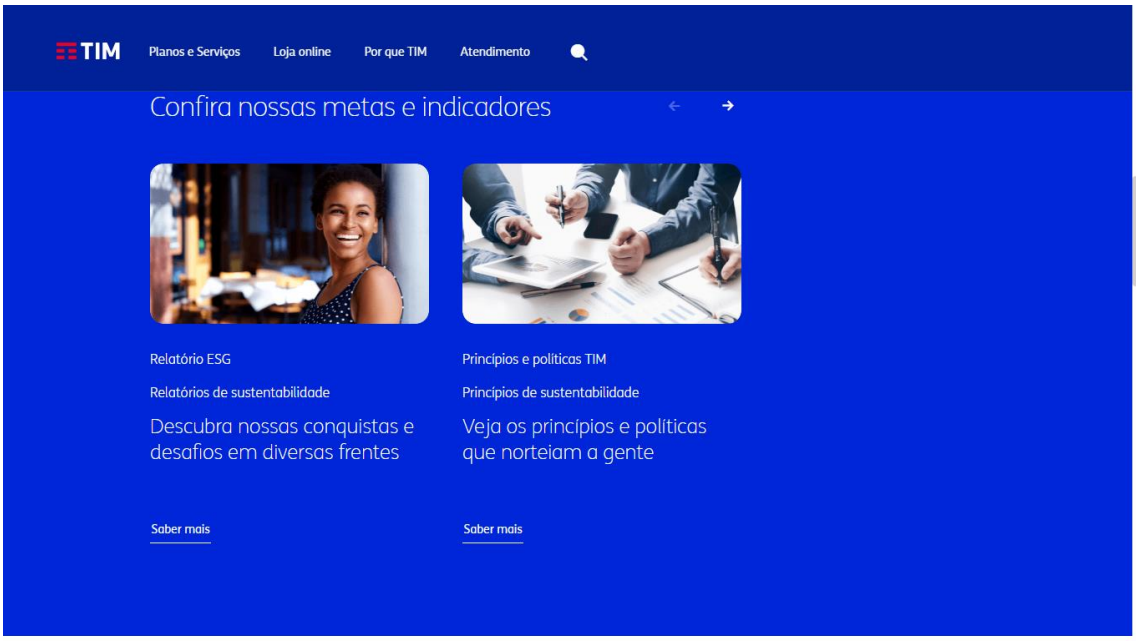
Resultado: 

Nesta categoria, a TIM Banda Larga obteve **três quartos de estrela,** pois atendeu integralmente aos parâmetros I, II, III e parcialmente ao parâmetro IV.

O **parâmetro I**, relativo à publicação de relatórios de transparência em português, foi considerado atendido, já que a TIM publicou este ano, em português, um Relatório de Sustentabilidade sobre suas atividades no Brasil. Mesmo que ainda caibam aperfeiçoamentos (vide itens abaixo), o relatório contém informações sobre a quantidade de ofícios recebidos do poder judiciário e o número de ações judiciais em que a empresa está envolvida, razão pela qual se considerou o parâmetro atendido.

O **parâmetro II**, relativo à acessibilidade do relatório de transparência, foi considerado atendido. Isso porque o Relatório de Sustentabilidade pode ser localizado em dois cliques a partir da página inicial da TIM, em "Sustentabilidade" e, logo após, em "Relatório de Sustentabilidade".

[38]Acesso em: https://www.telesintese.com.br/operadoras-criam-codigo-de-boas-praticas-de-protecao-de-dados/



Captura de tela de 13/10/2022. Página de sustentabilidade da TIM.[39]

O **parâmetro III**, relativo à periodicidade do relatório, foi considerado atendido. Na página de acesso aos relatórios estão disponíveis as versões publicadas nos anos anteriores.

O **parâmetro IV**, relativo às informações sobre pedidos de acesso a dados, foi considerado parcialmente atendido.

Sub-parâmetro (a): não atendido. Em seu relatório de transparência, a empresa informa (p. 46):

> Em 2021, foram iniciadas 718 ações judiciais relacionadas à privacidade de dados; 718 foram encerradas (incluindo casos abertos em anos anteriores), 59% delas com decisões favoráveis à Companhia. Nos 294 processos com decisões desfavoráveis, foram realizados pagamentos que totalizaram cerca de R$ 2,1 milhões. No mesmo intervalo, a Companhia recebeu 130 ações judiciais relativas à quebra de sigilo telefônico ou telemático: 135 casos foram encerrados.
> Mais de 1,5 milão de solicitações foram feitas pela Justiça à TIM para quebra de privacidade.
> Solicitações judiciais de quebra de privacidade por tipo:
> • Interceptações telefônicas: 325 mil
> • Dados cadastrais: 397 mil
> • Extratos telefônicos: 839 mil
> :

Não há, assim, informações que indiquem quantos pedidos foram atendidos ou rechaçados.

Sub-parâmetro (b): atendido. O item acima também traz o tipo de dado solicitado (interceptações telefônicas, dados cadastrais e extratos telefônicos.

[39] https://site.tim.com.br/sp/sobre-a-tim/sustentabilidade

Sub-parâmetro (c): não atendido. A empresa, em seu Relatório de Transparência, não traz dados considerados suficientes para atender ao sub-parâmetro.

Por fim, o **parâmetro V**, relativo à publicação de Relatórios de Impacto à Proteção de Dados, não foi considerado atendido. A empresa possui, de fato, um documento intitulado "O que é um relatório de impacto de proteção de dados". Embora consideremos positiva a atitude da Tim de disponibilizar um documento explicando o que é um relatório de impacto, não consideramos que seja suficiente para preencher o critério - já que, como boa prática, incentivamos as empresas a disponibilizarem o relatório.

CATEGORIA 6: Notificação do usuário

Resultado: ☆

A TIM não obteve estrela, pois não há menção à possiblidade de notificação do usuário em qualquer um dos documentos analisados.

VIVO

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a Vivo Móvel obteve **três quartos de estrela**, tendo atendido aos parâmetros I, II, III, IV e VII.

Embora não tenhamos localizado o contrato de prestação de serviços de internet móvel da empresa em seu site, a maior parte das informações aplicáveis está disponível no Relatório de Sustentabilidade, no Centro de Privacidade e nas Políticas de Privacidade da Vivo. No Centro de Privacidade, os usuários contam divisões visuais e acessíveis sobre "Segurança da Informação", "Exercício dos Direitos", dentre outras..

A Vivo atende ao parâmetro I, fornecendo informações claras e completas sobre todos os sub-parâmetros.

Sub-parâmetro (a): **integralmente atendido**. Em seu Centro de Privacidade, em "Tratamento de Dados", a empresa informa:

Natureza das informações coletadas

Na Vivo suas informações são importantes e necessárias para que ocorra a prestação dos serviços contratos por você. Sendo assim, coletamos os dados que você disponibilizou quando contratou os nossos serviços, por meio da sua interação e uso dos canais de informação. Entenda melhor quais informações coletamos:

Dados cadastrais, como nome, CPF, endereço, e-mail, bem como número de telefone. Informações de navegação e dados de conexão para envio e recebimento de dados. Transações de Recarga e o acompanhamento o uso desses créditos, volumes de dados trafegados em nossas redes, informações relacionadas ao seu uso e consumo, informações contábeis e fiscais de fatura e o pagamento dos serviços contratados por você. Eventos de SMS e eventos internacionais de operadoras em roaming, histórico de chamadas realizadas e recebidas, informações de atendimento em lojas, Call center e Meu Vivo.

captura de tela de 15.10.2022

A Política de Privacidade Local da Vivo expande o detalhamento dos tipos de dados coletados pela Vivo, por exemplo, dados biométricos de reconhecimento facial e reconhecimento de voz utilizados para o controle de fraudes, IMEI, dados sobre transações em contratos pré-pagos, etc.

Sub-parâmetro (b): **parcialmente atendido**. Nas seções "Natureza das informações coletadas" (vide trecho acima) e "Para que e como coletamos" (vide trecho abaixo), informa-se que os dados coletados são os disponibilizados (i) durante a contratação dos serviços e (ii) por meio da interação com canais de informação. Não há, porém, um descritivo com todas as possibilidades de coleta de dados praticadas pela Vivo, o que impede que o usuário entenda se há coleta de dados públicos, se há compra de dados por meio de terceiro intermediário, ou se há outras hipóteses de coleta de dados. Tampouco é possível ao usuário entender quais dos seus dados são coletados em cada hipótese de coleta.

Sub-parâmetro (c): não atendido. Não há informações sobre a coleta de dados públicos pela Vivo.

Sub-parâmetro (d): parcialmente atendido. A Política de Privacidade Local da Vivo traz diversas hipóteses de compartilhamento de dados dos titulares com terceiros, sem determinar, no entanto, se a própria Vivo coleta dados de titulares por meio destes parceiros. Na fase de discussão do relatório com a Vivo, nos foi apontado que há detalhamento nominal dos terceiros com os quais a Vivo compartilha dados de biometria nos Termos de Adesão dos seus planos.

Sub-parâmetro (e): integralmente atendido. A Política de Privacidade Local da Vivo afirma que: "*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*." A Política também reforça o compromisso da Vivo com o princípio da minimização em suas operações de compartilhamento de dados. Não somos, no entanto, informados sobre os procedimentos específicos para controle do nível de proteção de dados mantido pelos parceiros da Vivo.

Quanto ao **parâmetro II**, consideramos o seguinte:

Sub-parâmetro (a): integralmente atendido. No Centro de Privacidade, em "Para que coletamos" a empresa descreve algumas das finalidades dadas aos dados coletados pela Vivo, conforme abaixo:

Para que coletamos

Queremos que sua experiência com a Vivo seja cada vez mais transparente. Por isso, explicamos aqui alguns dos principais motivos pelo qual tratamos suas informações:

- Para garantir a prestação adequada dos produtos e serviços dos quais você é nosso cliente;
- Aprimorar o desempenho da nossa rede e de sistemas;
- Aumentar a qualidade dos nossos serviços e ajudar na tomada de decisões estratégicas de negócio;
- Corrigir falhas e avaliar a demanda por região geográfica;
- Melhorar a experiência de relacionamento entre você e a Vivo, como envio de marketing direto e fornecimento de ofertas ainda mais relevantes;
- Deixar os processos para elaboração de planos, serviços e ofertas ainda mais próximos do seu perfil;
- Para prevenir situações de fraude e assegurar a proteção ao crédito;
- Em cumprimento de obrigações legais e regulatórias.

captura de tela de 15.10.2022

Além disso, na Política de Privacidade Local da Vivo, a seção "7. Como tratamos os seus dados e com qual finalidade?" traz uma listagem mais detalhada de finalidades às quais são destinadas as várias formas de tratamento de dados realizadas pela Vivo. A descrição, contudo, não permite ao titular de dados identificar quais de seus dados são empregados para cada finalidade, e com pretexto em qual base legal. A análise da legitimidade de bases legais empregadas pela Vivo, portanto, não é facilitada pela Política atual.

Sub-parâmetro (b): integralmente atendido. A Vivo fornece informações sobre a forma de utilização dos dados nos trechos apontados acima (demonstrando as situações em que a coleta ocorre e a sua finalidade) e informações sobre tempo e local de armazenagem etc.

Quanto ao parâmetro III, consideramos o seguinte:

Sub-parâmetro (a): **atendido**. Na Política de Privacidade Local da Vivo, a seção "14. POR QUANTO TEMPO MANTEREMOS OS SEUS DADOS?" descreve as hipóteses de retenção de dados pela empresa, fornecendo alguns dos prazos de retenção adotados para casos de cumprimento de obrigação legal ou regulatória e exercício de direitos.

Quanto às localidades de armazenamento, a Política apenas reafirma que: "A Vivo se compromete em manter os seus dados armazenados, adotando boas práticas e medidas técnicas e administrativas para impedir sua perda, alteração e acesso não autorizados, conforme determinação da legislação aplicável".

Sub-parâmetro (b): não atendido. Não há descrição clara das hipóteses de deleção de dados adotadas pela Vivo.

Sub-parâmetro (c): atendido integralmente. Conforme descrito no **Sub-parâmetro (a)**.

Sub-parâmetro (d): parcialmente atendido. A Vivo compromete-se com o cumprimento da Política Global de Segurança da Telefônica, que define parâmetros administrativos e organizacionais de segurança, inclusive cibernética, para o Grupo Telefônica como um todo. Porém, não somos informados sobre a estrutura organizacional específica da Vivo para lidar com ameaças à proteção de dados.

Sub-parâmetro (e): integralmente atendido. A Política Global de Segurança da Telefônica é disponibilizada, apesar de não contar com informações sobre o seguimento de protocolos internacionais de proteção (ex.: ISO 27001) ou softwares empregados para a estrutura técnica de proteção dos dados. No entanto, no Relatório de Sustentabilidade, encontramos algumas informações adicionais sobre os procedimentos de Segurança de Informação da Vivo. O Relatório informa que a Vivo possui políticas de informação publicadas na intranet, além de um Plano de Resposta a Incidentes e procedimentos para a elaboração de Análises de Impacto e Planos de Continuidade de Negócios (PGC, PGI, PRD e PCO) testados minimamente a cada seis meses. No relatório do ano passado (2020), a Vivo também informou que utilizou padrões de segurança "com base nos requisitos de segurança da companhia e frameworks de mercado (ISO 27001 e ISO 22301, NIST, PCI/DSS etc.), especialmente relacionados a sistemas e servidores seguros", uma "lista extensa de protocolos a serem seguidos". Além disso, no Centro de Privacidade, em "Segurança e Confidencialidade ", a empresa informa alguns padrões de segurança que utiliza, como a criptografia na transferência dos dados pessoais dos dispositivos dos usuários, declara permitir o acesso aos dados somente a pessoas autorizadas,

conforme o 'princípio do privilégio mínimo', afirma propiciar auditabilidade de quaisquer atividades tomadas com os dados, dentre outros.

Sub-parâmetro (f): não atendido. Não contamos com informações sobre o controle de acessos empregado pela Vivo para tratamento de dados pessoais.

Sub-parâmetros (g) e (h): integralmente atendido. A Política de Privacidade Local da Vivo traz diversas hipóteses de compartilhamento de dados dos titulares com terceiros,agrupados por categoria (ex.: "Parceiros de Vendas", "Dealers", etc.), com breve descrição das finalidades de compartilhamento com cada categoria de parceiro.

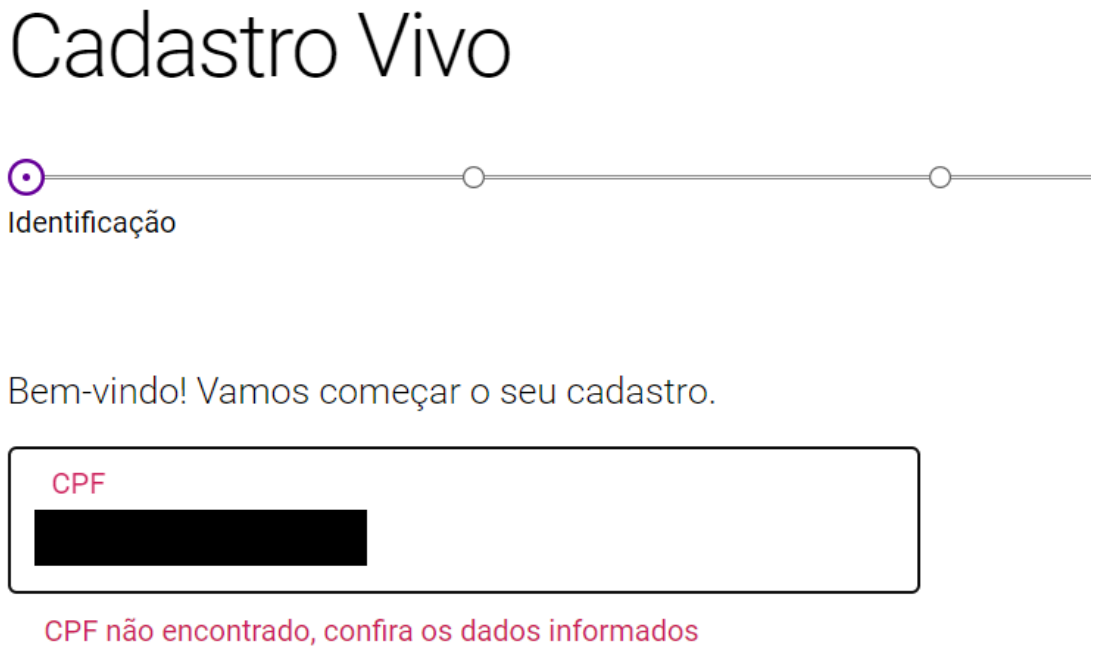
Sub-parâmetro (i): parcialmente atendido. A Política de Privacidade Local da Vivo traz, na seção "10. A TRANSFERÊNCIA INTERNACIONAL DOS SEUS DADOS", algumas das finalidades e hipóteses de transferência internacional empregadas pela empresa. No entanto, não há correlação entre os tipos de dados e as finalidades de transferência internacional, o que permitira ao titular dos dados analisar a legitimidade de tais transferências.

Quanto ao **parâmetro IV**, consideramos o seguinte:

Sub-parâmetro (a): integralmente atendido. A Política de Privacidade Local da Vivo informa o titular sobre o canal específico para reclamações relacionadas à proteção de dados pessoais de maneira clara e direta.

Sub-parâmetro (b): integralmente atendido. No Centro de Privacidade, em "Exercício dos Direitos", a empresa lista alguns direitos dos titulares sobre seus dados. Além disso, a mesma página oferece portais, e-mails ou número de telefone e de SMS para que se possa exercer tais direitos, a depender do direito a que se refere. Por fim, a Política de Privacidade Local da Vivo traz a seção 15. QUAIS SÃO OS SEUS DIREITOS COMO TITULAR E COMO EXERCÊ-LOS?", com descrição de todos os dados garantidos pelo artigo 18 da LGPD. Vale apontar que os direitos de prestação informacional ao titular de dados, dispostos nos artigos 8 e 9 da LGPD, não são explicitamente mencionados.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado **não atendido**. O InternetLab realizou pedido de acesso a dados em 03 de novembro de 2022 por meio de e-mail ao DPO da empresa. O contato foi retornado no dia seguinte, quando recebemos uma mensagem afirmando que as informações sobre os tipos de dado tratados pela Vivo poderiam ser encontradas por meio do Centro de Privacidade, na área "Exercício dos direitos" e em seguida "Acesso e consulta aos dados pessoais" (https://www.vivo.com.br/a-vivo/informacoes-aos-clientes/centro-de-privacidade/privacidade-e-seguranca/exercicio-dos-direitos). No entanto, o acesso a tal página exige a realização de cadastro na plataforma "App Vivo", o que não foi possível dado que o CPF informado não foi reconhecido no site da Vivo.



A incapacidade de exercer os direitos foi considerada como uma falha técnica de responsabilidade da operadora.

Vale ressaltar que, como alternativa para os não clientes, o Centro de Privacidade da Vivo disponibiliza um formulário que deve ser enviado pelo correio. Além disso, há exigência no Formulário de que o titular envie (i) cópia autenticada de documento de identificação (RG e CPF ou CNH); e (ii) firma reconhecida por cartório na assinatura do Formulário. Embora possa a checagem de identidade seja importante para fins de prevenção à fraude, a exigência de que o envio seja feito apenas pelo correio e com firma reconhecida em cartório configura uma barreira desnecessária para o exercício de direitos do titular de dados pessoais.

O **parâmetro VI**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, **não foi considerado atendido**. Nenhum documento da Vivo mencionava tal possibilidade, e sua própria Política de Privacidade Local afirma, na cláusula 17, que "esta Política de Privacidade e Proteção de Dados poderá ser revisada a qualquer tempo e sem prévio aviso." Na fase de engajamento de 2021, a empresa informou que sua política de privacidade local seria atualizada para prever a notificação dos usuários no caso de sua alteração. No entanto, na data de fechamento deste relatório, a mudança ainda não tinha sido realizada, ainda constando o texto aqui mencionado na cláusula 17.

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado parcialmente atendido. Isso porque a Vivo dispõe de um Centro de Privacidade, mencionado diversas vezes acima, com informações claras e, no geral, completas sobre o tema. Além disso, o centro pode ser facilmente acessado na página inicial da Vivo:

captura de tela de 23.07.2021

No entanto, não pôde ser localizado o contrato de prestação de serviços de internet móvel ou o contrato de internet banda larga da Vivo, e a disposição de tais informações no contrato seria recomendável para que estas pudessem ser acessadas por todos os clientes, consentidas legalmente por eles, e pormenorizadas de acordo com cada tipo de serviço contratado.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ★

Nesta categoria, a Vivo obteve **estrela cheia**, pois atendeu a quatro dos cinco parâmetros.

Quanto ao **parâmetro I**, consideramos o seguinte: integralmente atendido. Na página 22 do *Informe de Transparencia en las Comunicaciones 2021* da Telefônica (ainda vigente), há a definição de quais seriam as autoridades competentes para interceptações e requisição de metadados de acordo com a legislação brasileira, além de menção da competência dos "juízes de qualquer esfera":

> *"Interceptación legal: De acuerdo con el artículo 3o de la Ley Federal brasileña n. 9.296/1996 (ley de las interceptaciones), solamente el Juez (de la esfera criminal) puede determinar las interceptaciones (telefónicas y telemáticas), a petición de la Fiscalía (Ministério Público) o Comisario de Policía (Autoridade Policial).*
> *Metadatos asociados a las comunicaciones: Autoridades competentes » Fiscalía, Comisarios de Policía y Jueces de cualquier esfera, como también Presidentes de las Comisiones Parlamentarias de Investigación: el nombre y dirección del usuario registrado (datos de abonado), así como la identidad de los equipos de comunicación (incluyendo IMSI o IMEI)."*
> *Jueces de cualquier esfera: los datos para identificar el origen y el destino de una comunicación (por ejemplo, números de teléfono, nombres de usuario*

para los servicios de Internet), la fecha, hora y duración de una comunicación y la localización del dispositivo."

Isso significa que a Vivo entrega dados cadastrais mediante requisição de representantes Ministério Público ("Fiscalía"), autoridades policiais ("comisarios de policía") e juízes. Registros de conexão e dados de localização são disponibilizados apenas mediante ordem de um juiz.

Quanto ao **parâmetro II**, consideramos o seguinte: integralmente atendido. No *Informe de Transparencia en las Comunicaciones*, é citado, ao lado de outros diplomas legais, o Art. 15 da Lei 12.850/13 (Lei das Organizações Criminosas) como "Contexto Legal" para a requisição de "metadados associados às comunicações". Além disso, no seu Centro de Privacidade, em "Protocolo de Entrega de Dados para Autoridades", a Vivo Informa:

Leis que amparam

Leis que amparam a entrega de dados e autoridades competentes para requisição de dados sigilosos

A quebra do sigilo dos dados e das comunicações pode ocorrer nas hipóteses definidas pela Constituição Federal, pela Lei e pela Regulamentação. Dessa forma, listamos aqui uma relação dos principais artigos da Constituição e das principais Leis e Regulamentos que determinam exceção ao sigilo das comunicações e dados pelas empresas do setor no Brasil:

- Constituição Federal do Brasil de 1998 – Art. 5º, inciso XII e Art. 58, §3º
- Lei Interceptação – Lei n.º 9296/1996 – Art. 1º, § único
- Lei Geral de Telecomunicações – Lei n.º 9472/1997 – Art. 3
- Lei Lavagem de Dinheiro – Lei n.º 12.683/2012 - Art. 17-B
- Lei Delegados – Lei n.º 12.830/2013 - Art. 2
- Lei Organização Criminosa – Lei n.º 12.850/2013 - Art. 15
- Lei Marco Civil da Internet – Lei 12.695/2014 – Art. 7;10 e 19
- Decreto n.º 8771/2016 – Art. 11
- Lei 13.344/2016 – Tráfico de Pessoas – Art.13-B
- Lei Busca Pessoa Desaparecida – Lei n.º 15.292/2014 – Art. 9º
- Resolução Anatel n.º 73/1998 – Art. 65 H, parágrafo único e 65 K - Regulamento dos Serviços de Telecomunicações
- Resolução Anatel n.º 614/2013 – Art. 56, V - Regulamento do Serviço de Comunicação Multimídia

captura de tela de 23.07.2021

O InternetLab enaltece a listagem das leis que permitem a entrega de dados para autoridades competentes no centro de privacidade da Vivo, de forma facilmente acessível para seus usuários.

Quanto ao **parâmetro III**, consideramos o seguinte: não atendido. Mesmo que o Informe de Transparência mencionado acima inclua a "localização do dispositivo" dentre os dados que podem ser requisitados por ordem judicial, e que o Protocolo de Entrega de Dados mencione a possibilidade de dados de "Localização de Estação Rádio-Base", não há qualquer detalhamento sobre as circunstâncias em que compartilha dados geolocacionais e por quê, não fornecendo as informações exigidas pelos sub-parâmetros desse item.

Quanto ao **parâmetro IV**, consideramos o seguinte: parcialmente atendido. Por um lado, o mesmo trecho apontado acima é claro ao definir que somente juízes terão acesso aos dados sobre origem e destino de uma comunicação, de que se depreende que tal acesso se dará mediante ordem judicial.

No entanto, o trecho não se restringe estritamente aos termos do Marco Civil da Internet (ou seja, não especifica que somente a data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado serão compartilhados).

Por fim, o **parâmetro V**, foi considerado parcialmente atendido. Este ano, tal como em 2021, localizamos uma seção específica no Centro de Privacidade da Vivo voltada a tais solicitações, com o próprio título de "Protocolo de Entrega de Dados a Autoridades".

Protocolo de entrega de dados à Autoridades

Conduta Colaborativa

O respeito e a proteção do sigilo de dados e comunicações de nossos clientes é um dos pilares que sustentam a atuação da Vivo, razão pela qual, reforçando o compromisso de transparência com nossos clientes e investidores, esclarecemos que recebemos das autoridades competentes requisições para a quebra do sigilo de dados e comunicação dos clientes nos termos da Lei.

A quebra de sigilo dos dados e das comunicações é uma imposição legal e regulamentar do setor voltada, principalmente, ao auxílio a investigações e identificação de pessoas de interesse da Justiça, sendo que reconhecemos a relevância da colaboração com os órgãos investigativos e judiciais com o cumprimento de tais ordens.

Contudo, independente da obrigação legal imposta e a postura colaborativa adotada, a Vivo reforça o seu compromisso com a proteção do sigilo de dados e comunicações de seus clientes, adotando uma postura ativa na defesa de tais direitos perante as autoridades e a Justiça de forma a garantir que sejam respeitados tais direitos e garantias de seus clientes.

captura de tela de 17.10.2022

O InternetLab enaltece a conduta da Telefónica Global de tornar públicas diversas interpretações sobre a entrega de dados, autoridades competentes, quantidade de pedidos rechaçados e atendidos, dentre outros, em seu relatório de transparência.

No entanto, reforçamos que há necessidade de apresentar tais informações em português e no site da Vivo para que a informação seja considerada clara e facilmente acessível.

Além disso, não foram disponibilizados no site da Vivo os contratos relativos aos serviços de banda larga e internet móvel com vigência em 2022. O link para acesso aos Contratos da Vivo[40] retornou apenas documentos antigos, indicados pelo próprio site como vencidos (nenhum resultado para seleções com "Vigência Atual").

CATEGORIA 3: Defesa dos usuários no Judiciário

[40] Acesso em: https://www.vivo.com.br/para-voce/contratos-e-regulamentos?q=contratos

Resultado: ★

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

Quanto ao **parâmetro I**, referente à contestação de legislação, realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte, e não localizamos quaisquer ações onde a Vivo contesta a legislação relacionada aos procedimentos de entrega de dados ao judiciário. Ressaltamos que nossa busca, por questões de escopo e tempo, não buscou por ações do tipo nos tribunais estaduais, relativas, portanto, a legislações ou interpretação de legislações de âmbito estadual. As empresas têm a possibilidade de, durante a fase de discussão dos parâmetros e troca de documentos, comprovar sua atuação nesse sentido.

Em 29/03/2022, o STF publicou o julgamento da Ação Direta de Inconstitucionalidade número 4924/DF[41], onde a Associação Nacional das Operadoras Celulares - ACEL, da qual a Vivo faz parte, pediu pela declaração de inconstitucionalidade da Lei 17.107/12, do Estado do Paraná, que dispõe sobre penalidades ao responsável pelo acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres (trote telefônico). A lei visava estabelecer obrigação às operadoras de telefonia de fornecer os dados dos proprietários de linhas telefônicas que acionem indevidamente os serviços de atendimento diante de mero ofício por qualquer órgão ou instutuição pública envolvida. A ACEL argumentou em falor da inviolabilidade da intimidade, vida privada horna e do sigilo das comunicações telefônicas (segundo estabelecido no artigo 5º, incisos X e XII da Constituição Federal), mencionando a indisponibilidade do direito à proteção de dados pessoais em sua argumentação.

Além disso, a ACEL havia ajuizado a ADI 5040/PI[42], publicada em 2021 (não incluída em nosso relatório anterior), onde questionava a legalidade da Lei Nº 6.336/2013 do Estado do Piauí, que obrigava as empresas prestadoras de serviço de telefonia móvel pessoal a fornecerem, aos órgãos de segurança pública, dados relativos à localização de telefones celulares e cartões "SIM" que tivessem sido objeto de furto, roubo e latrocínio ou utilizados na prática de delitos. Entre seus argumentos, a ACEL também alegou grave ofensa à privacidade de seus clientes na hipótese de divulgação das informações pessoais, citando a Constituição e o direito fundamental à privacidade, além da inviolabilidade dosigilo telefônico.

Por fim, para averiguação do **parâmetro II**, referente à contestação de pedidos abusivos, 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 21/06/2021 e 19/10/2022. Encontramos diversas ações onde a Vivo contestou pedidos de dados de seus clientes, seja pela falta de ordem judicial determinando a entrega dos dados[43] ou fundamentação jurídica insuficiente dos pedidos[44].

---

[41] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183

[42] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4461936

[43] É o caso do Processo 1058034-44.2020.8.26.0100, acesso em: http://www.dje.tjsp.jus.br/cdje/consultaSimples.do?cdVolume=15&nuDiario=3242&cdCaderno=15&nuSeqpagina=1

[44] É caso da Apelação Cível nº 1073466-74.2018.8.26.0100, acesso em: https://esaj.tjsp.jus.br/cjsg/resultadoCompleta.do;jsessionid=9CE74DFCA39C8E79F7FB21BAC5930EEF.cjsg3

Por exemplo, encontramos, no relatório do acórdão referente ao Processo 1058034-44.2020.8.26.0100:

"A corré Telefônica Brasil SA apresentou contestação (fls. 315/323). ***Sustenta a inexistência de obrigação legal da telefônica em fornecer parte dos dados solicitados pertinentes às conexões realizadas há mais de um ano da data da citação da ré, o que foi feito no intuito de cooperar com o pleito do autor****. Alega que não se nega a prestar informações, observada a determinação judicial necessária para a quebra do sigilo de dados, garantido constitucionalmente, pelo que pugna pelo afastamento da condenação sucumbencial."*

Também no Processo 1042581-72.2021.8.26.0100, deste ano:

"*Citada, a corré Telefônica Brasil S.A. apresentou contestação às fls. 120/132. A partir do fornecimento das informações pelo Facebook, o autor identificou os responsáveis pelos endereços de IP. Dentre os endereços de IP identificados pelo autor, a ré verificou que apenas 01 IP é de sua responsabilidade (fl. 121).* ***Afirmou que não se opõe a realização das pesquisas e fornecimento de dados que dispuser, desde que disponíveis, tendo em vista a pesquisa fora do prazo prescricional de um ano; seja fornecidos todos os parâmetros de pesquisa e seja expedida ordem judicial expressa e específica nesse sentido****. Esclareceu que, na qualidade de provedora de conexão, possui obrigação legal de armazenar os registros de acesso de conexão pelo período de um ano (art. 13 do Marco Civil da Internet). Esclareceu ainda que, por vedação legal do art. 14 do Marco Civil da Internet,* ***não armazena registros de acesso a aplicação, razão pela qual deverá ser indeferido o pedido para fornecimento dos responsáveis pelas publicações dos perfis falsos e suas URLs****. Ressaltou que o fornecimento de informações somente será possível* ***mediante ordem judicial expressa do juízo****."*

Na Apelação Cível nº 1073466-74.2018.8.26.0100, encontramos a exigência de que os pedidos de informação devem ser acompanhados da indicação das portas lógicas específicas ao IPs solicitados:

"Recorre a Telefônica Brasil S/A. Assevera ter cumprido a liminar e apresentado todos os números das linhas telefônicas utilizadas simultaneamente pelos IPs nateados com "range" "177.79", em consonância com os parágrafos 1º e 2º, do artigo 10, da Lei n.º 12.965/20145, amparada por ordem judicial específica. Informa que a r. sentença desconsiderou o fornecimento de todos os dados imediatamente disponíveis pela ora Apelante e, por conseguinte, fixou a majoração da multa diária em R$ 5.000,00 (cinco mil reais). Assevera que, no tocante às informações relativas a usuários dos IP's compartilhados, ***a Apelante esclareceu a necessidade de prévia indicação das portas lógicas de origem.*** *Sem esses dados seria impossível cumprimento, ressaltando ser ônus do autor. Rebela-se contra o valor da multa diária fixada no vultoso valor de R$ 5.000,00 por dia. Pretende a reforma da sentença ou a redução da condenação."*

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, a Ação Direta de Inconstitucionalidade (ADI) 5642[45], da ACEL, não foram consideradas, já que não registraram

[45] A Associação Nacional das Operadoras Celulares (Acel), da qual algumas operadoras fazem parte, ajuizou a Ação Direta de Inconstitucionalidade (ADI) 5642, no Supremo Tribunal Federal (STF), para impugnar dispositivo da Lei 13.344/2016, que confere a delegados de polícia e membros do Ministério Público a prerrogativa de requisitar informações e dados necessários à investigação criminal nos casos de tráfico de pessoas, independentemente de autorização judicial. A ACEL pede a concessão de liminar para que o STF dê à Lei 13.344/2016 interpretação conforme a Constituição Federal de modo a impedir entendimento que leve a medidas como interceptação telemática e de voz, localização de terminal ou IMEI (Identificação Internacional de Equipamento Móvel) de cidadão em tempo real por meio de ERB, extrato de ERB, dados

movimentações relevantes em vista da suspensão do julgamento e pedido de vista pelo Ministro Nunes Marques (em 17/06/2021).

Nessa categoria, convidamos as empresas, nessa fase de envio e discussão dos resultados preliminares do relatório, a compartilharem conosco ações judiciais e administrativas em que tenham participado e que possam ser consideradas para essa categoria. Ressaltamos, também, que processos que ocorram sob segredo de justiça ou cujas informações possam violar a privacidade de seus usuários poderão ser compartilhados com seus números, nomes, autoridades solicitantes e outros dados potencialmente pessoais ou sensíveis suprimidos, de forma somente a comprovar, para nós, a atuação da empresa na defesa judicial ou administrativa de seus clientes, durante o período analisado.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Vivo obteve **meia estrela,** pois atendeu a um dos parâmetros analisados.

O **parâmetro I**, relativo ao posicionamento em geral da empresa, foi considerado integralmente atendido. Em algumas oportunidades ao longo do ano, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários.

A Vivo, por exemplo, participou, por meio da Conexis do lançamento do Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações, apresentado à Autoridade Nacional de Proteção de Dados[46].

A empresa também informa, em seu Relatório de Sustentabilidade, que realiza anualmente um evento de Cyber War Games (Exercícios de Guerra Cibernética), onde uma equipe realiza cenários de ataques cibernéticos simulados para que outra equipe possa identificar e realizar todas as defesas necessárias, para avaliar a maturidade de Segurança Digital, testar os processos estabelecidos, reforçar procedimentos de detecção e respostas a incidentes e proteger o ambiente da Vivo. Identificamos este evento como uma promoção do hacking ético e de procedimentos de conscientização, da empresa e do público geral, a respeito das possibilidades de falhas de segurança e exploits, sendo uma técnica empregada pelas maiores companhias de tecnologia americanas (que geralmente, oferecem altos valores para a detecção efetiva de exploits com potencial de prejudicar os seus usuários e clientes).

A Vivo também realiza o Compliance Day, evento no qual foram estimuladas discussões a respeito da Proteção de Dados Pessoais nos últimos anos.

---

cadastrais de usuários de IP, extratos de chamadas telefônicas e SMS, entre outros dados de caráter sigiloso. No mérito, pede a declaração de inconstitucionalidade parcial do dispositivo questionado.

[46]Acesso em: https://www.telesintese.com.br/operadoras-criam-codigo-de-boas-praticas-de-protecao-de-dados/

Durante a fase de discussão dos relatórios preliminares com as empresas, a Vivo esclareceu que entre 2021 e 2022, ofereceram contribuições e comentários aos temas propostos na Agenda Regulatória da ANPD, em conjunto com associações empresariais (por exemplo, Brasscom e Conexis) e em nome próprio e por meio da Plataforma Participa + Brasil. Também fomos informados de que a Vivo participou de duas Consultas Públicas e uma Tomada de Subsídios promovidas pela ANPD no período. Por exemplo, entre 30/08/2022 e 14/10/2022, a Vivo enviou suas sugestões e comentários à norma de aplicação da LGPD para microempresas e empresas de pequeno porte[47]. Entre 18/05/2022 e 30/06/2022, a Vivo participou e enviou contribuições sobre diversos questionamentos promovidos pela ANPD sobre o tópico de transferência internacional de dados. Entre 16/08/2022 e 15/09/2022, a Vivo participou da consulta pública sobre a minuta de Resolução que regulamenta a aplicação de sanções pela ANPD, em atenção aos artigos 52 e 53 da LGPD e complementando a Resolução CD/ANPD nº 01 de 2021, que especifica as diretrizes gerais sobre o processo administrativo que será conduzido pela autoridade.

A Vivo também realizou uma manifestação formal contrária aos Ofícios 256, 399 e ao processo 53500.056673/2020-00 da ANATEL, que determinavam que os "dados dos consumidores coletados e disponibilizados pela ANATEL às operadoras via API para tratamento de demandas [seriam] alterados a partir de 01/05/2022".

A partir de março de 2021, de forma semanal ou a cada duas semanas, a Vivo também participou de reuniões promovidas pelo Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica da ANATEL (GT – Cyber), grupo de trabalho da agência criado pelo Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações (aprovado pela Resolução nº 740/202 e designado pela Portaria ANATEL nº 1.878 de 30 de dezembro de 2020)[48].

Consideramos o parâmetro II não atendido. Não encontramos qualquer posicionamento público da Vivo com relação à proteção de dados pessoais relativa às tecnologias de reconhecimento facial. Tampouco identificamos qualquer participação, em consultas públicas ou como amicus curiae, em processos da ANATEL ou do STF.

No entanto, segundo diversas reportagens, a Vivo tem utilizado a tecnologia de reconhecimento facial para cadastro de seus assinantes desde 2018[49].

Na fase de discussão dos relatórios preliminares, a Vivo esclareceu que informa os titulares de dados sobre a coleta de seus dados biométricos em sua Política de Privacidade e nos Termos de Adesão aos seus planos de telefonia. Não consideramos, no entanto, estas ações como suficientes para atingir o cumprimento do parâmetro em questão, dado que são mera consequência do cumprimento de

---

[47] Acesso em: https://www.gov.br/participamaisbrasil/minuta-de-resolucao-para-aplicacao-da-lgpd-para-microempresas-e-empresas-de-pequeno-porte-#ctb_CP-042634

[48] Acesso em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO7yWfLAuQ-xt0ryvn6Moky23ZfdO0tw8pd7J91WEMwuJiHWzVUWCRvZeN-oiYJnFCggjDhwwXwORf95zykIXQ-j

[49] Acesso em: https://teletime.com.br/22/11/2018/vivo-inicia-cadastro-de-rostos-de-assinantes-em-suas-lojas/
https://www.minhaoperadora.com.br/2018/11/vivo-esta-cadastrando-rostos-de-clientes.html
https://www.mobiletime.com.br/noticias/22/11/2018/vivo-inicia-cadastro-de-rostos-de-assinantes-em-suas-lojas/

obrigações legais da empresa relacionadas ao fornecimento de informações ao titular enquanto controladora de dados pessoais.

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

Resultado: 

Nesta categoria, a Vivo Banda Larga obteve três quartos de **estrela,** pois atendeu aos parâmetros I, II e III.

O **parâmetro I** foi considerado integralmente atendido.

Na fase de discussão do relatório preliminar com a Vivo, a empresa nos forneceu o link para um Informe de Transparência das Comunicações da Telefônica em português (publicado no Centro de Transparência da Vivo), com dados relacionados à Vivo especificamente no corpo do documento.

O **parâmetro II**, relativo à acessibilidade do relatório de transparência, foi considerado integralmente atendido. Tanto o Relatório de Sustentabilidade quanto o Informe de Transparência da Vivo podem ser facilmente encontrados no Centro de Privacidade da Vivo.

O **parâmetro III**, relativo à periodicidade do relatório, foi atendido. A Telefônica publica regularmente seus relatórios de transparência anuais.

O **parâmetro IV**, relativo às informações sobre pedidos de acesso a dados, foi considerado atendido.

Sub-parâmetro (a): parcialmente atendido. Embora constem informações relevantes sobre os pedidos recebidos no Informe de Transparência da Telefônica, a Vivo esclareceu, em fase de discussão do relatório, que não contabiliza o número de pedidos rechaçados (ou seja, o número de ocasiões em que rejeita ou apresenta contra-argumento à solicitação de dados por autoridade legal).

O sub-parâmetro (b) foi considerado atendido. No Informe de Transparência, somos informados sobre os tipos de dados solicitados por autoridades públicas.

O sub-parâmetro (c) foi considerado atendido. No Informe de Transparência, a Vivo informa o número de acessos afetados pelas solicitações.

Por fim, o **parâmetro V**, relativo à publicação de Relatórios de Impacto à Proteção de Dados, não foi considerado atendido. Não foram localizados quaisquer documentos nesse sentido em nossas buscas.

CATEGORIA 6: Notificação do usuário

Resultado: ☆

A Vivo não obteve estrela, pois não há menção à possibilidade de notificação do usuário em qualquer um dos documentos analisados.

ALGAR

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a Algar obteve **estrela cheia**, pois atendeu integralmente aos parâmetros II, III, IV, VI e VII. E atende parcialmente ao parâmetro I.

Ressaltamos, no entanto, que o parâmetro V, relativo aos pedidos de acesso aos dados feitos pelos integrantes do InternetLab à empresa, ainda não foi avaliado, em vista de o referido pedido ainda não ter sido realizado. Os resultados obtidos com tal solicitação poderão melhorar a nota final da empresa nessa categoria.

A Algar atende parcialmente ao **parâmetro I.** A empresa oferece informações claras e completas sobre o Sub-parâmetro (b); e cumpre parcialmente os **Sub-parâmetro (a)**.

O ***Sub-parâmetro (a)***, referente aos dados coletados, foi considerado parcialmente atendido. Na seção "Privacidade de Dados Pessoais", de sua Política de Dados, a empresa apresenta uma tabela que afirma coletar dados cadastrais e quais seriam dados (nome, data de nascimento, dados bancários etc). A tabela também informa a finalidade do uso dos dados:

4.1.4 - Tipo de Dados

TIPO DE DADOS	DADOS PESSOAIS	FINALIDADE DO USO DOS DADOS
Cadastrais	● Nome; ● Data de Nascimento; ● RG; ● Nome da Mãe; ● CPF; ● CNPJ; ● Razão Social; ● Nome de Contato; ● Endereço de Instalação; ● Endereço de Correspondência; ● Dados bancários (Débito Automático); ● Foto de Documentos Pessoais; ● E-mail.	● Identificar o cliente/usuário; ● Cumprir obrigação legal, compartilhando com terceiros e autoridades, quando requisitado e realmente necessário; ● Proteção do crédito e procedimentos de cobrança; ● Garantir a segurança do cliente/usuário.

Captura de tela de 19.10.2022

Ainda que seja positivo que a empresa discrimine quais são os dados cadastrais coletados, essa informação foi considerada insuficiente para esta edição do relatório, porque a empresa informa apenas um tipo de dado coletado. A empresa não informa outros tipos de dados que coleta, como, por exemplo, dados de localização, dados de tráfego (como duração de ligação, perfil de consumo), entre outros. Por isso, o sub-parâmetro foi considerado parcialmente atendido.

O *Sub-parâmetro (b)*, referente às situações em que a coleta ocorre, foi considerado atendido. Na seção "Privacidade de Dados Pessoais", a empresa informa na cláusula 4.1.3 algumas hipóteses de situações em que a coleta ocorre, como, por exemplo, no preenchimento do contrato, na contratação de outros serviços etc. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

> "4.1.3 - Coleta de dados pessoais
> 4.1.3.1 - Os dados são coletados a partir do preenchimento do contrato de prestação de serviço, contratação de outros serviços ou de informações inseridas em termos, ficha ou formulários físicos ou digitais, quando o processamento está de acordo com nossos interesses legítimos e não menosprezam seus interesses relacionados à proteção de dados ou liberdades e direitos fundamentais;
> 4.1.3.2 - Havendo necessidade, a Algar Telecom pode receber seus dados pessoais ou dados de uso de terceiros. Por exemplo, se você estiver em outro site e optar por ser contatado pela Algar Telecom, esse site transmitirá seu endereço de email e outros dados pessoais para nós, para que possamos entrar em contato com você conforme solicitado."

O Sub-parâmetro (c), referente à possibilidade de coleta de dados disponíveis publicamente, foi considerado não atendido. Não há menção acerca da coleta de dados públicos.

O Sub-parâmetro (d), referente à listagem por nome de quais terceiros fornecem dados à empresa, foi considerado não atendido. Não há listagem dos terceiros fornecedores de dados.

O Sub-parâmetro (e), relativo à conformidade legal de terceiros com a LGPD, foi considerado não atendido. Isso porque essa necessidade de conformidade não foi encontrada em nenhum documento público da empresa.

O **parâmetro II**, referente ao fornecimento de informações acerca da finalidade dos dados coletados, foi considerado, na média, atendido, pois a empresa atendeu ao **Sub-parâmetro (a)** parcialmente e ao (b) integralmente.

O **Sub-parâmetro (a)**, referente à finalidade do tratamento de dados, foi considerado parcialmente atendido. Na sua Política de Privacidade de Dados Pessoais (vide tabela reproduzida no **Sub-parâmetro (a)**), a empresa informa quatro finalidades do tratamento de dados: (i) identificar o cliente; (ii) cumprir obrigação legal; (iii) proteção de crédito e procedimentos e cobrança; e (iv) garantir a segurança do cliente. De forma indireta, a cláusula 4.1.5.1 (vide trecho abaixo) elenca como finalidade do tratamento de dados fins comerciais. Tais informações foram consideradas excessivamente genéricas e pouco esclarecedoras. No entanto, como houve preocupação em listar ao menos 5 hipóteses distintas, o parâmetro foi considerado parcialmente cumprido.

O *Sub-parâmetro (b)*, referente à forma como se dá a utilização, foi considerado atendido. Na mesma seção "Privacidade de Dados Pessoais", de sua Política de Dados, a empresa informa nove hipóteses de utilização dos dados coletados como, por exemplo, para comunicar o cliente sobre sua conta ou para fornecer acesso a determinadas áreas e recursos dos sites:

> "4.1.5 - Tipo de Dados

> 4.1.5.1 - A Algar Telecom utiliza os dados de uso coletados por meio de sites para fins comerciais, incluindo:
> ● Responder as perguntas e pedidos de seus clientes;
> ● Fornecer acesso a determinadas áreas e recursos dos sites;
> ● Verificar a identidade do usuário;
> ● Comunicar com o cliente sobre a sua conta e atividades nos canais de atendimento;
> ● Ajustar conteúdo, anúncios e ofertas fornecidas;
> ● Processar pagamentos por produtos ou serviços;
> ● Melhorar o site e demais canais de atendimento;
> ● Desenvolver novos produtos e serviços;
> ● Processar aplicações e transações."

O **parâmetro III**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, foi considerado, na média, cumprido, pois a empresa fornece informações claras e completas sobre os sub-parâmetros (a), (b), (c) e (i); e cumpre parcialmente os sub-parâmetros (e), (g) e (h).

O ***Sub-parâmetro (a)***, referente ao tempo e local de armazenamento dos dados, foi considerado atendido. Sobre o local de armazenamento, a empresa informa, em sua Política de Privacidade de Dados Pessoais e na Política de Governança de Dados, que armazena os dados em servidores próprios da Algar no Brasil e também em servidores na nuvem.

> 4.1.9 - Servidores de Armazenamento
> Os dados coletados serão armazenados em servidores próprios da Algar Telecom localizados no Brasil, bem como em ambiente de uso de recursos ou servidores na nuvem (cloud computing), o que enseja, neste último caso, transferência ou processamento dos dados fora do Brasil, cumprindo disposições sobre transferência internacional de dados, conforme artigo 33 da Lei Geral de Proteção de Dados ou demais normas aplicáveis.
> Governança dos Dados:
> 4.5.1 - O armazenamento dos dados pessoais pode ser feito de modo físico (guarda de crachás, cartões, fichas, papéis com anotações à mão, formulários, notas fiscais, contratos e outros documentos em papel, por exemplo) ou digital (em mídias como CD, DVD, Blu-Ray, HD externo, pendrive, cartão de memória SD, nas plataformas digitais da Algar Telecom ou em serviço contratado para esta finalidade);
> 4.5.2 - No caso de armazenamento fora do Brasil, a gerência de proteção de dados deve estar atenta para o país em que o hardware se localiza e, localizando-se no exterior, deve-se acionar a área jurídica da Algar Telecom para verificar se há amparo legal e contratual para que os dados pessoais estejam armazenados esse país;
> 4.5.3 - Os meios físicos e digitais de armazenamento dos dados pessoais devem assegurar a sua qualidade, devendo ser mantidos exatos e atualizados, de acordo com a necessidade para o cumprimento da finalidade de tratamento;
> 4.5.4 - Quando o titular dos dados pessoais solicitar a correção ou atualização de seus dados pessoais, o encarregado pelo tratamento de dados pessoais, após análise da requisição, deve acionar as áreas responsáveis para

> assegurar que os meios físicos e digitais onde esses dados pessoais foram replicados e armazenados sejam também atualizados

Tais informações sobre o armazenamento dos dados pessoais foram consideradas satisfatórias.

Quanto ao tempo de armazenamento, no mesmo documento, a empresa informa que mantém dados cadastrais e de identificação por até 5 anos após o término da relação. Quanto aos "outros dados", a empresa afirma armazenar "enquanto durar a relação e não houver pedido de apagamento ou revogação de consentimento":

PRAZO DE ARMAZENAMENTO	FUNDAMENTO LEGAL
Dados cadastrais e de identificação	
5 anos após o término da relação	Art. 12 e 34 do Código de Defesa do Consur
Outros dados	
Enquanto durar a relação e não houver pedido de apagamento ou revogação de consentimento	Art. 9, Inciso II da Lei Geral de Proteção de D Pessoais

Captura de tela de 19.10.2022

Quanto ao *Sub-parâmetro (b)*, referente a quando/se os dados são apagados, foi atendido. Isso porque, a empresa se compromete a apagar os dados "findo o prazo e a necessidade legal" e tendo cumprido a finalidade do tratamento:

> Política de Privacidade dos Dados Pessoais
> 4.2.2 - Exclusão dos Dados
> 4.2.2.1 - Os dados poderão ser apagados antes desse prazo, caso solicitado pelo cliente/usuário. No entanto, pode ocorrer de os dados precisarem ser mantidos por período superior, nos termos do artigo 16 da Lei Geral de Proteção de Dados, para cumprimento de obrigação legal ou regulatória, cumprimento do contrato, transferência a terceiro (respeitados os requisitos de tratamento de dados dispostos na mesma lei);
> 4.2.2.2 - Findo o prazo e a necessidade legal, os dados serão excluídos com uso de métodos de descarte seguro ou utilizados de forma anonimizada para fins estatísticos.
>
> Governança de Dados
> Eliminação dos dados pessoais
>
> 4.9.1 - Os dados pessoais devem ser armazenados por período limitado, levando em consideração a finalidade específica do tratamento;
> 4.9.2 - Após cumprida a finalidade do tratamento e findo o prazo de armazenamento determinado pela tabela de temporalidade, os dados podem ser eliminados de modo seguro, sejam eles registrados em meios físicos ou digitais;

> 4.9.3 - A eliminação dos dados pessoais poderá ser realizada também a pedido do titular do dado ou da Autoridade Nacional de Proteção de Dados;
> 4.9.4 - Para a eliminação dos dados devem ser seguidas as definições indicadas no procedimento de eliminação de dados seguro;
> 4.9.5 - A conservação dos dados pessoais após atingida sua finalidade só será possível nos caso de cumprimento de obrigação legal ou regulatória por parte da Algar Telecom;
> 4.9.6 - A solicitação de eliminação do dado pessoal pelo titular não será possível quando o dado já tiver sido anonimizado;
> 4.9.7 - A solicitação também não poderá ser realizada no caso de cumprimento de obrigação legal quanto ao armazenamento destes dados para fins regulatórios, desde que respeitada a tabela de temporalidade.

O Sub-parâmetro (c), relativo a quais circunstâncias os dados são retidos, foi considerado não atendido. A empresa apenas cita, em seu documento "Governança de Dados", que o tratamento de dados pessoais deve ser realizado considerando o tempo de retenção dos dados pessoais (item 4.2.2 (a)), porém não especifica quais as circunstâncias da retenção.

O Sub-parâmetro (d), relativo às práticas de segurança da empresa, foi considerado atendido. Em sua Política de Privacidade de Dados Pessoais a empresa se compromete, genericamente, na aplicação de medidas de segurança:

> 4.1.8 - Segurança dos Dados
> A Algar Telecom envidará seus melhores esforços para proteção da informação, principalmente dados pessoais, aplicando as medidas de proteção administrativa e técnica necessárias e disponíveis à época, exigindo de seus fornecedores o mesmo nível aceitável de Segurança da Informação, com base em melhores práticas de mercado, a partir de cláusulas contratuais

Tais esforços mencionados na Política de Privacidade são destrinchados na Política de Segurança da Informação da Algar. No documento, a empresa informa se compromete a "garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida" e estabelece uma estrutura para segurança da informação, com informações sobre quem são as pessoas que podem ter acesso aos sistemas da Algar Telecom, os ativos disponibilizados e procedimentos a serem adotados nos sistemas e aplicativos da empresa.

> PROTEÇÃO DE DADOS PESSOAIS
> 10.1. A Algar Telecom respeita a privacidade. Assim, deve garantir a disponibilidade, integridade e confidencialidade dos dados pessoais em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, por meio de:
>
> 10.1.1. Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente;
> 10.1.2. Adoção de medidas de segurança para proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito;
> 10.1.3. Armazenamento de modo seguro, controlado e protegido;

10.1.4. Processos de anonimização e pseudonimização, sempre que necessário;
10.1.5. Protocolos de criptografia na transmissão e armazenamento, sempre que necessário;
10.1.6. Registro lógico das operações de tratamento;
10.1.7. Descarte seguro dos dados pessoais ao término de sua finalidade, ou quando solicitado pelo titular dos dados pessoais, e sua conservação de acordo com as hipóteses legais e regulatórias;
10.1.8. Transferência a terceiros de modo seguro e contratualmente previsto;
10.1.9. Avaliação de impacto e sistemática à privacidade dos titulares de dados;
10.1.10. Gestão e tratamento adequado de incidentes que envolvam dados pessoais;
10.1.11. Testes, monitoramento e avaliações periódicas de sua efetividade

Já em sua Política de Governança de Dados, a empresa informa, com mais detalhes, as práticas de segurança adotadas:

4.17.1 - Durante todo ciclo de vida do dado pessoal devem ser observadas as diretrizes de segurança existentes na Política de Segurança da Informação e Política - Privacidade de Dados da Algar Telecom disponíveis na biblioteca de documentos da Algar Telecom e portal Algar Telecom na internet;
4.17.2 - A área de gestão de segurança da informação deve assegurar a confidencialidade, integridade e disponibilidade do dado pessoal em todos os meios de armazenamento e transmissão de dados pessoais, considerando:
a) Controles técnicos de segurança envolvidos, como, mas não se limitando:
● Firewall;
● Criptografia;
● Uso de VPN para acesso aos dados fora das dependências da Algar Telecom;
● Controles de acesso físico e lógico;
● Autenticação em dois fatores;
● Armazenamento seguro de documentos físicos;
● Gerenciadores de senha.
b) Assegurar que somente pessoas e agentes de tratamento autorizados tenham acesso aos dados pessoais em observância à necessidade e relevância da concessão do acesso;
c) Adoção de medidas de segurança da informação para assegurar que os dados pessoais se mantenham íntegros sem alterações indevidas, exatos, completos e atualizados;
d) Garantia de que os dados pessoais sejam acessíveis e utilizáveis pelas pessoas e entidades autorizadas sempre que sejam necessários;
e) Registro de logs e trilhas de auditoria do ciclo de vida do dado pessoal;
f) Criptografia, pseudonimização e anonimização dos dados pessoais quando for o caso;
g) Treinamento em proteção de dados pessoais e supervisão da adoção das práticas ensinadas.

As informações constantes nos quatro documentos foram considerados suficientes para o sub-parâmetro.

O Sub-parâmetro (e), relativamente a se há Política de Segurança Cibernética/TI publicada com informações sobre proteções específicas contra malware. ransomware, worms e outros vírus, foi considerado parcialmente atendido. Isso porque em seu documento "Segurança da Informação", a empresa cita, no item 17, "Histórico de Alterações", a revisão geral a partir dos requisitos da norma ISO 27001:2013, em 21/10/2019. Porém, não há maiores explicações da aplicação da norma ou da política de segurança cibernética.

O Sub-parâmetro (f), relativamente a quais categorias de colaboradores podem ter acesso aos dados, foi considerado não atendido. Apesar dos controles de acesso serem citados no documento sobre Governança de Dados Pessoais, bem como no documento sobre Segurança da Informação, não há explicação sobre quais as categorias de colaboradores.

O *Sub-parâmetro (g)*, referente aos terceiros com quem os dados são compartilhados, foi considerado parcialmente atendido. Em sua Política Privacidade de Dados e em sua Política de Governança, a empresa informa que "compartilha dados pessoais com parceiros e fornecedores autorizados" e que para que os dados sejam compartilhados é preciso que as partes "tenham firmado contrato com cláusulas referentes à proteção de dados pessoais", mas não determinam quais terceiros podem recebê-los. As informações oferecidas pela empresa foram consideradas insatisfatórias. No entanto, por haver preocupação em apontar informações sobre o tema, com um mínimo de detalhamento, o sub-parâmetro foi considerado parcialmente atendido.

> Política de Privacidade
> 4.1.6 - Compartilhamento
> A Algar Telecom somente compartilha os dados pessoais com parceiros e fornecedores autorizados para atendimento das finalidades informadas nesta política, tendo ainda que compartilhar com terceiros e autoridades dentro das hipóteses de cumprimento de obrigação legal ou regulatória, administração pública, cumprimento do contrato, realização de estudos por órgãos de pesquisa, proteção de crédito ou segurança do cliente/usuário. Nestes casos, a Algar Telecom irá compartilhar o mínimo de informações necessárias para atingir sua finalidade, garantindo sempre que possível, a anonimização dos dados pessoais.
>
> Governança de Dados
> 4.7.1 - O compartilhamento de dados pessoais ou de documentos/arquivos com dados pessoais em território nacional pode ser feito para agentes de tratamento autorizados, com as medidas de segurança indicadas pela área de gestão de segurança da informação a partir do relatório de impacto à proteção de dados pessoais (DPIA/RIPD), quando o caso e somente para as finalidades de uso ou tratamento prévia e devidamente informadas e legitimadas junto ao titular dos dados pessoais;
> 4.7.2 - O compartilhamento de dados pessoais com demais agentes de tratamento, excetuando-se o compartilhamento realizado para cumprimento de obrigações legais, somente poderá ocorrer caso estes tenham firmado contrato com cláusulas referentes à proteção de dados pessoais, conforme disposto no item 4.21 deste documento; 4.7.3 - No caso de impossibilidade de celebração de contrato ou aditivo com a parte em

> questão, um relatório de impacto à proteção dos dados pessoais (DPIA/RIPD) deve ser elaborado e a partir deste relatório devem ser adotados controles mitigatórios em relação à segurança e proteção do tratamento dos dados pessoais;
> 4.7.4 - O compartilhamento de dados pessoais cujo tratamento tenha como hipótese legal o consentimento somente poderá ocorrer com o consentimento do titular dos dados pessoais, com ciência deste compartilhamento, sendo que este deve ser coletado anteriormente ao início do tratamento dos dados pessoais;
> 4.7.5 - Os dados pessoais anonimizados podem ser transferidos para terceiros, desde que respeitados os requisitos de tratamento disposto na legislação aplicável e no presente documento;
> 4.7.6 - O compartilhamento de dados pessoais deve ocorrer somente por canais com medidas de segurança aplicadas

Quanto ao *Sub-parâmetro (h)*, relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi parcialmente atendido. Isso porque as informações trazidas sobre o tema, são pouco claras e afirmam apenas que são realizadas para "atendimento das finalidades informadas nesta política". Não são dadas informações mais claras sobre as hipóteses de compartilhamento e suas finalidades. No entanto, por haver preocupação em apontar informações sobre o tema, com um mínimo de detalhamento, o sub-parâmetro foi considerado parcialmente atendido.

Quanto ao *parâmetro (i)*, relativo às hipóteses de transferência internacional de dados, considerou-se atendido. Em sua Governança de Dados, a empresa informa, de maneira bastante completa, sobre as condições e as finalidades para a transferência internacional de dados:

> 4.8.1 - Caso os dados pessoais tenham a previsão de serem transferidos para outro país, a possibilidade de compartilhamento com outro controlador deverá ser submetida à análise do encarregado pelo tratamento de dados pessoais (DPO), pela área de gestão de segurança da informação e a área jurídica, de modo que possam avaliar se o país de destino possui grau de proteção de dados que esteja adequado ao ordenamento jurídico brasileiro;
> 4.8.2 - Se o controlador receptor oferecer e comprovar garantias de cumprimento dos direitos do titular, a transferência internacional de dados também poderá ser possível na forma de
> (i) cláusulas contratuais específicas para determinada transferência;
> (ii) cláusulas-padrão contratuais;
> (iii) normas corporativas globais; e
> (iv) selos, certificados e códigos de conduta emitidos pela Autoridade Nacional de Proteção de Dados;
>
> 4.8.3 - A transferência internacional de dados pessoais também pode ocorrer a partir das finalidades elencadas abaixo:
> a) Quando a transferência for necessária para a proteção da vida do titular ou de terceiros;
> b) Quando a Autoridade Nacional autorizar a transferência;
> c) Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

d) Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente está de outras finalidades;
e) Para cumprimento de obrigação legal ou regulatória pela Algar Telecom;
f) Quando necessária para execução de contrato e procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

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

O **Sub-parâmetro (a)**, referente à informação sobre quais são e os meios para exercício dos direitos dos titulares sobre seus dados, foi considerado atendido. Isso porque a empresa informa, em sua Privacidade de Dados Pessoais, o e-mail e o nome do responsável pelo tratamento dos dados (DPO).

O Sub-parâmetro (b), referente à informação aos titulares sobre seus direitos segundo a LGPD, foi considerado atendido. A empresa, em sua Privacidade de Dados Pessoais, reserva um item para informar sobre os direitos dos titulares:

4.3 - Direitos do Titular dos Dados Pessoais
4.3.1 - Direitos Básicos
O cliente/usuário poderá solicitar ao nosso Encarregado de Dados Pessoais a confirmação da existência tratamento de Dados Pessoais, além da exibição ou retificação de seus Dados Pessoais, por meio do nosso Canal de Atendimento.

4.3.2 - Limitação, Oposição e Exclusão de dados
Pelos Canais de Atendimento, o cliente/usuário poderá também requerer:
● A limitação ou anonimização do uso de seus Dados Pessoais;
● Manifestar sua oposição e/ou revogar o consentimento quanto ao uso de seus Dados Pessoais;
● Solicitar a exclusão de seus Dados Pessoais que tenham sidos coletados e registrados pela Algar Telecom, desde que decorrido o prazo legal mínimo relacionado à guarda de dados; ou,
● A portabilidade dos dados a outro prestador de serviços de telecomunicação, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional;
● Cancelar os comunicados de marketing que enviamos quando desejar.

As informações foram consideradas satisfatórias para atender ao sub-parâmetro.

O **parâmetro V**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado **parcialmente atendido**. Embora a empresa tenha respondido dentro do prazo determinado, afirmou não tratar dados pessoais para a conta indicada, que possui plano com a operadora, sem maiores explicações. Consideramos, assim, a resposta insuficiente.

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 empresa inclui em seu site o seguinte aviso:

> A Algar Telecom reserva a si o 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 ao cliente/usuário verificá-lo junto à Algar Telecom através do site www.algartelecom.com.br. Caso seja necessário alteração da Política, o cliente/usuário será informado via e-mail.

Por fim, o **parâmetro VII**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado atendido. A empresa dispõe de uma seção intitulada "Privacidade e Segurança da Informação", que pode ser acessado no rodapé de seu site[50], onde constam as Políticas de Privacidade de Dados, Gestão de Serviços, Segurança da Informação, Governança de Dados Pessoais, Uso de Cookies, Termo de Uso de Serviços e Termo de Uso do Site. As informações que constam nos documentos são claras e de fácil acesso ao cliente.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ★

Nesta categoria, a Algar obteve **estrela cheia**, pois atendeu aos parâmetros I, II, IV e V

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado cumprido. No documento Compartilhamento de Dados Pessoais com Autoridades, a empresa informa que apenas fornece dados cadastrais às autoridades administrativas por força da lei ou mediante ordem judicial. As autoridades competentes para as quais a empresa oferece dados são Ministérios Públicos, Autoridades Policiais, Receita Federal e Presidência de Comissões Parlamentares de Inquérito, em conformidade com as previsões legais aplicáveis que autorizam a quebra de sigilo. Tais informações foram consideradas suficientes para fins desta avaliação.

O **parâmetro II**, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, foi considerado atendido. Além de mencionar as autoridades competentes (vide parâmetro acima), a empresa informa quais são as hipóteses legais em que a empresa fornece dados cadastrais às autoridades legais:

> Constituição Federal de 1988 – artigo 5º. Inciso XII e artigo 58, par. 3º.;
> - Lei 9296/1996 – artigo 1º., parágrafo único – Lei da Interceptação Telefônica;
> - Lei 9472/1997 – artigo 3º. – Lei Geral das Telecomunicações;
> - Lei 12.683/2012 – artigo 7º., "B" – Lavagem de Dinheiro

[50] Ver: https://algartelecom.com.br/politicas/politica-dados.html

> - Lei 12.830/2013 – artigo 2º. – Investigação Criminal conduzida por Delegado de Polícia
> - Lei 12850/2012 – artigo 15 – Organização Criminosa
> - Lei 12.695/2014 – artigo 7º. e 10 - Marco Civil da Internet
> - Lei 13.344/2016 – artigo 13-B – Busca de Pessoa Desaparecida
> - Resolução Anatel 632/2014 –artigo 3º. V – Regulamento Geral de Direitos do Consumidor de Telecomunicações.

O **parâmetro III**, referente ao oferecimento de informações sobre dados de geolocalização, também não foi considerado atendido. Não foi encontrada menção ao tema nos documentos analisados da Algar.

O **parâmetro IV**,referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, foi considerado atendido. No documento Compartilhamento de Dados Pessoais com Autoridades, a empresa faz a diferenciação entre dados cadastrais e registros de conexão, bem como suas as hipóteses de fornecimento dos dados:

> No que se refere à disponibilização de dados cadastrais para a apuração de crimes, a Algar Telecom fornece dados cadastrais relativos à qualificação pessoal, filiação e o endereço mediante ordem judicial. A Algar Telecom disponibilizará dados cadastrais a Delegados de Polícia ou o Ministério Público quando relativos à qualificação pessoal, filiação e o endereço, mediante requisição, sem ordem judicial, em consonância com o artigo 15, da Seção IV da Lei 12.850/2013, da Lei 9.613/98 (artigo 17-B, Capítulo X) e do artigo 13-A do Código de Processo Penal.
>
> Registros de conexão, como tal entendido como 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 serão informados pela Algar Telecom mediante a apresentação de ordem judicial ou, mediante requisição do Delegados de Polícia ou O Ministério Público, em conformidade com o artigo 15, da Seção IV da Lei 12.850/2013, da Lei 9.613/98 (artigo 17-B, Capítulo X) e do artigo 13-A do Código de Processo Penal.
>
> A Algar disponibiliza informações reais ou pretéritas, apenas mediante ordem judicial.

Por fim, o **parâmetro V**, relativo à existência de protocolos específicos sobre entrega de dados ao Estado, foi considerado atendido. A empresa disponibiliza em sua Política de Dados um documento denominado “Compartilhamento de Dados Pessoais com Autoridades”, em que a empresa informa hipóteses específicas de entregas de dados ao Estado. Tal documento foi considerado suficiente para fins desta avaliação.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: ★

Nesta categoria, a Algar obteve **meia estrela**, pois não atendeu a um dos parâmetros.

Quanto ao **parâmetro I**, referente à contestação de legislação, realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte, foi considerado cumprido.

Em 29/03/2022, o STF publicou o julgamento da Ação Direta de Inconstitucionalidade número 4924/DF[51], em que a Associação Nacional das Operadoras Celulares - ACEL, da qual a Algar faz parte, pediu pela declaração de inconstitucionalidade da Lei 17.107/12, do Estado do Paraná, que dispõe sobre penalidades ao responsável pelo acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres (trote telefônico). A lei visava estabelecer obrigação às operadoras de telefonia de fornecer os dados dos proprietários de linhas telefônicas que acionem indevidamente os serviços de atendimento diante de mero ofício por qualquer órgão ou instutuição pública envolvida. A ACEL argumentou em favor da inviolabilidade da intimidade, vida privada horna e do sigilo das comunicações telefônicas (segundo estabelecido no artigo 5º, incisos X e XII da Constituição Federal), mencionando a indisponibilidade do direito à proteção de dados pessoais em sua argumentação.

Além disso, a ACEL havia ajuizado a ADI 5040/PI[52], publicada em 2021 (não incluída em nosso relatório anterior), em que questionava a legalidade da Lei Nº 6.336/2013 do Estado do Piauí, que obrigava as empresas prestadoras de serviço de telefonia móvel pessoal a fornecerem, aos órgãos de segurança pública, dados relativos à localização de telefones celulares e cartões "SIM" que tivessem sido objeto de furto, roubo e latrocínio ou utilizados na prática de delitos. Entre seus argumentos, a ACEL também alegou grave ofensa à privacidade de seus clientes na hipótese de divulgação das informações pessoais, citando a Constituição e o direito fundamental à privacidade, além da inviolabilidade do sigilo telefônico.

Também, em 30/08/2019, o STF julgou a Ação Direta de Inconstitucionalidade número 4401/MG[53], em que a Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competititvas - TELCOMP, da qual a Algar faz parte, pediu a declaração de inconstitucionalidade dos artigos 1º a 4º da Lei 18.721/10, do Estado de Minas Gerais,que dispõe sobre o fornecimento de informações por concessionária de telefonia fixa e móvel para fins de segurança pública. A lei visava a obrigatoriedade das empresas "a fornecer informações sobre a localização de aparelhos de clientes à polícia judiciária do Estado, mediante solicitação, ressalvado o sigilo do conteúdo das ligações telefônicas." (art. 1º, caput). A TELCOMP argumentou pela inconstitucionalidade das normas estaduais em função de usurpação de competência legislativa, pois a legislação sobre telecomunicações seria de competência privativa da União.

Por fim, para averiguação do **parâmetro II**, referente à contestação de pedidos abusivos, 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 "Algar Telecom E sigilo E quebra" e por acórdãos publicados entre 01/08/2020 e 21/06/2021. Nas buscas, não foram localizadas quaisquer ações nesse

[51] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183

[52] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4461936

[53] Acesso em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=3860438

sentido. Ressaltamos que a escolha pelo Jusbrasil como fonte secundária se dá pelo fato de agregar julgados de todos os tribunais estaduais brasileiros, em detrimento da busca em todos os tribunais individualmente.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, a Ação Direta de Inconstitucionalidade (ADI) 5642[54], da ACEL, não foram consideradas, já que não registraram movimentações.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Algar obteve meia **estrela,** pois atendeu a um parâmetro.

Não foi encontrada nenhuma participação da empresa em quaisquer consultas públicas ou como *amicus curiae* em processos relativos à aprovação de normas ou adoção de técnicas que aumentem a proteção conferida aos usuários dos seus serviços.

O **parâmetro I**, relativo ao posicionamento em geral da empresa, foi considerado atendido. Em algumas oportunidades ao longo do ano, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários.

A Algar participou, por meio da Conexis do lançamento do Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações, apresentado à Autoridade Nacional de Proteção de Dados[55].

Consideramos o **parâmetro II** não atendido. Não encontramos qualquer posicionamento público da Algar com relação à proteção de dados pessoais relativa às tecnologias de reconhecimento facial. Tampouco identificamos qualquer participação, em consultas públicas ou como *amicus curiae*, em processos da ANATEL ou do STF. A empresa, na fase de engajamento conosco, também não mostrou evidências de que não utilize a tecnologia em suas contratações.

---

[54] A Associação Nacional das Operadoras Celulares (Acel), da qual algumas operadoras fazem parte, ajuizou a Ação Direta de Inconstitucionalidade (ADI) 5642, no Supremo Tribunal Federal (STF), para impugnar dispositivo da Lei 13.344/2016, que confere a delegados de polícia e membros do Ministério Público a prerrogativa de requisitar informações e dados necessários à investigação criminal nos casos de tráfico de pessoas, independentemente de autorização judicial. A ACEL pede a concessão de liminar para que o STF dê à Lei 13.344/2016 interpretação conforme a Constituição Federal de modo a impedir entendimento que leve a medidas como interceptação telemática e de voz, localização de terminal ou IMEI (Identificação Internacional de Equipamento Móvel) de cidadão em tempo real por meio de ERB, extrato de ERB, dados cadastrais de usuários de IP, extratos de chamadas telefônicas e SMS, entre outros dados de caráter sigiloso. No mérito, pede a declaração de inconstitucionalidade parcial do dispositivo questionado.

[55] Acesso em: https://www.telesintese.com.br/operadoras-criam-codigo-de-boas-praticas-de-protecao-de-dados/

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

Resultado: ☆

Nesta categoria, a Algar obteve **estrela vazia,** pois atendeu aos parâmetros I, II e III.

O **parâmetro I** não foi considerado atendido. Embora a empresa publique relatório de sustentabilidade em seu portal, ele não foi considerado suficiente para preencher o critério por não ter informações a respeito de solicitações do governo (por exemplo, em relação a requerimentos de dados de usuários, ou bloqueios de conteúdos).
O **parâmetro II** foi considerado não atendido.

O **parâmetro III** foi considerado não atendido.

O **parâmetro IV** foi considerado não atendido. Não há informações, no Relatório de Transparência, acerca de pedidos de acessos a dados.

Por fim, o **parâmetro V**, relativo à publicação de Relatórios de Impacto à Proteção de Dados, não foi considerado atendido. Não foram localizados quaisquer documentos nesse sentido em nossas buscas.

CATEGORIA 6: Notificação do usuário

Resultado: ☆

A Algar não obteve estrela, pois não há menção à possibilidade de notificação do usuário em qualquer um dos documentos analisados.

BRISANET

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a Brisanet Banda Larga obteve **três quartos de estrela**, tendo atendido 4 dos sete parâmetros analisados.

Quanto ao **parâmetro I**, consideramos o seguinte:

Sub-parâmetro (a): parcialmente atendido. Em sua Política de Privacidade, no item "Sobre os dados que coletamos", a empresa informa diversos tipos de dados, cadastrais (nome completo, CPF, RG, e-mail, telefone residencial, celular, endereço, tipo de moradia, data de nascimento, estado civil, tipo de público) e de identificação digital (endereço IP e porta lógica de origem, versão do sistema operacional do dispositivo, geolocalização, registro de data e hora de ações realizadas, telas acessadas, ID de sessão, cookies) coletados. No entanto, não há discriminação completa de todos os dados coletados. Não sabemos, por exemplo, quais dados são coletados por meio de cookies quando da navegação do site da Brisanet.

Sub-parâmetro (b): parcialmente atendido. A Política apenas menciona que os dados "poderão ser coletados quando você os submete ou interage com nosso Site e serviços". No entanto, a redação é excessivamente genérica, não sendo exaustiva em relação a quais dados são coletados em cada situação, de que forma se dá a coleta durante a própria prestação dos serviços da Brisanet, quais são as hipóteses apontadas no "dentre outros" da redação da própria política da empresa etc.

Sub-parâmetro (c): não atendido. A Política de Privacidade da Brisanet não faz referência à coleta de dados públicos dos titulares de dados.

Sub-parâmetro (d): não atendido. A Política de Privacidade da Brisanet não faz menção à coleta de dados por meio de terceiros, e 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**, consideramos o seguinte:

Sub-parâmetro (a): parcialmente atendido. Em sua Política de Privacidade, no item "Sobre os dados que coletamos", a empresa informa as finalidades associadas aos tipos de dados (cadastrais ou de identificação digital), mas não há uma correlação estrita de quais dados são empregados para cada finalidade. Sendo assim, os titulares de dados não podem ter certeza de que o tratamento de todos os seus dados está ocorrendo com finalidades e bases legais legítimas.

No Contrato de Prestação de Serviços de Banda Larga da Brisanet, encontramos o seguinte:

> *"12.1.2 A CONTRATADA se compromete a utilizar os dados pessoais do CLIENTE e demais informações coletadas para as seguintes finalidades, com as quais o CLIENTE expressamente declara ter pleno conhecimento e concordância ao aderir ao presente contrato, seja através de TERMO DE CONTRATAÇÃO (presencial ou eletrônico) ou outras formas de adesão previstas no presente Contrato: (i) para cumprimento de obrigação legal ou regulatória, incluindo mas não se limitando à manutenção dos dados cadastrais e os Registros de Conexão do CLIENTE pelo prazo mínimo de 01 (um) ano, nos termos da Lei n.o 12.965/2014 (Marco Civil da Internet); e a manutenção da gravação das ligações do CLIENTE para o Centro de Atendimento ao Cliente disponibilizado pela CONTRATADA; (ii) para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis, decretos e regulamentos do Poder Público, ANATEL, ou qualquer outro órgão público, autarquia ou autoridade Federal, Estadual ou Municipal; (iii) para o fiel cumprimento ou execução de quaisquer direitos ou deveres inerentes ao presente contrato, ou de procedimentos preliminares relacionados ao presente contrato; (iv) para o exercício regular de direitos em processo judicial, administrativo ou arbitral;(v) para a proteção do crédito (incluindo medidas de cobrança judiciais ou extrajudiciais); (vi) para garantir o cumprimento do presente contrato, incluindo o combate à fraude ou a prática de quaisquer ilícitos; (vii) para enviar ao CLIENTE qualquer comunicação ou notificação prevista no presente contrato; (viii) e para seu legítimo interesse."*

Muito embora haja descrição mais detalhada de finalidades, o titular de dados ainda não dispõe de ferramentas para compreender quais de seus dados serão empregados em cada processo realizado pela Brisanet, especialmente nas hipóteses de legítimo interesse.

Já o Contrato de Adesão ao Serviço de Internet Móvel Pré Pago da Brisanet, único outro contrato disponível no site da Brisanet, não conta com similares disposições referentes à privacidade.

Sub-parâmetro (b): integralmente atendido. Contanto que as formas de utilização listadas na Política de Privacidade da Brisanet correspondam a todas suas formas de tratamento de dados, a listagem encontrada no item "Sobre os dados que coletamos" será considerada suficiente. Contudo, conforme acima, a Política não associa as formas de tratamento aos dados especificamente tratados pela Brisanet em cada processo, o que é necessário para a avaliação do titular sobre a legitimidade do processamento de seus dados.

Quanto ao **parâmetro III**, consideramos o seguinte:

Sub-parâmetro (a): atendido. A Política de Privacidade, no item "Como armazenamos seus dados pessoais e o registro de atividades", traz uma listagem de prazos de armazenamento, informando o período e o fundamento legal.

Sub-parâmetro (b): não atendido. A empresa não informa em que ocasiões realiza a deleção de determinados tipos de dados (ex.: dados sensíveis), ou se o faz com regularidade.

Sub-parâmetro (c): atendido. Conforme acima, a Política de Privacidade cita hipóteses de retenção de dados.

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): não atendido. Não identificamos informações sobre as medidas específicas de segurança cibernética empregadas pela empresa. O Contrato de Prestação de Serviços de Banda Larga afirma, apenas, que, entre as obrigações da Brisanet está "*3.2.4 [...] zelar pelo sigilo inerente aos serviços de telecomunicações e pela confidencialidade dos dados, inclusive registros de conexão, e informações do Assinante, empregando todos os meios e tecnologia necessários para tanto"*.

Sub-parâmetro (f): não atendido. Não identificamos informações sobre as medidas específicas relativas ao controle de acessos empregadas pela empresa.

Sub-parâmetro (g): parcialmente atendido. No item "Como compartilhamos dados e informações", a Política de Privacidade da Brisanet menciona algumas hipóteses de compartilhamento de dados de clientes com terceiros. No entanto, não há especificação de quais terceiros em específico recebem dados de titulares da Brisanet.

No Contrato de Prestação de Serviços de Banda Larga da Brisanet, encontramos o seguinte:

> *"12.3. A BRISANET e empresas do mesmo Grupo Econômico poderão, a qualquer tempo, consultar suas informações – incluindo seus dados pessoais, histórico de crédito, entre outros – no Cadastro Positivo, Órgãos Reguladores, Birôs de Crédito ou outras entidades que prestam serviço para fins de proteção ao crédito. Desse modo, O ASSINANTE autoriza que todo o conglomerado BRISANET consulte débitos e responsabilidades decorrentes de operações com características de crédito.*
> *12.4 O CLIENTE reconhece e concorda que a PRESTADORA está sujeita à supervisão das autoridades e entidades regulatórias do Brasil, e, ainda, autoriza que as suas informações sejam divulgadas para estas autoridades e entidades regulatórias."*

O titular de dados, no entanto, não conta com informações sobre as circunstâncias em que os dados são compartilhados com tais entidades - e tampouco com um detalhamento de quais tipos de dados podem ser divulgados (e.g. "entre outros"). Já o Contrato de Adesão ao Serviço de Internet Móvel Pré Pago da Brisanet, único outro contrato disponível no site da Brisanet, não conta com similares disposições referentes ao compartilhamento com terceiros.

Sub-parâmetro (h): parcialmente atendido. No item "Como compartilhamos dados e informações", a Política de Privacidade da Brisanet indica todas as finalidades de compartilhamento com os terceiros citados. No entanto, algumas das finalidades são excessivamente genéricas e não permitem ao usuário avaliar a legitimidade do compartilhamento (ex.: "com empresas parceiras e prestadores de serviços necessários à execução dos nossos serviços e funcionalidades").

Sub-parâmetro (i): não atendido. A Política de Privacidade da Brisanet apenas menciona que alguns dados serão armazenamdos 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.

Quanto ao **parâmetro IV**, consideramos o seguinte:

Sub-parâmetro (a): integralmente atendido. Na Política de Privacidade, no item "Canais de atendimento", a empresa informa os canais de atendimento, horários e endereços que poderão ser

acionados pelo titular de dados para reclamar seus direitos. Há, inclusive, um canal específico para contato com o Encarregado de Dados da empresa.

Sub-parâmetro (b): não atendido. Na Política de Privacidade, no item "Quais são os seus direitos e como exercê-los", a Brisanet informa aos titulares de dados sobre alguns de seus direitos. O site não contém, no entanto, descrição clara e acessível de todos os direitos de titular conferidos pelos artigos 8º e 9º da LGPD, além de todos os direitos compreendidos nos incisos do artigo 18 da mesma lei. Os direitos citados só incluem, genericamente, "a limitação do uso de seus dados pessoais', "manifestar sua oposição ou revogar o consentimento quanto ao uso [dos dados]". e "solicitar a exclusão de seus dados pessoais".

Além disso, o Contrato de Prestação de Servicos de Banda Larga da Brisanet traz a seguinte redação:

> *"12.6 Sem prejuízo do disposto nos itens acima, a privacidade e confidencialidade deixam de ser obrigatórias, se comprovado documentalmente que as informações relacionadas aos dados pessoais do CLIENTE e demais informações coletadas: (i) Estavam no domínio público na data celebração do presente Contrato; (ii) Tornaram-se partes do domínio público depois da data de celebração do presente contrato, por razões não atribuíveis à ação ou omissão das partes; (iii) Foram reveladas em razão de qualquer ordem, decreto, despacho, decisão ou regra emitida por qualquer órgão judicial, legislativo ou executivo que imponha tal revelação. (iv) Foram reveladas em razão de solicitação da Agência Nacional de Telecomunicações – ANATEL, ou de qualquer outra autoridade investida em poderes para tal."*

Ressaltamos que, na condição de Controladora de Dados Pessoais, a Brisanet é obrigada ao cumprimento da legislação de proteção de dados, inclusive quando do tratamento de dados públicos - conforme especificado nos parágrafo 7º do artigo 7º da LGPD. A saber:

> *"§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º* [dados feitos manifestamente públicos pelo titualr] *deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei."*

A inclusão da cláusula, portanto, é inadequada diante das obrigações da Brisanet em cumprir com os direitos de titular, induzindo-o ao erro quanto à possibilidade de reclamação de seus direitos.

Quanto ao **parâmetro V**, consideramos o seguinte: **não atendido**. No Centro de Privacidade da Brisanet, a empresa disponibiliza um espaço nomeado "Acesso os seus dados", onde os usuários podem selecionar as opções de solicitação de dados para "Clientes Brisanet", "Titulares não clientes ou ex-clientes" e "Colaboradores e ex-funcionários". Enquanto a disponibilização das informações aos Clientes se dá, supostamente, por meio do aplicativo "Brisacliente", as demais categorias de titular são redirecionadas ao preenchimento de um Formulário, que deve ser enviado por correio à sede da Brisanet no Ceará. O documento informa que a Brisanet responderá à solicitação em 15 (quinze) dias do recebimento do formulário. Além disso, há exigência no Formulário de que o titular envie (i) cópia autenticada de documento de identificação que possua foto; e (ii) firma reconhecida por cartório na assinatura do Formulário.Tal exigência não encontra respaldo qualquer na legislação de proteção de dados, e configura uma barreira desnecessária para o exercício de direitos do titular de dados pessoais. Além disso, a tentativa de contato via email ao DPO para solicitação da confirmação de tratamento não foi respondida, nem no prazo legal de 15 (quinze) dias nem no prazo estendido de 1 (um) mês.

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**. Em sua Política de Privacidade, a empresa afirma explicitamente que "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." O trecho prossegue informando ao titular de dados que uma notificação apenas será enviada quando das "atualizações neste documento e que demandem nova coleta de consentimento" , 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**. No rodapé da página inicial do site da Brisanet, há o link para a Central de Privacidade da Empresa. As informações que constam no Portal de Privacidade são bastante claras e de fácil acesso ao cliente.

captura de tela de 18.10.2022

No entanto, não há disponibilização pública do contrato de prestação de serviços de internet banda larga, e a disposição de tais informações no contrato seria recomendável para que estas pudessem ser acessadas por todos os clientes, consentidas legalmente por eles, e pormenorizadas de acordo com cada tipo de serviço contratado. Obtivemos acesso ao contrato de prestação de serviços de banda larga da Brisanet apenas diante de solicitação direta de disponibilização pelo atendimento ao cliente (via Whatsapp).

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ☆

Nesta categoria, a Brisanet obteve **estrela vazia,** não tendo cumprido 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 menciona somente 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 identificado no Centro de Privacidade da Brisanet.

No Contrato de Prestação de Serviços de Banda Larga da Brisanet, encontramos o seguinte:

> *"12.1.4 A CONTRATADA apenas tornará disponíveis os dados cadastrais e os registros de conexão, incorrendo em suspensão de sigilo de telecomunicações, quando solicitado formalmente pela autoridade judiciária ou outra legalmente investida desses poderes, e quando taxativamente determinada a apresentação de informações relativas ao CLIENTE."*

Embora a redação destine-se a estabelecer as hipóteses de compartilhamento de dados com as autoridades, a Brisanet não faz menção à necessidade estrita de ordem judicial para a quebra de sigilo, e tampouco descreve as hipóteses legais específicas que autorizariam o compartilhamento de dados sem ordem judicial.

O **parâmetro II**, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, também foi considerado **não atendido**. Não localizamos essas informações nos contratos ou documentos da Brisanet.

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

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, 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 da Brisanet.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: ★

Nesta categoria, a Brisanet Banda Larga obteve **estrela cheia**, pois atendeu aos dois parâmetros analisados.

Quanto ao **parâmetro I**, referente à contestação de legislação, realizamos buscas exploratórias nos sites do Supremo Tribunal Federal e do Superior Tribunal de Justiça por processos em que a empresa fosse parte, buscando ações envolvendo a contestação de legislação que viola princípios de privacidade e proteção de dados. O parâmetro foi considerado **atendido**.

Em 30/08/2019, o STF julgou a Ação Direta de Inconstitucionalidade número 4401/MG, em que a Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competititvas - TELCOMP, da qual a Brisanet faz parte, pediu a declaração de inconstitucionalidade dos artigos 1º a 4º da Lei 18.721/10, do Estado de Minas Gerais,que dispõe sobre o fornecimento de informações por concessionária de telefonia fixa e móvel para fins de segurança pública. A lei visava a obrigatoriedade das empresas "a fornecer informações sobre a localização de aparelhos de clientes à polícia judiciária do Estado, mediante solicitação, ressalvado o sigilo do conteúdo das ligações telefônicas." (art. 1º, caput). A TELCOMP argumentou pela inconstitucionalidade das normas estaduais em função de usurpação de competência legislativa, pois a legislação sobre telecomunicações seria de competência privativa da União.

Por fim, para averiguação do **parâmetro II**, referente à contestação de pedidos abusivos, realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado do Ceará pelo nome da Parte "Brisanet" e no portal "Jusbrasil", pelos termos "Brisanet S/A" E "sigilo" E "quebra" e por sentenças ou acórdãos com data de distribuição entre 31/06/2021 e 19/10/2022. Nas buscas, não foram localizadas quaisquer ações de acesso público envolvendo a solicitação de quebra de sigilo de clientes da Brisanet.

Encontramos, no entanto, ao menos uma ação em que a Brisanet é intimada a responder ao Ministério Público do Estado do Ceará em Carta Precatória Criminal[56] e uma ação relacionada à Proteção de Dados Pessoais[57]. Todavia, nenhuma das peças processuais em ambas as ações estão disponíveis ao público.

Por meio da busca no Jusbrasil, identificamos ao menos uma ação em que a Brisanet recusa um pedido de quebra de sigilo, baseando-se nos termos do Marco Civil da Internet:

> *"[A] provedora BRISANET SERVIÇOS DE TELECOMUNICAÇÕES S.A respondeu ao ofício expedido pelo Juízo da 10ª Vara do Trabalho nos seguintes termos:*
> *'Dessa forma, a Brisanet Serviços de Telecomunicações S/A, informa que não realiza a guarda de registro das conexões WI-FI dos clientes, com base no artigo 14 da lei 12.965.*
> *[...]*
> *Sendo assim, não possuímos o registro de conexões de quem utilizou ou não o WI-FI do cliente. Pois conforme já mencionado acima, o provedor de conexão (BRISANET) somente realiza buscas mediante o acesso de determinado IP. Logo, cabe ao provedor de aplicação armazenar os registros de acesso a aplicações de internet, que consistem no conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. Com a informação do provedor de aplicação, qual seja, a hora, o segundo, o dia e o IP que foi utilizado para acessar determinado site, o provedor de conexão conseguirá localizar aquele determinado usuário."*

Ressaltamos que a escolha pelo Jusbrasil como fonte secundária se dá pelo fato de agregar julgados de todos os tribunais estaduais brasileiros, em detrimento da busca em todos os tribunais individualmente.

---

[56] Acesso em: https://esaj.tjce.jus.br/cpopg/show.do?processo.código=41000022I0000&processo.foro=145 processo.número=0010012-18.2022.8.06.0145

[57] Acesso em: https://esaj.tjce.jus.br/cpopg/show.do?processo.codigo=4N00023K30000&processo.foro=167&processo.numero=0204217-78.2022.8.06.0167

CATEGORIA 4: Postura pública pró-privacidade

Resultado: ☆

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

O **parâmetro I**, relativo ao posicionamento em geral da empresa, foi considerado **não atendido**. Em algumas oportunidades ao longo do ano, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários. Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido.

Também consideramos o **parâmetro II não atendido**. Não encontramos qualquer posicionamento público da Brisanet com relação à proteção de dados pessoais relativa às tecnologias de reconhecimento facial. Tampouco identificamos qualquer participação, em consultas públicas ou como *amicus curiae*, em processos da ANATEL ou do STF. Uma matéria redigida pelo Idec, no entanto, cita a Brisanet como uma das responsáveis pela instalação de câmeras de reconhecimento dacial na Paraíba, em 2019:

> *"Na Paraíba, houve teste durante aquele que é considerado o "maior São João do mundo", na cidade de Campina Grande. A Medow Entertainment, empresa organizadora do evento, contratou a plataforma digital Facewatch, que usou câmeras de reconhecimento facial em todas as entradas do Parque do Povo durante os 31 dias de festa. A operadora Brisanet também participou da operação. Foram instaladas 265 câmeras capazes de encontrar uma pessoa com um zoom de até dois quilômetros de distância, noticiou a Secretaria de Segurança Pública. Soldado da Polícia Militar da Paraíba, Jimmy Felipe, também Gerente de Projetos do órgão, disse à reportagem que mais de 800 mil rostos foram gravados. Desse total, "300 pessoas foram cadastradas. Delas, 12 foram presas. Uma só era irmã gêmea [de um procurado], o que mostra que o sistema foi suficiente. Não foram feitos armazenamentos de pessoas que não estavam nessa base de dados ou que não tinham nenhum tipo de envolvimento, nenhuma busca na polícia", afirma. Felipe acrescenta que "os dados que não tiveram correlação aos procurados foram descartados após 24h".*

Também nessa categoria, convidamos as empresas, nessa fase de envio e discussão dos resultados preliminares do relatório, a compartilharem conosco ações judiciais ou posicionamentos e ações reportadas na mídia em que tenham atuado na promoção da proteção dos dados pessoais, inclusive com respeito ao reconhecimento facial.

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

Resultado: ☆

Nesta categoria, a Brisanet obteve **estrela vazia,** pois não atendeu a nenhum dos parâmetros.

Os **parâmetros I ao IV**, relativos ao Relatório de Transparência, **não foram atendidos**. Não foram localizados documentos desta natureza da Brisanet, e o Relatório de Sustentabilidade da Brisanet não traz informações relevantes sobre privacidade e proteção de dados ou sobre os pedidos de

autoridades públicas em relação a dados pessoais. Além disso, o Relatório de Sustentabilidade possui link para as políticas da empresa, listando a existência de uma "Política de Informação" que não é disponibilizada no site[58].

O **parâmetro V**, por sua vez, relativo à publicação de Relatórios de Impacto à Proteção de Dados, também foi considerado **não atendido**. Não foram localizados quaisquer documentos nesse sentido em nossas buscas.

CATEGORIA 6: Notificação do usuário

Resultado: ☆

A Brisanet não obteve estrela, pois não há menção à possibilidade de notificação do usuário em qualquer um dos documentos analisados.

[58]Acesso em: https://ri.brisanet.com.br/governanca-corporativa/estatuto-codigo-de-etica-e-politicas/2022