

QUEM DEFENDE SEUS DADOS?

2021

INTERNETLAB
pesquisa em direito e tecnologia

E ELECTRONIC
FRONTIER
FOUNDATION **FF**

SUMÁRIO

| | |
|---|-----------|
| I. INTRODUÇÃO..... | 3 |
| II. METODOLOGIA E RESULTADO GERAL | 4 |
| III. CATEGORIAS | 6 |
| CATEGORIA 1: Informações sobre a política de proteção de dados..... | 6 |
| CATEGORIA 2: Protocolos de entrega de dados para investigações | 7 |
| CATEGORIA 3: Defesa dos usuários no Judiciário | 10 |
| CATEGORIA 4: Postura pública pró-privacidade | 11 |
| CATEGORIA 5: Relatórios de transparência e de impacto à proteção de dados | 12 |
| CATEGORIA 6: Notificação do usuário | 14 |
| IV. RESULTADOS | 16 |
| CLARO MÓVEL..... | 16 |
| NET | 29 |
| OI BANDA LARGA..... | 41 |
| OI MÓVEL | 61 |
| TIM BANDA LARGA..... | 81 |
| TIM MÓVEL..... | 97 |
| VIVO BANDA LARGA | 113 |
| VIVO MÓVEL..... | 126 |
| ALGAR..... | 138 |
| BRISANET MÓVEL | 155 |
| BRISANET BANDA LARGA | 162 |

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 lançará em 2021 a sexta 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 Latina¹. 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 inúmeras notícias sobre incidentes de segurança ocorridos com as maiores operadoras de telefonia no ano passado. Além disso, atualizamos quais empresas de telefonia são avaliadas pelo relatório. Com base em levantamento recente da Anatel², selecionamos, em junho/2021, todas as empresas com mais de 1% do mercado nacional de telefonia. Com isso, passou-se a avaliar a empresa Brisanet e deixou-se de avaliar a Sky. A Nextel, por ter sido completamente assimilada pela Claro, não sendo mais oferecidos serviços sob sua marca, também deixou de ser avaliada.

Com as mudanças, 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 que vêm despontando na indústria. 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-isp-care-about-their-users-privacy>; México: <https://www.eff.org/deeplinks/2015/06/new-report-shows-which-mexican-isp-stand-their-users>; Paraguai: <https://qtdt.tedic.org>; Chile: <https://www.derechosdigitales.org/publicaciones/quien-defiende-tus-datos-2017/>.

² <https://informacoes.anatel.gov.br/paineis/aceessos/ranking>

Vale ressaltar que os resultados são amplamente divulgados na imprensa nacional³ e internacional⁴.

Em sua sexta edição, o projeto avaliará as seguintes empresas: **Oi** banda larga fixa e móvel; **Vivo** banda larga fixa e móvel, **TIM** banda larga fixa e móvel, **NET**, **Claro**, **Algar** e **Brisanet**.

II. METODOLOGIA E RESULTADO GERAL

Cada empresa foi avaliada a partir de 6 categorias, cuja elaboração levou em consideração as exigências da legislação vigente (especialmente da Lei Geral de Proteção de Dados e do Marco Civil da Internet) e boas práticas internacionais em matéria de proteção à privacidade. **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 21/06/2021.** 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 agosto de 2020 e julho de 2021.

Com base nas respostas obtidas, atribuímos as seguintes notas: **A.** 1 estrela cheia; **B.** $\frac{3}{4}$ de estrela; **C.** $\frac{1}{2}$ estrela; **D.** $\frac{1}{4}$ 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.

³ 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>.

⁴ 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>.

Em 2021, as empresas obtiveram as seguintes notas:

| QSD? | | 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 |
|---|---|---|---|-----------------------------------|---------------------------------|--|------------------------|
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |
|  |  | ★ | ★ | ★ | ★ | ★ | ★ |

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 alguns aspectos do 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.

Além disso, 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 titulares, 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).

Quais foram os parâmetros de avaliação?

[Informações sobre coleta e finalidade] A empresa fornece informações claras e completas sobre: (a) quais dados são coletados; (b) em que situações a coleta ocorre; (c) a finalidade e (d) a forma como se dá a utilização, além de (e) informar sobre quais são e fornecer meios (e.g. e-mails ou links) para exercício dos direitos dos titulares sobre seus dados.

[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) quando/se são apagados; (c) quais práticas de segurança observa; (d) quem tem acesso aos dados; (e) com quais terceiros (f) para quais finalidades os dados são compartilhados; (g) quais as hipóteses de transferência internacional de dados; e (h) qual a data da última atualização da política de privacidade.

[Respostas a solicitações de direitos] A empresa processou e satisfaz, em menos de um mês, os pedidos de acesso aos dados realizados por seus titulares, integrantes do InternetLab.

[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.

[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 4 a 5 parâmetros.



O provedor de Internet atende a 3 parâmetros.



O provedor de Internet atende a 2 parâmetros.



O provedor de Internet atende a apenas um 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, 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. 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 locais 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.

Quais foram os parâmetros de avaliação?

[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.

[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.

[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.

[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).

[Protocolos específicos] A empresa publica protocolo de resposta a pedidos de entrega de dados pessoais a autoridades públicas.

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?

[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).

[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?

Essa categoria levou em consideração a postura adotada pelas empresas em relação a casos de incidentes de segurança, bem como medidas defendidas pela empresa para a mitigação de riscos cibernéticos.

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 a temas de segurança e mitigação de riscos cibernéticos. Em 2020 e 2021, foram registrados diversos casos de incidentes de segurança, alguns deles envolvendo provedores de conexão⁵. Investigações sobre os incidentes foram abertas pela Secretaria Nacional do Consumidor (Senacon) e pelo Procon-SP. Órgãos reguladores, em resposta, implementaram iniciativas que visavam o combate a ameaças de cibersegurança. São exemplos dessas iniciativas a criação do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações pela Anatel⁶ e a nota técnica publicada pela Autoridade Nacional de Proteção de Dados (ANPD) com orientações ao mercado para casos de incidentes de segurança de dados pessoais⁷.

⁵ TECNOBLOG. Claro, Vivo, TIM e Oi terão que explicar megavazamento à Senacon. 16 de fevereiro de 2021. Disponível em: <https://tecnoblog.net/412412/claro-vivo-tim-e-oi-terao-que-explicar-megavazamento-a-senacon/>.

⁶ GOV.BR. Anatel aprova Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. 17 de dezembro de 2020. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-aprova-regulamento-de-seguranca-cibernetica-aplicada-ao-setor-de-telecomunicacoes>.

⁷ GOV.BR. ANPD inicia processo de regulamentação sobre incidentes de segurança com tomada de subsídios. 22 de fevereiro de 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-processo-de-regulamentacao-sobre-incidentes-de-seguranca-com-tomada-de-subsidios>.

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?

[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?

[Posicionamento sobre medidas de segurança] A empresa se posicionou em nome próprio, em consultas públicas, debates, ou na mídia, especializada ou não, a favor de técnicas e práticas para promover a segurança dos dados de seus usuários, fornecendo informações concretas sobre estratégias de mitigação de riscos e de prevenção de incidentes de segurança?

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 nesta 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?

[Publica relatório] Publica relatório de transparência em português sobre privacidade e proteção de dados.

[Acessibilidade do relatório] Possui relatório de transparência facilmente acessível ao público em geral.

[Periodicidade do relatório] Publica relatório de transparência com periodicidade mínima anual.

[Informações sobre pedidos de acesso a dados] Apresenta, no relatório de transparência, informações sobre pedidos de acesso a dados recebidos, atendidos e rechaçados.

[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.

Qual foi o parâmetro de avaliação?

[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

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a Claro Móvel obteve **estrela cheia**, tendo atendido aos parâmetros I, II, IV e V.

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

O sub-parâmetro (a), referente aos dados coletados, foi considerado cumprido. 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.

O sub-parâmetro (b), referente às situações em que a coleta ocorre, também foi considerado cumprido. 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.

O sub-parâmetro (c), referente à finalidade do tratamento de dados, foi considerado atendido. Na mesma seção apontada no sub-parâmetro (a) acima, cada tipo de dado é seguido da finalidade de sua coleta e processamento. Por exemplo, que dados cadastrais “são importantes para algumas ações, como preenchimento do seu contrato de serviço, emissão de nota fiscal e, também para nos comunicarmos com você”, que dados de pagamentos são “usados somente para efetuar a cobrança pelos serviços de telecomunicações ou outros serviços que você tenha contratado através da Claro”, que dados de perfil de consumo “são importantes para a formação do seu perfil de crédito pela Claro e por parceiros que desempenham atividades relacionadas à proteção ao crédito e prevenção à fraude”, dentre outros.

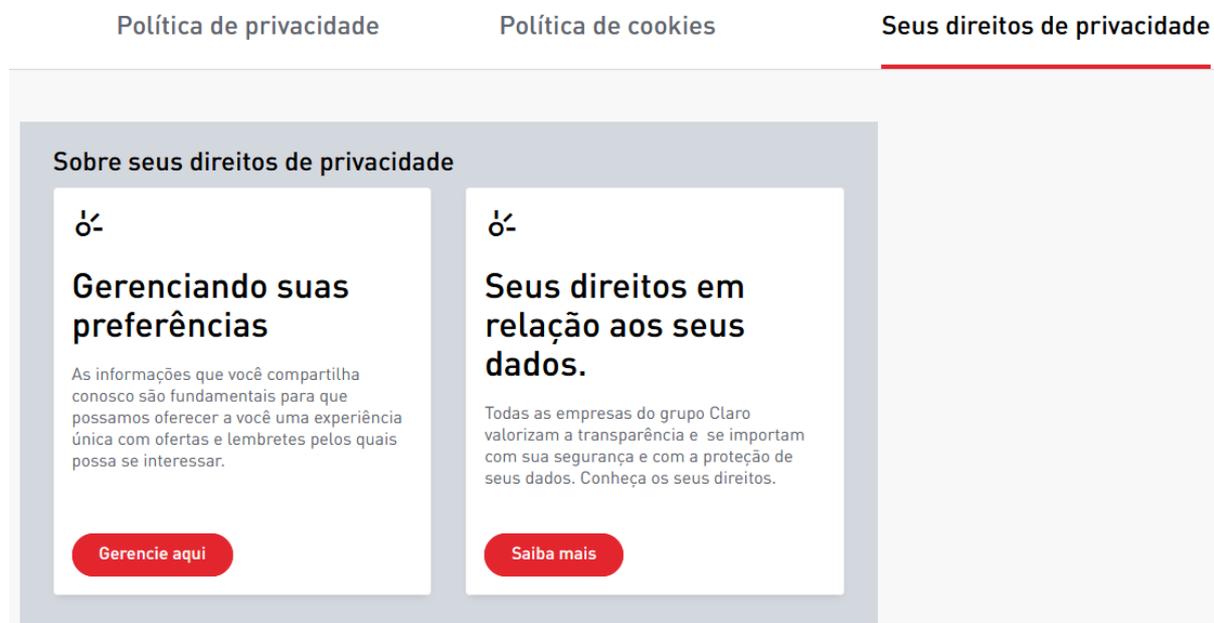
O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. No mesmo trecho copiado para o sub-parâmetro (a) acima, e ao apontar as finalidades de sua coleta conforme apontado no sub-parâmetro (c) acima, a Claro indiretamente esclarece as maneiras de uso dos dados pessoais coletados. Além disso, aponta no início do seu Portal de Privacidade:

Aqui, você fica por dentro dos tratamentos de dados feitos pela Claro em:

- serviços de mobilidade, como planos pré-pagos, controle e pós-pagos;
- soluções de entretenimento, como NOW e TV (DTH e cabo);
- serviços de conectividade, como banda larga Virtua e Wi-fi;
- soluções Claro empresas e Embratel.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercício desses direitos, também foi considerado 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 mediante o próprio Portal da Privacidade, ou mediante e-mail ao DPO da Claro:



captura de tela de 23.07.2021

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, considerou-se, na média, que foi atendido, pois os sub-parâmetros (a), (c), (f) e (h) foram atendidos, enquanto os sub-parâmetros (b), (e) e (g) foram considerados parcialmente atendidos.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado cumprido. 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:

- três anos - registros de conexão à internet, sendo que não guardará os registros de acesso a funcionalidades de internet;
- seis meses - registros de acesso a funcionalidades de internet nos aplicativos próprios da Claro;
- dez anos - dados cadastrais e de faturamento;
- 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.

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. A Claro também contrata armazenamento em nuvem, o que é uma prática comum e segura de mercado. Esse tipo de armazenamento, por definição, poderá ser realizado fora do território nacional. A Claro segue atenta às orientações da ANPD, que futuramente regulamentará esse tipo de tratamento.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, considerou-se que foi parcialmente atendido. Isso porque, no mesmo trecho apontado acima, infere-se que os dados são apagados após o decurso do prazo apontado. No entanto, seria ideal se a empresa apontasse explicitamente que os dados são apagados após o decurso dos referidos prazos.

O sub-parâmetro (c), 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 2020 (p. 92) 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.

O sub-parâmetro (d), referente a quem tem acesso aos dados, não foi considerado atendido. Em nenhum dos documentos analisados encontramos informações sobre quem tem acesso aos dados, a empresa limita-se a informar com quem os dados são compartilhados, ponto que será avaliado no sub-parâmetro (e).

O sub-parâmetro (e), referente aos terceiros com quem os dados são compartilhados, foi considerado parcialmente atendido. A empresa informa, na seção “Com quem a Claro compartilha dados?” de seu Portal de Privacidade, o seguinte:

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.
7. Parceiros de Televendas – Oferta de produtos e serviços a você, por ligações ou SMS, consultando antes se você chegou a pedir para não ser chamado.
8. Companhia Seguradora – Propor seguros de aparelhos celulares e compartilhar seus dados com a seguradora e a corretora para fins de cobertura do seguro, e também com o terceiro para fins de cobrança do prêmio na fatura.

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.

Mesmo que a lista seja louvável, não há informações detalhadas sobre quais empresas, especificamente, recebem os dados da Claro, razão pela qual o sub-parâmetro foi considerado parcialmente atendido. Na fase de engajamento, a empresa nos esclareceu que tais informações podem ser solicitadas pelos titulares e prestadas diretamente a estes; no entanto, em benefício da máxima transparência, espera-se para os fins deste relatório que a informação relativa a quem recebe os dados dos titulares seja publicamente disponível.

Quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se que foi atendido, em vista dos detalhes de cada compartilhamento conforme trecho do Portal da Privacidade apontado acima.

O sub-parâmetro (g), relativo à transferência internacional de dados, foi considerado parcialmente atendido. A política de privacidade da empresa informa: “A Claro também contrata armazenamento em nuvem, o que é uma prática comum e segura de mercado. Esse tipo de armazenamento, por definição, poderá ser realizado fora do território nacional.” Mesmo que seja louvável que haja menção à hipótese de transferência internacional de dados nos documentos da Claro, o parâmetro foi considerado parcialmente atendido, já que não há maiores especificações quanto a quais entidades internacionais recebem tais dados.

Por fim, o sub-parâmetro (h), referente à data de última atualização da política de privacidade, foi considerado atendido. Ao fim do seu Portal da Privacidade, a empresa aponta a data de sua última atualização.

Claro

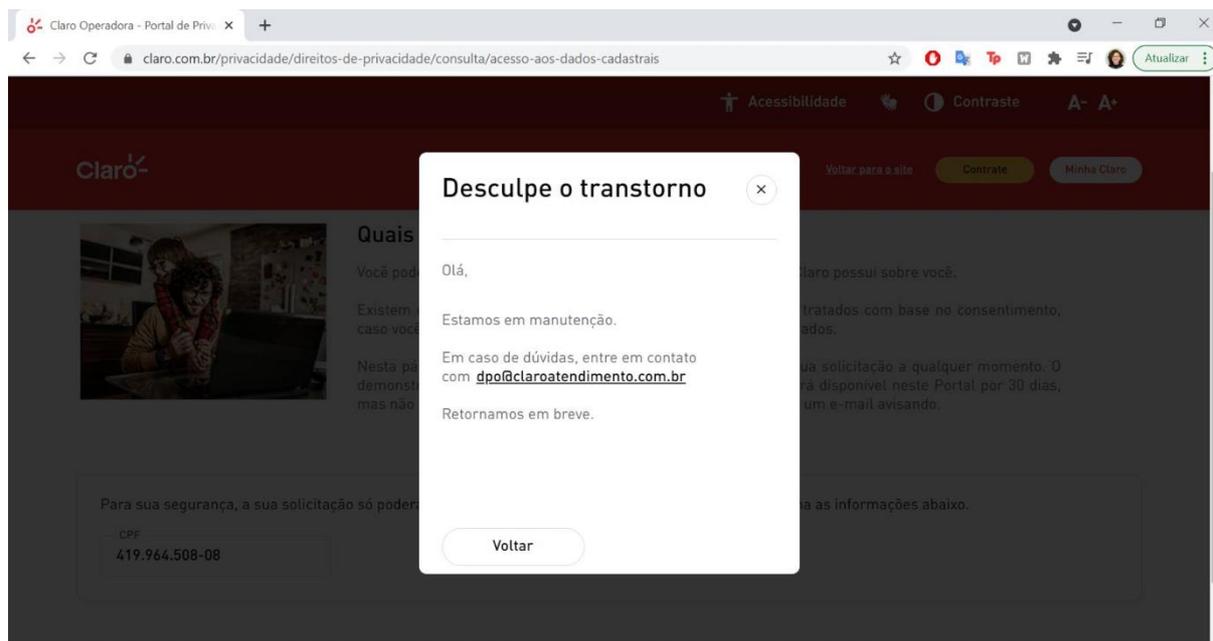
[Voltar para o site](#) [Contrate](#) [Minha Claro](#)

- Quais são os seus direitos em relação aos seus dados pessoais? ▾
- Medidas de Segurança: Como a Claro protege seus dados? ▾
- A Claro, seus dados e a COVID-19 ▾
- Ficou com dúvidas? ▾

Atualizada em 28 de junho de 2021

captura de tela de 23.07.2021

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, não foi considerado atendido. Em 21.07.2021, o InternetLab tentou, por meio do portal de privacidade da Claro, obter cópia das informações pessoais de um titular. Foi informado por e-mail ao titular que um extrato seria gerado; no entanto, o portal seguia exibindo uma mensagem de erro, que continuava sendo apresentada após aprox. 3 meses, até a data de fechamento deste relatório. Foi tentado contato com a empresa solicitando-se a correção da situação, sem sucesso. O InternetLab enaltece a qualidade do portal de direitos da privacidade da Claro, que é granular, simples, e de fácil acesso. No entanto, as mensagens de erro impediram que o parâmetro pudesse ser atendido.



captura de tela de 30.07.2021

O **parâmetro IV**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado atendido. Mesmo que, em seu Portal de Privacidade, a empresa não forneça informações nesse sentido, durante a fase de engajamento, a Claro comprovou que comunica seus clientes por meio de mensagens, notificações ou e-mails sobre alterações em suas políticas de privacidade. Para melhor esclarecimento da situação e maior transparência, o InternetLab sugere que se prometa publicamente o envio de tais notificações.

Por fim, o **parâmetro V**, 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 Claro⁸, em que constam a “Política de privacidade”, a “Política de cookies” e “Seus direitos de privacidade”. As informações que constam no Portal de Privacidade são bastante claras e de fácil acesso ao cliente.

⁸ <https://www.claro.com.br/politica-de-privacidade>

A Claro oferece diversos serviços para a sua conectividade e diversão. E, mais do que isso, a Claro quer garantir transparência no relacionamento e segurança para você. Por isso, contamos com ferramentas avançadas de controle de privacidade e trabalhamos constantemente para proteger seus dados.

Aqui, você fica por dentro dos tratamentos de dados feitos pela Claro em:

- serviços de mobilidade, como planos pré-pagos, controle e pós-pagos;
- soluções de entretenimento, como NOW e TV (DTH e cabo);
- serviços de conectividade, como banda larga Virtua e Wi-fi;
- soluções Claro empresas e Embratel.

Quais dados pessoais a Claro coleta e para quais finalidades eles são utilizados?



captura de tela de 23.07.2021

Além disso, as principais informações que constam na Política de Privacidade são apresentadas nos contratos da Claro, conforme alterações feitas pela empresa durante a fase de engajamento deste relatório. O InternetLab enaltece o fato de as informações estarem também contidas em seus contratos, o que é prática pouco comum na indústria.

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 e não cumprindo 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:

9. Setor Público - Atendimento a fiscalizações do 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); Lei 12.850 de 02 de agosto de 2013 (Lei do Crime Organizado); Lei 12.683 de 09 de julho de 2012

(Lavagem de Dinheiro); 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 esclarece:

Contrato de prestação de serviços SMP pré-pago:

“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.”

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, não foi considerado atendido. Não foi encontrada menção ao tema nos documentos analisados da Claro.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

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

O **parâmetro I**, referente à contestação de legislação, foi considerado atendido. Na fase de engajamento com as empresas, a Claro apresentou algumas ações nesse sentido. Por exemplo, mencionamos uma ação, protocolada em conjunto com outras operadoras de telefonia, em que se contesta a Lei Estadual nº 20.089/2019, do Paraná, que estabeleceu às Operadoras de Telefonia a obrigação de divulgação irrestrita dos códigos de acesso dos usuários nas ligações telefônicas (Ação Ordinária 0001787-36.2020.8.16.0004).

Por fim, o **parâmetro II** foi igualmente considerado atendido. Na fase de engajamento com as empresas, a Claro apresentou ao InternetLab, com informações sensíveis tarjadas, algumas respostas a ofícios administrativos em que se negou a fornecer dados pessoais a autoridades públicas. Por exemplo, negou-se a fornecer dados à Controladoria Geral da União alegando que “o fornecimento dos dados cadastrais não-sensíveis de uma pessoa sem prévia autorização judicial, violaria a Constituição e a lei infraconstitucional, independentemente das diversas leis mencionadas no ofício”.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Civil Pública nº 0005292-42.2003.4.03.6110, que questiona, entre outros, a entrega de dados de portas lógicas às autoridades policiais, e a Ação Direta de Inconstitucionalidade (ADI) 5642⁹, da ACEL, não foram consideradas, já que não registraram movimentações.

CATEGORIA 4: Postura pública pró-privacidade

⁹ 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 Claro Móvel obteve **estrela cheia**, pois atendeu aos dois 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.

Durante a fase de engajamento, a empresa nos forneceu algumas situações em que se posicionou publicamente em debates sobre privacidade. Em um dos casos, defendeu, na tomada de subsídios da Autoridade Nacional de Proteção de Dados quanto à regulação do tratamento de dados por microempresas, que os direitos dos titulares de dados não fossem flexibilizados, buscando “impedir práticas potencialmente abusivas e proteger os direitos dos consumidores”.

Mesmo o parâmetro tendo sido considerado atendido em vista da manifestação mencionada acima, devem-se ressaltar duas situações em que o posicionamento da empresa foi, na visão do InternetLab, prejudicial à privacidade dos titulares. Por exemplo, na consulta pública relativa à estratégia brasileira de inteligência artificial, a empresa defendeu que a legislação não precisaria ser atualizada para a inteligência artificial, entendendo que a LGPD já seria suficiente para fazer frente aos desafios desta tecnologia. Respeitadas as opiniões divergentes, não há discussão sobre de que forma a privacidade dos usuários poderia ser protegida mesmo no contexto do processamento de dados pessoais por algoritmos de IA, que apresentam desafios próprios como a possibilidade de inferência de informações pessoais a partir de outras informações, tendência a resultados enviesados ou discriminatórios, entre outros. Além disso, na tomada de subsídios para regulamentação do dever de comunicação sobre incidentes de segurança, a empresa defendeu, por meio da Brasscom, que somente incidentes que tenham potencial de gerar riscos ou prejuízos ao titular de dados sejam notificados à autoridade nacional, na contramão da ampliação de seu dever de transparência pública. Este relatório tem como um de seus objetivos estimular a transparência e a regulação de práticas de tratamento de dados (como a inteligência artificial) de maneira protetiva e específica. Assim, tais posicionamentos da empresa e do setor, por meio da Brasscom, devem ser aqui publicamente obstados.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial¹⁰; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado

¹⁰ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

pela Anatel em 2020¹¹; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética¹²; entre outras.

Na Consulta Pública da Anatel para discussão da proposta de requisitos mínimos de segurança cibernética, a empresa defendeu uma “atuação mais incisiva da Agência na fiscalização dos equipamentos vendidos no varejo”, de forma a atingir “a segurança desejada, visto que parte dos incidentes resultam do baixo nível de segurança dos equipamentos”.

No entanto, vale ressaltar que a Claro sofreu em 2020 um suposto ataque cibernético, sendo que inclusive chegou a ser notificada pelo Procon¹³.

Em geral, no entanto, a empresa deu respostas genéricas ao caso, afirmando por exemplo que “investe fortemente em políticas e procedimentos de segurança e mantém monitoramento constante, adotando medidas, de acordo com melhores práticas, para identificar fraudes e proteger seus clientes”¹⁴. Não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. A resposta da empresa foi considerada excessivamente genérica. Contudo, nesta edição do relatório, as respostas relativas a tais vazamentos não foram consideradas para fins de pontuação.

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

Resultado: 

Nesta categoria, a Claro obteve $\frac{1}{4}$ de estrela, pois atendeu parcialmente aos parâmetros I e IV.

O **parâmetro I**, relativo à publicação de Relatório de Transparência sobre privacidade e proteção de dados, foi considerado parcialmente atendido. Durante a fase de engajamento, a empresa nos mostrou que o seu “Relatório Social”, publicado pelo Instituto Claro, pela primeira vez em 2021 apresentou estatísticas quanto a pedidos de acesso a dados feitos pelos próprios titulares. No entanto, não há informações mais granulares sobre o assunto, nem informações sobre pedidos de acesso a dados feitos por autoridades públicas.

Os **parâmetros II e III**, relativos à acessibilidade e periodicidade do Relatório de Transparência, não foram atendidos. A América Móvil publica a cada dois anos um Relatório de Sustentabilidade, em inglês e em espanhol. O documento apresenta algumas informações sobre privacidade e proteção de dados, no entanto não publica estatísticas de pedidos. Além disso, o mencionado Relatório de Transparência

¹¹ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

¹² TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

¹³ <https://www.cnnbrasil.com.br/business/2021/02/17/procon-sp-notifica-claro-oi-tim-vivo-e-empresa-de-seguranca-sobre-vazamento>

¹⁴ <https://g1.globo.com/economia/noticia/2021/02/18/operadoras-dizem-que-nao-detectaram-vazamentos-de-dados-de-clientes.ghtml>

do Instituto Claro não é facilmente acessível no site da Claro, e só apresentou informações sobre proteção de dados em 2021.

O **parâmetro IV**, relativo às informações sobre pedidos de acesso aos dados, foi considerado parcialmente atendido. Como há informações sobre pedidos de acesso feitos por titulares, considerou-se que o parâmetro poderia ser considerado atendido; no entanto, não são disponibilizadas informações quanto a pedidos feitos por autoridades públicas.

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

NET

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado:

Nesta categoria, a NET obteve **estrela cheia**, tendo atendido aos parâmetros I, II, IV e V.

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

O sub-parâmetro (a), referente aos dados coletados, foi considerado cumprido. Em seu Portal da Privacidade, que, de acordo com o site onde se encontra, aplica-se tanto aos serviços de internet móvel quanto de banda larga (Claro e NET, portanto), 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.

O sub-parâmetro (b), referente às situações em que a coleta ocorre, também foi considerado cumprido. 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.

O sub-parâmetro (c), referente à finalidade do tratamento de dados, foi considerado atendido. Na mesma seção apontada no sub-parâmetro (a) acima, cada tipo de dado é seguido da finalidade de sua coleta e processamento. Por exemplo, que dados cadastrais “são importantes para algumas ações, como preenchimento do seu contrato de serviço, emissão de nota fiscal e, também para nos comunicarmos com você”, que dados de pagamentos são “usados somente para efetuar a cobrança pelos serviços de telecomunicações ou outros serviços que você tenha contratado através da Claro”, que dados de perfil de consumo “são importantes para a formação do seu perfil de crédito pela Claro e por parceiros que desempenham atividades relacionadas à proteção ao crédito e prevenção à fraude”, dentre outros.

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. No mesmo trecho copiado para o sub-parâmetro (a) acima, e ao apontar as finalidades de sua coleta conforme apontado no sub-parâmetro (c) acima, a Claro 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:

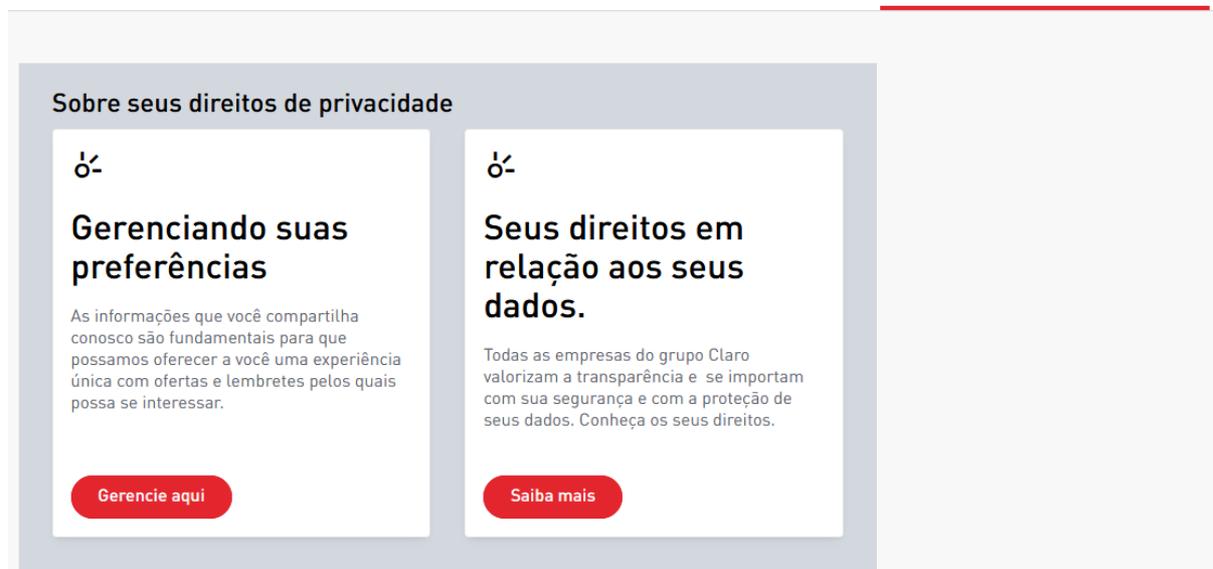
- serviços de mobilidade, como planos pré-pagos, controle e pós-pagos;
- soluções de entretenimento, como NOW e TV (DTH e cabo);
- serviços de conectividade, como banda larga Virtua e Wi-fi;
- soluções Claro empresas e Embratel.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercício desses direitos, também foi considerado 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 mediante o próprio Portal da Privacidade, ou mediante e-mail ao DPO da Claro:

[Política de privacidade](#)

[Política de cookies](#)

[Seus direitos de privacidade](#)



captura de tela de 23.07.2021

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, considerou-se, na média, que foi atendido, pois os sub-parâmetros (a), (c), (f) e (h) foram atendidos, enquanto os sub-parâmetros (b) e (e) foram considerados parcialmente atendidos.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado cumprido. 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:

- três anos - registros de conexão à internet, sendo que não guardará os registros de acesso a funcionalidades de internet;
- seis meses - registros de acesso a funcionalidades de internet nos aplicativos próprios da Claro;
- dez anos - dados cadastrais e de faturamento;
- 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.

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. A Claro também contrata armazenamento em nuvem, o que é uma prática comum e segura de mercado. Esse tipo de armazenamento, por definição, poderá ser realizado fora do território nacional. A Claro segue atenta às orientações da ANPD, que futuramente regulamentará esse tipo de tratamento.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, considerou-se que foi parcialmente atendido. Isso porque, no mesmo trecho apontado acima, infere-se que os dados são apagados após o decurso do prazo apontado. No entanto, seria ideal se a empresa apontasse explicitamente que os dados são apagados após o decurso dos referidos prazos.

O sub-parâmetro (c), 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 2020 (p. 92) 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.

O sub-parâmetro (d), referente a quem tem acesso aos dados, não foi considerado atendido. Em nenhum dos documentos analisados encontramos informações sobre quem tem acesso aos dados, a empresa limita-se a informar com quem os dados são compartilhados, ponto que será avaliado no sub-parâmetro (e).

O sub-parâmetro (e), referente aos terceiros com quem os dados são compartilhados, foi considerado parcialmente atendido. A empresa informa, na seção “Com quem a Claro compartilha dados?” de seu Portal de Privacidade, o seguinte:

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:

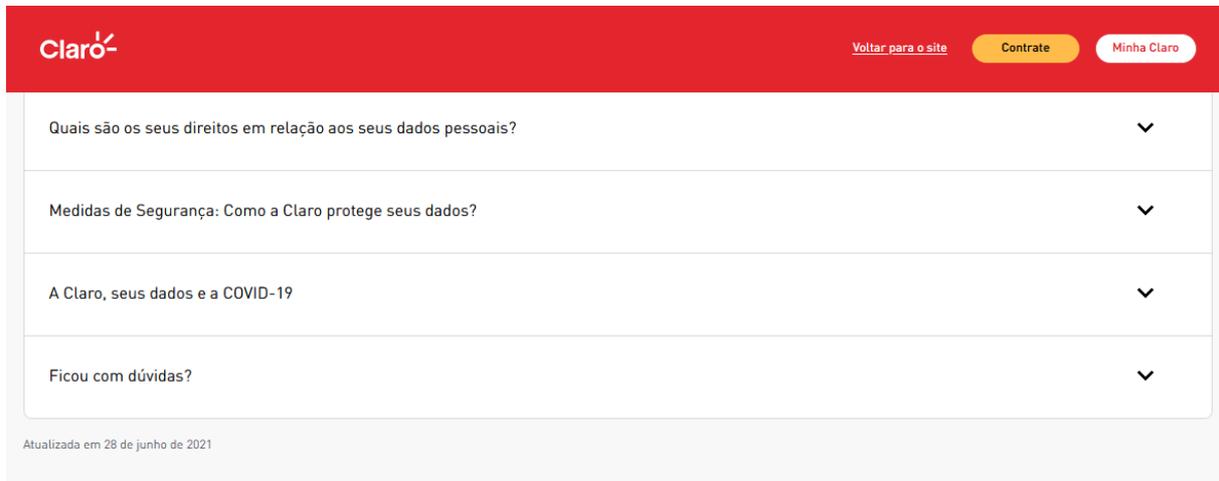
1. Empresas de Call Center – Realização de atendimento a clientes e clientes prospectivos.
2. Empresas de Serviços Técnicos – Instalação e manutenção de serviços Claro, como TV e Internet.
3. Empresas que comercializam conteúdos via Claro - Comercialização de conteúdos de terceiros nos canais de vendas 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.
7. Parceiros de Televendas – Oferta de produtos e serviços a você, por ligações ou SMS, consultando antes se você chegou a pedir para não ser chamado.
8. Companhia Seguradora – Propor seguros de aparelhos celulares e compartilhar seus dados com a seguradora e a corretora para fins de cobertura do seguro, e também com o terceiro para fins de cobrança do prêmio na fatura.

Mesmo que a lista seja louvável, não há informações detalhadas sobre quais empresas, especificamente, recebem os dados da Claro, razão pela qual o sub-parâmetro foi considerado parcialmente atendido. Na fase de engajamento, a empresa nos esclareceu que tais informações podem ser solicitadas pelos titulares e prestadas diretamente a estes; no entanto, em benefício da máxima transparência, espera-se para os fins deste relatório que a informação relativa a quem recebe os dados dos titulares seja publicamente disponível.

Quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se que foi atendido, em vista dos detalhamentos de cada compartilhamento conforme trecho do Portal da Privacidade apontado acima.

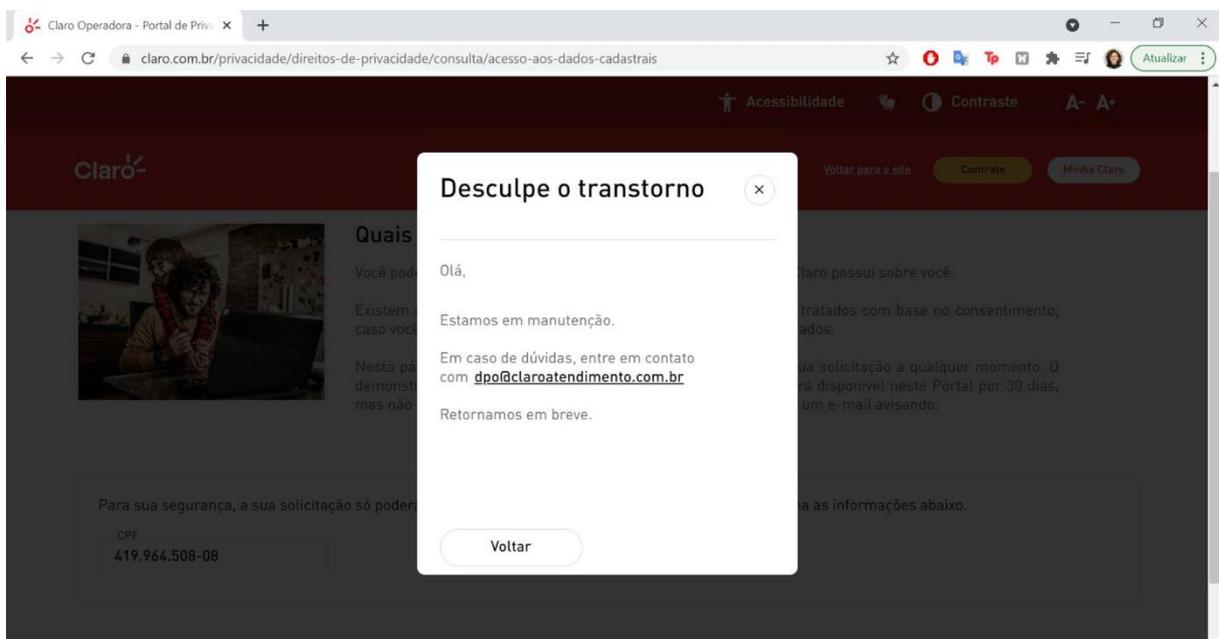
O sub-parâmetro (g), relativo à transferência internacional de dados, foi considerado parcialmente atendido. A política de privacidade da empresa informa: “A Claro também contrata armazenamento em nuvem, o que é uma prática comum e segura de mercado. Esse tipo de armazenamento, por definição, poderá ser realizado fora do território nacional.” Mesmo que seja louvável que haja menção à hipótese de transferência internacional de dados nos documentos da Claro, o parâmetro foi considerado parcialmente atendido, já que não há maiores especificações quanto a quais entidades internacionais recebem tais dados.

Por fim, o sub-parâmetro (h), referente à data de última atualização da política de privacidade, foi considerado atendido. Ao fim do seu Portal da Privacidade, a empresa aponta a data de sua última atualização.



captura de tela de 23.07.2021

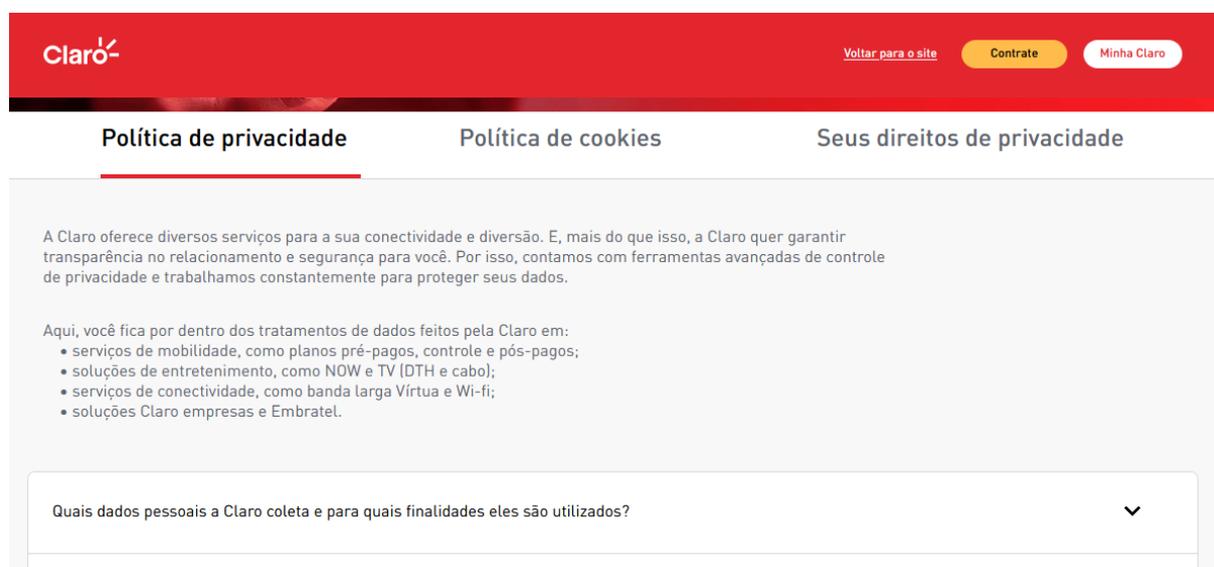
O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, não foi considerado atendido. Em 21.07.2021, o InternetLab tentou, por meio do portal de privacidade da Claro, obter cópia das informações pessoais de um titular. Foi informado por e-mail ao titular que um extrato seria gerado; no entanto, o portal seguia exibindo uma mensagem de erro, que continuava sendo apresentada após aprox. 3 meses, até a data de fechamento deste relatório. Foi tentado contato com a empresa solicitando-se a correção da situação, sem sucesso. O InternetLab enaltece a qualidade do portal de direitos da privacidade da Claro, que é granular, simples, e de fácil acesso. No entanto, as mensagens de erro impediram que o parâmetro pudesse ser atendido..



captura de tela de 30.07.2021

O **parâmetro IV**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado atendido. Mesmo que, em seu Portal de Privacidade, a empresa não forneça informações nesse sentido, durante a fase de engajamento, a Claro comprovou que comunica seus clientes por meio de mensagens, notificações ou e-mails sobre alterações em suas políticas de privacidade. Para melhor esclarecimento da situação e maior transparência, o InternetLab sugere que se prometa publicamente o envio de tais notificações.

Por fim, o **parâmetro V**, 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, em que constam a “Política de privacidade”, a “Política de cookies” e “Seus direitos de privacidade”. As informações que constam no Portal de Privacidade são bastante claras e de fácil acesso ao cliente.



captura de tela de 23.07.2021

Além disso, as principais informações que constam na Política de Privacidade são apresentadas nos contratos da Claro, conforme alterações feitas pela empresa durante a fase de engajamento deste relatório. O InternetLab enaltece o fato de as informações estarem também contidas em seus contratos, o que é prática pouco comum na indústria.

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 e não cumprindo 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:

9. Setor Público - Atendimento a fiscalizações do 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); Lei 12.850 de 02 de agosto de 2013 (Lei do Crime Organizado); Lei 12.683 de 09 de julho de 2012 (Lavagem de Dinheiro); 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) Net virtua

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.

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, não foi considerado atendido. Não foi encontrada menção ao tema nos documentos analisados da Claro.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

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

O **parâmetro I**, referente à contestação de legislação, foi considerado atendido. Na fase de engajamento com as empresas, a Claro apresentou algumas ações nesse sentido. Por exemplo, mencionamos uma ação, protocolada em conjunto com outras operadoras de telefonia, em que se contesta a Lei Estadual nº 20.089/2019, do Paraná, que estabeleceu às Operadoras de Telefonia a obrigação de divulgação irrestrita dos códigos de acesso dos usuários nas ligações telefônicas (Ação Ordinária 0001787-36.2020.8.16.0004).

Por fim, o **parâmetro II** foi igualmente considerado atendido. Na fase de engajamento com as empresas, a Claro apresentou ao InternetLab, com informações sensíveis tarjadas, algumas respostas a ofícios administrativos em que se negou a fornecer dados pessoais a autoridades públicas. Por exemplo, negou-se a fornecer dados à Controladoria Geral da União alegando que “o fornecimento dos dados cadastrais não-sensíveis de uma pessoa sem prévia autorização judicial, violaria a Constituição e a lei infraconstitucional, independentemente das diversas leis mencionadas no ofício”.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Civil Pública nº 0005292-42.2003.4.03.6110, que questiona, entre outros, a entrega de dados de portas lógicas às autoridades policiais, e a Ação Direta de Inconstitucionalidade (ADI) 5642¹⁵, da ACEL, não foram consideradas, já que não registraram movimentações.

CATEGORIA 4: Postura pública pró-privacidade

Resultado:

Nesta categoria, a NET obteve **estrela cheia**, pois atendeu aos 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.

Durante a fase de engajamento, a empresa nos forneceu algumas situações em que se posicionou publicamente em debates sobre privacidade. Em um dos casos, defendeu, na tomada de subsídios da Autoridade Nacional de Proteção de Dados quanto à regulação do tratamento de dados por microempresas, que os direitos dos titulares de dados não fossem flexibilizados, buscando “impedir práticas potencialmente abusivas e proteger os direitos dos consumidores”.

Mesmo o parâmetro tendo sido considerado atendido em vista da manifestação mencionada acima, devem-se ressaltar duas situações em que o posicionamento da empresa foi, na visão do InternetLab, prejudicial à privacidade dos titulares. Por exemplo, na consulta pública relativa à estratégia brasileira de inteligência artificial, a empresa defendeu que a legislação não precisaria ser atualizada para a inteligência artificial, entendendo que a LGPD já seria suficiente para fazer frente aos desafios desta tecnologia. Respeitadas as opiniões divergentes, não há discussão sobre de que forma a privacidade dos usuários poderia ser protegida mesmo no contexto do processamento de dados pessoais por algoritmos de IA, que apresentam desafios próprios como a possibilidade de inferência de informações pessoais a partir de outras informações, tendência a resultados enviesados ou discriminatórios, entre outros. Além disso, na tomada de subsídios para regulamentação do dever de comunicação sobre incidentes de segurança, a empresa defendeu, por meio da Brasscom, que somente incidentes que tenham potencial de gerar riscos ou prejuízos ao titular de dados sejam notificados à autoridade nacional, na contramão da ampliação de seu dever de transparência pública. Este relatório tem como um de seus objetivos estimular a transparência e a regulação de práticas de tratamento de dados

¹⁵ 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.

(como a inteligência artificial) de maneira protetiva e específica. Assim, tais posicionamentos da empresa e do setor, por meio da Brasscom, devem ser aqui publicamente obstados.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial¹⁶; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020¹⁷; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética¹⁸; entre outras.

Na Consulta Pública da Anatel para discussão da proposta de requisitos mínimos de segurança cibernética, a empresa defendeu uma “atuação mais incisiva da Agência na fiscalização dos equipamentos vendidos no varejo”, de forma a atingir “a segurança desejada, visto que parte dos incidentes resultam do baixo nível de segurança dos equipamentos”.

No entanto, vale ressaltar que a Claro sofreu em 2020 um suposto ataque cibernético, sendo inclusive que chegou a ser notificada pelo Procon¹⁹.

Em geral, no entanto, a empresa deu respostas genéricas ao caso, afirmando por exemplo que “investe fortemente em políticas e procedimentos de segurança e mantém monitoramento constante, adotando medidas, de acordo com melhores práticas, para identificar fraudes e proteger seus clientes”²⁰. Não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. A resposta da empresa foi considerada excessivamente genérica. Contudo, nesta edição do relatório, as respostas relativas a tais vazamentos não foram consideradas para fins de pontuação.

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

¹⁶ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

¹⁷ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

¹⁸ TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

¹⁹ <https://www.cnnbrasil.com.br/business/2021/02/17/procon-sp-notifica-claro-oi-tim-vivo-e-empresa-de-seguranca-sobre-vazamento>

²⁰ <https://g1.globo.com/economia/noticia/2021/02/18/operadoras-dizem-que-nao-detectaram-vazamentos-de-dados-de-clientes.ghml>

Resultado: 

Nesta categoria, a NET obteve **¼ de estrela**, pois atendeu parcialmente aos parâmetros I e IV.

O **parâmetro I**, relativo à publicação de Relatório de Transparência sobre privacidade e proteção de dados, foi considerado parcialmente atendido. Durante a fase de engajamento, a empresa nos mostrou que o seu “Relatório Social”, publicado pelo Instituto Claro, pela primeira vez em 2021 apresentou estatísticas quanto a pedidos de acesso a dados feitos pelos próprios titulares. No entanto, não há informações mais granulares sobre o assunto, nem informações sobre pedidos de acesso a dados feitos por autoridades públicas.

Os **parâmetros II e III**, relativos à acessibilidade e periodicidade do Relatório de Transparência, não foram atendidos. A América Móvil publica a cada dois anos um Relatório de Sustentabilidade, em inglês e em espanhol. O documento apresenta algumas informações sobre privacidade e proteção de dados, no entanto não publica estatísticas de pedidos. Além disso, o mencionado Relatório de Transparência do Instituto Claro não é facilmente acessível no site da Claro, e só apresentou informações sobre proteção de dados em 2021.

O **parâmetro IV**, relativo às informações sobre pedidos de acesso aos dados, foi considerado parcialmente atendido. Como há informações sobre pedidos de acesso feitos por titulares, considerou-se que o parâmetro poderia ser considerado atendido; no entanto, não são disponibilizadas informações quanto a pedidos feitos por autoridades públicas.

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

OI BANDA LARGA

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Oi Banda Larga obteve **estrela cheia**, pois atendeu, integralmente, ao parâmetro I, III e V, e atendeu parcialmente ao parâmetro II

Ressaltamos, no entanto, que o parâmetro III, 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 Oi Banda Larga atendeu ao **parâmetro I**, pois atendeu a todos os sub-parâmetros.

O *sub-parâmetro (a)*, referente aos dados coletados, foi considerado cumprido. Em seu Aviso de Privacidade, a empresa informa:

COMO A OI COLETA DADOS PESSOAIS?

Diretamente com você, por exemplo, na aquisição de serviços e produtos ou durante nossos processos seletivos;

Automaticamente, quando, por exemplo, você navega em nossos sites ou aplicativos.

Através de algum parceiro, caso, por exemplo, você já possua um vínculo com o terceiro.

Em seu Aviso de Privacidade, a empresa informa e exemplifica as categorias de dados pessoais coletados:

CATEGORIA DE DADO PESSOAL

DADOS DE CADASTRO E CONTRATO: Nome, número de CPF, número de RG, número de passaporte, filiação, endereço (físico ou e-mail), número de telefone celular e residencial, número ICCID (cartão SIM), data de nascimento, nacionalidade e profissão.

DADOS FINANCEIROS: Informações da fatura, como histórico, datas de pagamento, valores em aberto ou pagamentos recebidos, informações do cartão de crédito ou débito, conta bancária, entre outros.

DADOS DE LOCALIZAÇÃO E TRÁFEGO: Dados de localização aproximada, quando você tiver ativado a funcionalidade de localização do Sistema de Posicionamento Global (GPS) ou coletados por antenas ERB (Estações Rádio Base), número de telefone de ligações efetuadas ou recebidas, bem como respectivo tempo de duração, número de telefone relacionados ao envio e recebimento de SMS, uso e quantidade dos pacotes ou da conexão de dados, navegação em Wi-Fi, informações do perfil de consumo.

DADOS DE NAVEGAÇÃO NOS SITES E APLICATIVOS DA Oi: Dados de dispositivos e navegação (modelo, data, hora, IP) e cookies.

Em sua Política de Privacidade, a empresa informa de maneira exaustiva os dados de cadastros e contratos, as informações financeiras, os dados de localização, dados sobre uso do site e aplicativos, dados de atendimento, de tráfego e estatísticos coletados.

Que dados a Oi coleta?

Seus dados pessoais tratados e a forma de coleta poderão variar de acordo com os serviços contratados por você ou de acordo com a forma de uso dos seus serviços. Não importa se a coleta for feita a partir da inserção voluntária dos dados por você nas plataformas da Oi, de forma automática quando usa nossos serviços, quando acessa nossos sites ou qualquer outra forma de interação com a Oi.

Coletamos seus dados de cadastro e contrato

- Seu nome, número de CPF, número de RG, número de passaporte, filiação, endereço (físico ou e-mail), número de telefone celular e residencial, número ICCID (cartão SIM), data de nascimento, nacionalidade e profissão.

- Número de CPF, filiação, dados bancários, números de boleto, fatura ou débito em conta e gênero.

- Conteúdo de instrumentos de mandato (procurações) utilizados para ações de contratação ou gestão de contratos de serviços prestados pela Oi e número de telefone comercial.

Coletamos suas informações financeiras

- Informações da fatura, como histórico, datas de pagamento, valores em aberto ou pagamentos recebidos.

- Informações do cartão de crédito ou débito, da conta bancária e outras informações bancárias.

Coletamos seus dados de localização

- Dados de localização aproximada, quando você tiver ativado a funcionalidade de localização que utiliza os dados do Sistema de Posicionamento Global (GPS) ou outra tecnologia, e quando referentes aos sinais identificados pelas estações de base da rede móvel da Oi.

Coletamos seus dados sobre o modo de uso do site e dos aplicativos da Oi

- O histórico sobre o modo de uso e navegação realizada por você nos mais diversos meios e plataformas disponibilizados pela Oi.

Coletamos seus dados de atendimento

As informações prestadas nos serviços de atendimento ao cliente, através de qualquer meio disponibilizado pela Oi.

Coletamos seus dados de tráfego

- A duração das ligações, o uso e a quantidade dos pacotes ou da conexão de dados. Ou como você está usando os dados.

- As informações do perfil de consumo.

Coletamos dados estatísticos

A Oi faz o levantamento de informações de logs de uso para mapear o perfil de tráfego de voz e dados.

O *sub-parâmetro (b)*, referente às situações em que a coleta ocorre, também foi considerado cumprido. Isso porque na seção “Como a Oi Coleta Dados Pessoais” do Aviso de Privacidade (vide trecho acima), informa-se que os dados são coletados na aquisição de serviços e produtos, em processos seletivos; automaticamente quando o titular navega nos sites ou aplicativos da empresa; ou através de parceiros. Na Política de Privacidade, especifica-se a coleta de dados de uso dos produtos e serviços contratados, históricos de chamadas, dados de atendimento, transações de recarga, dentre outros. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

O *sub-parâmetro (c)*, referente à finalidade do tratamento de dados, foi considerado cumprido. Na seção “Para quais finalidades a Oi coleta dados pessoais”, a empresa informa quatro hipóteses de finalidade:

Prestação de Serviços: Se você for um de nossos clientes, como assinante da nossa fibra, vamos precisar coletar seus dados cadastrais, de localização, financeiros, entre outros, para formalizarmos o contrato de prestação de serviços e processarmos os pagamentos.

Processo Seletivo: Se quiser trabalhar com a gente, teremos que coletar informações profissionais, como histórico educacional, profissão, entre outros, para avaliarmos se o seu perfil é compatível com a vaga.

Parceiros: Agora, se você for um de nossos parceiros, necessitamos coletar dados cadastrais das pessoas físicas que vão trabalhar em nossas dependências, para controle de acesso, garantindo assim a segurança de todos os envolvidos na operação.

Cookies: Além disso, como a Oi busca melhorar cada vez mais seus produtos e serviços, podemos utilizar dados de navegação e dados de ativos tecnológicos, como cookies, em nossos sites, para melhorar a performance das páginas na web.

Na Política de Privacidade tais informações são destrinchadas em uma tabela, em que é especificado a finalidade do tratamento, quais são os dados tratados e qual é a sua base legal:

Microsoft Word - OIM005320A - Política de Privacidade.docx 3 / 11

nos baseamos para podermos tratá-los de forma adequada.

| Finalidade do tratamento | Dados tratados | Base legal |
|--|--|---|
| <ul style="list-style-type: none"> Atendimento de solicitações para prestação de serviço. Faturamento e processamento de pagamento dos serviços contratados. Atendimento direto, indireto ou, ainda, através de terceiros autorizados pela Oi. Prestação de serviços de roaming. | <ul style="list-style-type: none"> Dados de cadastro e contrato Informações financeiras Dados de tráfego Dados de atendimento Número ICCID (Cartão SIM) | <ul style="list-style-type: none"> Execução de contrato |
| <ul style="list-style-type: none"> Conduzir o planejamento de negócios. Geração e análise de indicadores, relatórios e previsões. Acompanhamento e análises de desempenhos. Estratégia de comunicação. Estratégia de vendas. Auditoria de qualidade. Gestão de controles. | <ul style="list-style-type: none"> Dados de atendimento Dados estatísticos Informações financeiras Dados de localização Dados de tráfego | <ul style="list-style-type: none"> Legítimo interesse |
| <ul style="list-style-type: none"> Prevenção de fraude, uso fraudulento dos serviços Oi e demais medidas que promovam a segurança do usuário na fruição dos serviços contratados. | <ul style="list-style-type: none"> Dados de cadastro e contrato Informações financeiras Dados de tráfego Dados de localização Número ICCID (Cartão SIM) | <ul style="list-style-type: none"> Prevenção à fraude e à segurança do titular Legítimo interesse |
| <ul style="list-style-type: none"> Inovação e evolução dos serviços, de acordo com o nível de serviço prestado aos usuários. | <ul style="list-style-type: none"> Dados de localização Dados sobre o modo de uso do site e aplicativos Dados de atendimento Dados de tráfego | <ul style="list-style-type: none"> Legítimo interesse |

captura de tela de 19.07.2021.

Microsoft Word - OIM005320A - Política de Privacidade.docx 4 / 11

| | | |
|--|---|---|
| <ul style="list-style-type: none"> Análise de tráfego, criando relatório de gestão de forma agregada e estatístico, visando a melhoria da prestação desses serviços sem que os usuários sejam identificados individualmente. Metodologia analítica ("Big Data Analytics") com foco no conjunto de dados variados para identificação de perfil e comportamento com implementação de medidas rigorosas de segurança, garantindo a proteção dos dados pessoais, tornando-os anonimizados sempre que possível. Aperfeiçoar o uso e a experiência do usuário em nossos serviços. | | |
| <ul style="list-style-type: none"> Publicidade de ofertas, promoções, lançamentos e materiais publicitários ou informativos relativos aos serviços da Oi ou de seus parceiros, bem como de terceiros. Uso de localização e metodologia analítica sobre comportamento de uso, padrões e tendências. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados sobre modo de uso do site e aplicativos Dados de tráfego Dados de localização | <ul style="list-style-type: none"> Legítimo interesse |
| <ul style="list-style-type: none"> Apresentar publicidade mais relevante de seus parceiros ou de terceiros em seus canais. Metodologia analítica ("Big Data Analytics") com foco no conjunto de dados variados para criação de público-alvo segmentado e, sempre que possível, anonimizado. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados sobre modo de uso do site e aplicativos Dados de tráfego Dados de localização | <ul style="list-style-type: none"> Legítimo interesse |
| <ul style="list-style-type: none"> Envio de informações, relatórios e indicadores à Anatel. Envio de informações, relatórios e pareceres ao Procon e demais órgãos e autoridades competentes. Quebra de sigilo telefônico, em determinados casos, quando solicitado por autoridade policial, Ministério Público e ordens judiciais. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados de atendimento Informações financeiras Dados de tráfego Dados de localização | <ul style="list-style-type: none"> Cumprimento de obrigação legal ou regulatória |
| <ul style="list-style-type: none"> Efetuar, exercer ou defender ações judiciais. Resposta a ofícios e cumprimento de liminares. Defesa em processos administrativos, relacionados aos órgãos de defesa do consumidor. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados de atendimento Informações financeiras Dados de tráfego | <ul style="list-style-type: none"> Exercício regular de direitos |

captura de tela de 19.07.2021.

No mesmo documento, a empresa detalha, também, quais são as bases legais para o tratamento de dados:

As bases legais para tratamento de dados

A Oi poderá realizar o tratamento dos seus dados pessoais amparada nas seguintes bases legais:

- Para a correta execução do contrato ou prestação do serviço contratado, ou até mesmo para eventuais procedimentos preliminares necessários, e também para o atendimento das suas eventuais solicitações.
- Para o cumprimento de obrigação legal ou regulatória.
- No atendimento ao seu legítimo interesse ou ao interesse do Grupo Oi, incluindo, mas não se limitando, ao apoio e promoção de suas atividades e na proteção, em relação aos titulares, do exercício regular de seus direitos ou prestação de serviços que os beneficiem de alguma forma.
- Mediante o fornecimento do seu consentimento, através de manifestação livre, informada e inequívoca, para uma finalidade determinada.
- Para medidas de prevenção à fraude e à sua segurança.
- Para o exercício regular de direitos no âmbito de processos judiciais ou administrativos.
- Para uso compartilhado de dados com a Administração Pública, para o tratamento necessário à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres

A empresa detalha de maneira exaustiva quais são os dados tratados, bem como suas finalidades e base legais especificamente para cada tipo de tratamento de dados. Consideramos positiva a forma como a empresa específica tais informações e, por isso, o sub-parâmetro foi considerado atendido.

O *sub-parâmetro (d)*, referente à forma como se dá a utilização, foi considerado cumprido. Na seção “Saiba mais” do Aviso de Privacidade, a empresa informa como utiliza dados pessoais em portais e nos aplicativos da Oi:

Minha Oi

Na Minha Oi, você consegue visualizar os produtos contratados, acompanhar consumo, saber sobre sua oferta atual, recarregar e ainda ter acesso a outros serviços da Oi. Para que tudo isso seja possível, utilizamos dados pessoais. Por exemplo:

- Para exibir as informações sobre sua oferta, precisamos ter acesso a seus dados pessoais, como número de telefone, além de dados de localização e tráfego.
- Se quiser comprar pacotes, mudar sua oferta ou ainda contratar outros serviços, vamos precisar de seus dados cadastrais, dados de localização e tráfego, além de dados financeiros, para processar pagamentos.
- Agora, se precisar de suporte técnico, podemos utilizar dados cadastrais, dados de localização e tráfego, além de dados de navegação e ativos tecnológicos, a depender de sua necessidade.
- Além disso, podemos utilizar dados cadastrais, dados de localização e tráfego para oferecer novos produtos e medir a qualidade dos nossos serviços.

Técnico Virtual Oi

Através do Técnico Virtual, oferecemos soluções para problemas com a internet banda larga ou fibra, TV por satélite ou telefone fixo. Por esse motivo, utilizamos dados pessoais, como dados cadastrais, dados de localização e tráfego e ainda dados de navegação e dados de ativos tecnológicos a fim de viabilizar a prestação do serviço.

Oi Play

É o serviço de streaming da Oi para você ter acesso a filmes, séries e canais de televisão em um só lugar. Nessa plataforma, podemos usar dados pessoais de diversas formas, como, por exemplo:

- Para efetuar a contratação do serviço, coletamos dados cadastrais, de localização, financeiros, entre outros, para formalizarmos o contrato de prestação de serviços e processarmos os pagamentos.
- Para que você possa acessar o conteúdo dos canais e plataformas, podemos precisar autenticar sua identidade, compartilhando algum dado pessoal, como, por exemplo, CPF, com a plataforma parceira.
- Ainda, podemos utilizar dados de navegação e dados de ativos tecnológicos, como cookies, com o objetivo de melhorar a performance do nosso portal e corrigir eventuais erros.

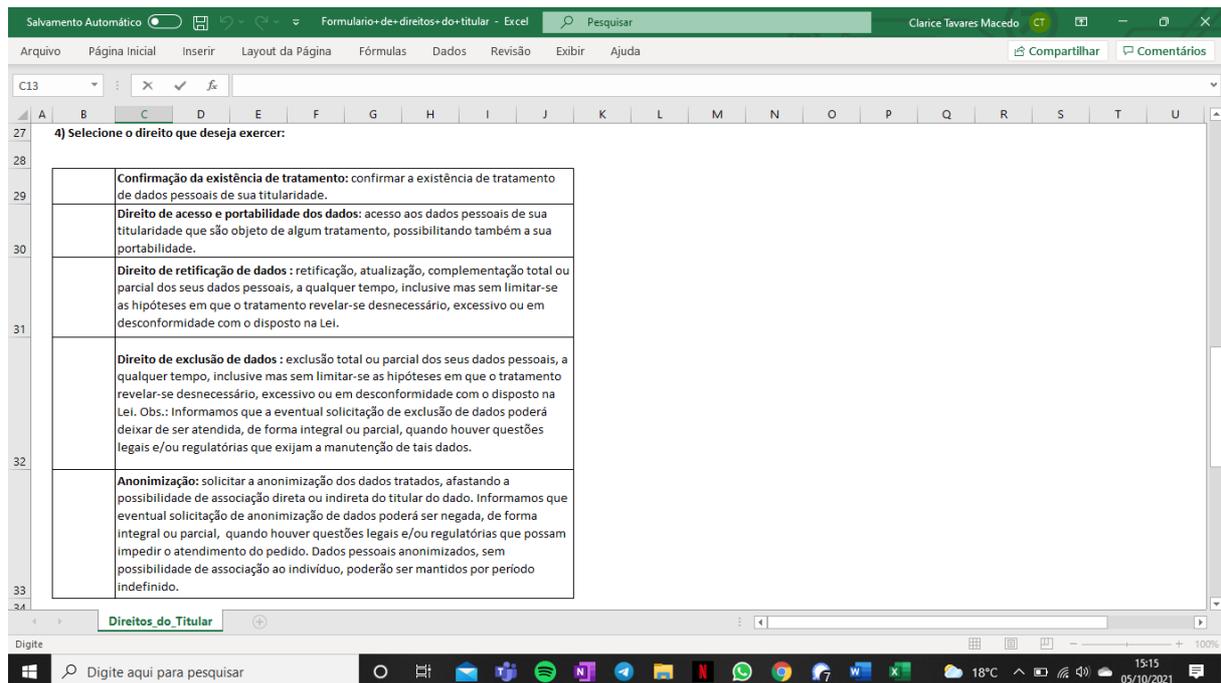
Na seção “As bases legais para o tratamento de dados” da Política de Privacidade (vide trecho acima), a empresa detalha como se dá a utilização, especificando que os dados são utilizados “para a correta execução do contrato ou prestação do serviço contratado”, “para o exercício regular de direitos no âmbito de processos judiciais ou administrativos”, “para uso compartilhado de dados com a Administração Pública” etc. Considerou-se que tais informações são capazes de detalhar a forma de utilização dos dados pessoais.

Por fim, o *sub-parâmetro (e)*, relativo à informação quanto aos direitos dos titulares e meios para exercício desses direitos, foi considerado atendido. Em seu Portal de Privacidade, na seção “Direito dos titulares”, a empresa informa um e-mail para o exercício desses direitos previstos na LGPD. A Oi fornece um canal específico para o titular dos dados, para o representante de um titular de dados e para colaboradores ou ex-colaboradores.

Direitos dos titulares

Agora, se quiser exercer algum dos direitos previstos na LGPD, baixe o arquivo XLSX através de um dos links abaixo e o encaminhe para o e-mail PP-PrivacidadeDireitoTitular@oi.net.br

Na seção “Quais são meus direitos” a empresa apenas informa genericamente que “a Lei Geral de Proteção de Dados Pessoais estabelece que você, enquanto titular de dados pessoais (dono de suas próprias informações), possui uma série de direitos, como acesso aos dados que possuímos sobre a sua pessoa, correção de informações desatualizadas, entre outros”. Nos formulários para o exercício dos direitos do titular, a empresa especifica e define os direitos elencados pela lei:



Captura de tela do formulário para exercício de direitos. 05 de outubro de 2021

Em sua Política de Privacidade, na seção “Quais são os seus direitos”, a empresa informa quais são os direitos sobre os dados pessoais previstos na Lei Geral de Proteção de Dados (direito de acesso e de confirmação de tratamento, de correção, de eliminação, de objeção, de portabilidade, de anonimização, de pedido de informações e o direito de fornecer ou revogar o consentimento) e informa um e-mail para o exercício desses direitos. Ademais, a empresa informa que, para atender determinadas exigências legais, não pode eliminar ou anonimizar dados que “sejam inerentes à prestação do serviço pela Oi”, a menos que haja determinação judicial para tal.

A Lei Geral de Proteção de Dados (LGPD) confere a você direitos sobre seus dados pessoais, conforme mostramos a seguir.

Direito de acesso e de confirmação de tratamento: você tem o direito de confirmar a existência de tratamento dos seus dados pessoais e também de acesso e requisição de cópia desses dados, ressalvadas as hipóteses de sigilo legal.

Direito de correção: você também tem o direito de solicitar a retificação, atualização ou complementação dos seus dados pessoais.

Direito de eliminação: você pode solicitar a exclusão dos seus dados pessoais, exceto se aplicável outra hipótese legal que impeça a exclusão ou que torne necessária a continuidade do tratamento.

Direito de objeção: você pode solicitar, temporária ou permanentemente, a interrupção do tratamento de todos ou alguns dos seus dados pessoais, exceto se aplicável outra hipótese legal que impeça a exclusão ou que torne necessária a continuidade do tratamento.

Direito de portabilidade: você pode pedir seus dados pessoais de forma estruturada, de forma que possam ser transmitidos a outro fornecedor de serviço ou produto, mediante solicitação.

Anonimização: você pode solicitar que seus dados pessoais tratados se tornem anônimos, podendo requerer o bloqueio ou a eliminação daqueles considerados desnecessários ou excessivos para finalidade aplicável ao caso concreto ou na hipótese de eventual tratamento em desacordo com a legislação aplicável. Exceto se aplicável outra hipótese legal que impeça a anonimização, bloqueio ou eliminação desses dados ou que torne necessária a continuidade do seu tratamento.

Informações de compartilhamento: você pode pedir informações sobre entidades públicas ou privadas com as quais seus dados pessoais foram compartilhados para o cumprimento das finalidades previstas nesta Política de Privacidade, com exceção dos casos de sigilo legal.

Consentimento: você também pode fornecer e revogar, a qualquer momento, o consentimento anteriormente dado à Oi mediante manifestação expressa, além de solicitar informações sobre a possibilidade de não fornecer consentimento e sobre as eventuais consequências da negativa.

Você pode exercer esses direitos a qualquer momento. Basta enviar uma mensagem para o e-mail PP-PrivacidadeDireitoTitular@oi.net.br

Você reconhece que os termos dos direitos citados nesta página serão assegurados nos termos legais e regulatórios aplicáveis em cada caso concreto.

Eliminação e anonimização

Para atender determinadas exigências legais estabelecidas pelos órgãos reguladores, com exceção de determinação judicial, não poderão ser eliminados ou anonimizados dados que sejam inerentes à prestação do serviço pela Oi, como dados cadastrais, dados de cobrança, dados de localização e dados de tráfego.

O **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, foi considerado parcialmente atendido, pois a empresa atendeu aos sub-parâmetros (c), (e), (f) e (h) e parcialmente ao sub-parâmetro (g).

O *sub-parâmetro (a)*, referente ao tempo e local de armazenamento dos dados, não foi considerado cumprido. Quanto ao tempo de armazenamento, na seção “Por quanto tempo meus dados são armazenados pela Oi?” do Aviso de Privacidade, a empresa informa que mantém os dados pelo período necessário para cumprimento da finalidade e afirma que armazena os dados de acordo com as normas legais. No entanto, a empresa não especifica quais seriam esses dados ou qual seria a legislação vigente aplicável. Tais informações foram consideradas insuficientes, visto que a empresa não estabelece prazos mínimos ou máximos pelo qual armazena os dados de seus clientes.

POR QUANTO TEMPO MEUS DADOS SÃO ARMAZENADOS PELA OI?

Seus dados ficarão conosco apenas pelo período necessário para o cumprimento de alguma finalidade, como, por exemplo, para prestação de

nossos serviços, atendimento a uma obrigação legal/regulatória, ou para nos ajudar a melhorar nossos produtos. Em qualquer caso, armazenaremos seus dados de acordo com a lei, de forma segura, transparente e por tempo limitado.

Na seção “Retenção e término do tratamento dos dados pessoais” da Política de Privacidade, a empresa informa apenas que os dados poderão ser mantidos após o encerramento do contrato e informa genericamente que “os dados pessoais usados para fornecer uma experiência personalizada a você serão mantidos exclusivamente pelo tempo permitido, de acordo com a legislação vigente” e que os dados são mantidos por tempo “estritamente necessário para o cumprimento de obrigação legal e regulatório após o cumprimento do contrato”. No entanto, a empresa não especifica quais seriam esses dados ou qual seria a legislação vigente aplicável. Tais informações foram consideradas insuficientes, visto que a empresa não estabelece prazos mínimos ou máximos pelo qual armazena os dados de seus clientes.

Retenção e término do tratamento dos dados pessoais

- A Oi poderá manter armazenados os seus dados pessoais após o encerramento de contrato ou o término do serviço contratado por você, conforme se revele estritamente necessário para o cumprimento de obrigação legal ou regulatória a que estejamos sujeitos. Ou ainda para exercício de algum direito da Oi em processo administrativo, judicial ou extrajudicial, sem prejuízo da aplicação das hipóteses mencionadas pelo art. 16 da Lei Geral de Proteção de Dados Pessoais (LGPD).

- Os dados pessoais usados para fornecer uma experiência personalizada a você serão mantidos exclusivamente pelo tempo permitido, de acordo com a legislação vigente. - Seus dados pessoais serão tratados apenas durante o período necessário para o alcance das finalidades pretendidas, conforme estabelecido no item 3 desta Política de Privacidade.

Quanto ao local de armazenamento dos dados, o Aviso de Privacidade e a Política de Privacidade não oferece quaisquer informações sobre o local de armazenamento dos dados. Tais informações também não foram encontradas em nenhum dos contratos da empresa.

Quanto ao *sub-parâmetro (b)*, referente a quando/se os dados são apagados, não foi considerado cumprido. A empresa informa apenas que os dados são armazenados de acordo com a lei e por tempo limitado (vide trecho acima), sem especificar prazos ou quais são as legislações aplicáveis.

Na seção “Eliminação e anonimização”, a empresa prevê que, em razão do cumprimento de exigências legais, determinados dados, como dados cadastrais, dados de cobrança, dados de localização e dados de tráfego, não poderão ser eliminados ou sequer anonimizados. Tal informação diverge da legislação atualmente posta. O Marco Civil da Internet, por exemplo, estabelece prazos mínimos pelos quais os dados devem ser guardados, mas não prevê a proibição de que sejam eliminados. Ainda, a empresa informa apenas, na seção “Retenção e término do tratamento dos dados pessoais” da Política de Privacidade” (vide trecho acima) que mantém os dados armazenados apenas “conforme se revele estritamente necessário para o cumprimento de obrigação legal ou regulatória”, sem prever expressamente o apagamento dos dados.

Eliminação e anonimização

- Para atender determinadas exigências legais estabelecidas pelos órgãos reguladores, com exceção de determinação judicial, não poderão ser eliminados ou anonimizados dados que sejam inerentes à prestação do serviço pela Oi, como dados cadastrais, dados de cobrança, dados de localização e dados de tráfego.

Quanto ao *sub-parâmetro (c)*, referente a quais práticas de segurança observa, considerou-se que foi atendido. Em seu Aviso de Privacidade, na seção “Meus dados estão protegidos na Oi?”, a empresa informa:

Na Oi, temos como propósito transformar o ambiente digital, aplicando as melhores tecnologias disponíveis no mercado para garantir segurança das informações que possuímos e fazer jus à confiança que você nos deposita. Quando falamos de dados pessoais, essa preocupação é ainda maior e não medimos esforços para assegurar sua privacidade, por isso, aplicamos e renovamos constantemente nossos protocolos de segurança, além de possuímos regras internas que orientam o armazenamento de dados pessoais em locais seguros, reduzindo a possibilidade de acessos não autorizados ou o vazamento de informações.

Em sua Política de Privacidade, na seção “Segurança da Informação”, a empresa informa:

Segurança da informação

A Oi se compromete a garantir a segurança e a manutenção da proteção dos seus dados pessoais armazenados com a adoção das medidas técnicas e administrativas aptas a proteger os dados pessoais exportados de acessos não autorizados e de situações acidentais ou ilícitas, de acordo com as legislações aplicáveis.

Os colaboradores da Oi têm o compromisso de zelar pela segurança dos seus dados pessoais e de respeitar esta Política de Privacidade, sob pena de sofrerem sanção disciplinar em caso de violação dessas normas.

Esperamos que você também contribua com a segurança, mantendo seus dados pessoais seguros. Ao se cadastrar nas plataformas da Oi, escolha uma senha forte o suficiente para evitar que outras pessoas a adivinhem.

A Oi recomenda que você nunca revele ou compartilhe a sua senha com outras pessoas. Você

é o único responsável por manter a senha confidencial e por qualquer ação realizada através de sua conta nos sites e serviços do Grupo Oi.

As proteções citadas elencadas nesta seção não se aplicam a informações que você tenha escolhido compartilhar em áreas públicas, como fóruns e redes sociais de outras companhias.

A Oi se compromete a divulgar para você e órgãos competentes qualquer incidente de segurança e quais as medidas que serão aplicadas nesse caso.

Em seu Relatório de Sustentabilidade, a empresa detalha as práticas de segurança que observa. Afirma ter a certificação ISO 27001 e afirma utilizar o antivírus chamado Endpoint Security EDR. Essas informações foram consideradas suficientes para o sub-parâmetro.

A Oi possui a certificação ISO 27001, que assegura a qualidade e a confiabilidade do sistema de gestão da Segurança da Informação da Companhia, protegendo as redes de dados dos clientes de todo o país contra possíveis ataques cibernéticos.

Em 2020, para fazer com que empresas públicas ou privadas estivessem menos vulneráveis a ciberataques, entre outros riscos decorrentes do ambiente on-line, a Oi passou a oferecer esses serviços de segurança cibernética como tema de alta prioridade.

Em meio ao aumento de ciberataques ocasionados principalmente por conta do regime de home office adotado pela maioria das empresas, devido às necessidades impostas pela pandemia, a Oi desenvolveu um antivírus chamado Endpoint Security EDR, que combina inteligência artificial e machine learning para bloquear ameaças em tempo real – enquanto o antivírus roda, identifica as novas variantes que vão surgindo e já se adapta para combater a ameaça.

Com base na experiência da Companhia para a proteção de dados de seus clientes e sistemas internos, a Oi, por meio do Oi Soluções, oferece esse serviço e pretende ampliar a sua oferta de projetos de segurança em 2021.

O *sub-parâmetro (d)*, referente a quem tem acesso aos dados, não foi considerado cumprido. Na seção “Meus dados estão protegidos na Oi?” (vide trecho acima), a empresa informa apenas que adota protocolos de segurança para proteger os dados de “acessos não autorizados”, mas não oferece quaisquer informações sobre quem tem acesso aos dados pessoais.

O *sub-parâmetro (e)*, referente aos terceiros com quem os dados são compartilhados, foi considerado atendido. Em seu Aviso de Privacidade, a empresa informa, genericamente, algumas hipóteses de compartilhamento de dados:

A OI COMPARTILHA MEUS DADOS PESSOAIS COM ALGUÉM?

Para a prestação de nossos serviços, a Oi conta com parceiros de negócios que podem ter acesso a alguns de seus dados pessoais. Todos os nossos parceiros passam por um processo de avaliação prévio, de modo que apenas aqueles que compartilham nossos valores participarão de nossas atividades.

Ainda adotamos medidas específicas para garantia da segurança e controle de seus dados pessoais, mesmo quando compartilhados. O compromisso que estabelecemos com você neste aviso também se estende às pessoas que trabalham conosco. Além de nossos parceiros, podemos compartilhar seus dados com autoridades governamentais, como, por exemplo, autoridades policiais, Ministério Público, Tribunais de Justiça, órgãos de defesa do consumidor, Anatel, entre outros, para cumprimento de alguma obrigação legal, regulatória ou ordem judicial.

Da mesma forma, podemos compartilhar dados pessoais para instituições de proteção ao crédito para reduzir o risco de crédito e o uso fraudulento dos serviços Oi. Seja para onde for, compartilharemos seus dados de acordo com a legislação brasileira e reafirmamos nosso compromisso de transparência com você.

Em sua Política de Privacidade, a empresa informa com quais terceiros compartilha os dados e para quais finalidades:

Compartilhamento dos dados

A Oi não compartilha os seus dados pessoais com empresas, organizações ou terceiros, apenas nestes casos abaixo, e sempre de acordo com esta Política de Privacidade e outras medidas de segurança e de confidencialidade adequadas:

- Entre empresas do Grupo Oi para manutenção, promoção e melhoria dos serviços.
- Para parceiros comerciais no desenvolvimento de promoções e ações comerciais conjuntas com a Oi.
- Para prestadores de serviço de marketing, como envio de e-mail marketing, SMS e veiculação de anúncios online.
- Para parceiros de vendas e lojas franqueadas, na colaboração às vendas de produtos e serviços fornecidos pela Oi.
- Para terceiros contratados ou autorizados para cuidados relacionados à execução ou gestão dos serviços Oi, como, por exemplo, prestadores de serviço de suporte técnico e reparo de serviços, análise de dados, consultoria, impressão de faturas, consultas ao sistema de proteção ao crédito e centrais de atendimento ao cliente.
- Para autoridades governamentais, como, por exemplo, autoridades policiais, Ministério Público, Tribunais de Justiça, órgãos de defesa do consumidor ou Anatel, por conta de obrigação legal, regulatória, ordem judicial ou demais solicitações de autoridades com poderes para tanto, para proteger de prejuízos à propriedade ou à segurança do Grupo Oi ou de seus clientes, conforme solicitado ou permitido por lei.
- Para instituições de proteção ao crédito, para reduzir o risco de crédito e o uso fraudulento dos serviços Oi.
- Para terceiros, não previstos aqui, mediante o seu consentimento específico.
- Para agências de cobranças de dívidas, em casos de inadimplência.
- Para terceiros, em razão de reestruturação societária no Grupo Oi.

A Oi solicitará a você o consentimento específico para compartilhar qualquer dado pessoal sensível

Em seu Programa Oi de Privacidade, a empresa apresenta um fluxo de dados em que informa os trajetos que os dados percorrem dentro da empresa, com os titulares e com terceiros:



Captura de tela feita em 06 de outubro de 2021, p. 21.

O fluxo é claro e facilita a comunicação com os usuários. Parabenizamos a empresa pela iniciativa e pela transparência.

Quanto ao *sub-parâmetro (f)*, relativo às finalidades do compartilhamento de dados com terceiros, considerou-se atendido. O Aviso de Privacidade e a Política de Privacidade informa, em algumas hipóteses a finalidade do compartilhamento de dados com terceiros (vide trecho acima), como por exemplo, por obrigação legal, para reduzir o risco de crédito e uso fraudulento. Tais informações foram consideradas suficientes.

Quanto ao *sub-parâmetro (g)*, relativo às hipóteses de transferência internacional de dados, foi considerado parcialmente cumprido. Em seu Aviso de Privacidade, a empresa informa que transfere dados para outros países para armazenamento em nuvem ou para prestação de serviços. A empresa não especifica, no entanto, com quais países, nem em quais hipóteses. No entanto, como houve a preocupação em informar sobre a possibilidade de transferência internacional de dados em seu Aviso de Privacidade, o sub-parâmetro foi considerado parcialmente atendido.

A OI TRANSFERE DADOS PESSOAIS PARA OUTROS PAÍSES?

A internet possibilitou quebrar barreiras geográficas e conectar as pessoas ao redor do mundo e, para que isso aconteça, muitas vezes os dados pessoais circulam entre os países. Como buscamos empregar as melhores tecnologias disponíveis no mercado, em algumas situações, pode haver transferência de dados pessoais para fora do Brasil, como, por exemplo, para armazenamento em nuvem ou se necessário para prestação de um serviço. Em qualquer caso, sempre fazemos isso respeitando a legislação brasileira.

Por fim, quanto ao *sub-parâmetro (h)*, relativo à data da última atualização da política de privacidade, foi considerado cumprido. O Aviso de Privacidade e a Política de Privacidade da empresa apresentam o dia da última atualização, por isso o sub-parâmetro foi considerado atendido. No entanto, vale ressaltar que tal informação não consta nos contratos da empresa. Recomendamos que a prática de

informar a última atualização não se limite às políticas de privacidade e que seja aplicado em todos os documentos da empresa.

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. Após pedido de acesso a dados, a empresa respondeu, tempestivamente, à solicitação.

O **parâmetro IV**, que avalia se a empresa promete enviar notificações ao usuário na hipótese de atualização de suas políticas de privacidade, não foi considerado cumprido. Em seu Aviso de Privacidade a empresa apenas informa que o documento poderá ser alterado e recomenda que o titular faça visitas periódicas ao site, sem se comprometer a notificar o usuário.

ESTE AVISO DE PRIVACIDADE PODE MUDAR?

Como a Oi está sempre melhorando seus serviços e produtos, este Aviso de Privacidade pode ser atualizado. Por isso, sugerimos sua visita periódica nesta página.

Em sua Política de Privacidade, a empresa informa que a Oi tem o direito de alterar a política sem aviso prévio e apenas se compromete a divulgar a alteração na página inicial e em outros canais de comunicação, sem, no entanto, prometer enviar notificações aos usuários.

Alterações à política de privacidade

A Oi tem o direito de, quando necessário, sem aviso prévio e com efeitos imediatos, alterar, acrescentar ou revogar, parcial ou totalmente, esta Política de Privacidade, desde que de acordo com a legislação vigente. Recomendamos que você acesse esta página com frequência, ou sempre que tiver dúvidas, para acompanhar qualquer atualização ou mudança em nossa Política de Privacidade. No caso de alterações em nossa Política de Privacidade, divulgaremos imediatamente através de aviso em destaque na página inicial do nosso site e em outros canais de comunicação e relacionamento da Oi com seus clientes.

Na cláusula 7.13 do Contrato de Adesão de Serviço IP Connect, a empresa se compromete a comunicar o contratante, mas não informa como se daria essa comunicação. Já no Contrato de Adesão à Banda Larga, a empresa não faz nenhuma menção à notificação ao usuário em caso de atualização do contrato.

Contrato de Adesão de Serviço IP Connect:

7.13 O CONTRATO poderá ser alterado a qualquer momento por força de alterações decorrentes da lei e da regulamentação aplicável. A CONTRATANTE será comunicada pela Oi previamente, salvo se o prazo estabelecido não comportar aviso prévio, hipótese que a alteração será automaticamente aplicada ao presente CONTRATO.

Contrato de Adesão à Banda Larga:

13.3. O presente Contrato poderá ser alterado, a qualquer tempo, unilateralmente pela Oi, mediante registro em Cartório e publicação no site www.oi.com.br.

Em virtude da redação ampla da cláusula do contrato e da falta de comprometimento de notificar o cliente no Aviso de Privacidade e na Política de Privacidade, o parâmetro não foi considerado atendido.

Por fim, o **parâmetro V**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado cumprido. Isso porque a Oi dispõe de um Portal de Privacidade com informações claras sobre o tema. O portal pode ser facilmente acessado ao final da página inicial da Oi.



Captura de tela feita em 05 de outubro de 2021.

No entanto, a Política de Privacidade da empresa, o documento mais completo e com mais informações sobre as operações de tratamento de dados realizadas pela Oi, não está disponível no Portal de Privacidade. Para acessar o documento é preciso realizar uma busca ativa, por meio da seção “de A a Z”, ao final da página inicial da empresa. Recomenda-se que a Política de Privacidade, em razão do seu detalhamento e importância, esteja mais acessível, preferencialmente, no próprio Portal da empresa.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Oi Banda Larga obteve **¼ de estrela**, pois atendeu parcialmente ao parâmetro I

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente atendido. Em seu Aviso de Privacidade e Política de Privacidade, a empresa informa, genericamente, que compartilha dados com autoridades governamentais, como autoridades policiais, Ministério Público, Tribunais de Justiça ou Anatel, para o cumprimento de obrigações legais. No entanto, a empresa não discrimina com quais das autoridades citadas o compartilhamento é realizado sem ordem judicial e quais das autoridades podem ter acesso aos dados apenas mediante autorização judicial.

A OI COMPARTILHA MEUS DADOS PESSOAIS COM ALGUÉM?:

(...) podemos compartilhar seus dados com autoridades governamentais, como, por exemplo, autoridades policiais, Ministério Público, Tribunais de Justiça, órgãos de defesa do consumidor, Anatel, entre outros, para cumprimento de alguma obrigação legal, regulatória ou ordem judicial.

No Contrato de Adesão de Serviço IP Connect, a empresa se compromete respeitar as hipóteses legais de quebra de sigilo das telecomunicações e em Contrato de Adesão à Banda Larga se compromete a fornecer dados cadastrais apenas a autoridades administrativas competentes, sem, no entanto, identificá-las.

Contrato de Adesão de Serviço IP Connect:

3. CLÁUSULA TERCEIRA – DOS DIREITOS E OBRIGAÇÕES DA CONTRATANTE:

3.1.6 Inviolabilidade e sigredo de sua comunicação, respeitadas as hipóteses legais de quebra de sigilo das telecomunicações.

3.1.7 Privacidade nos documentos de cobrança, na utilização de seus dados cadastrais pela Oi e privacidade de seus dados pessoais.

Contrato de Adesão à Banda Larga:

11.15. Fornecer dados cadastrais, sem a necessidade de prévia ordem judicial, apenas para autoridades administrativas que possuam competência legal para a requisição.”

Apesar de a empresa identificar as autoridades em seu Aviso de Privacidade e de se comprometer a fornecer dados cadastrais apenas a autoridades administrativas competentes, a redação das duas cláusulas foi considerada insatisfatória e por isso o parâmetro foi considerado parcialmente cumprido.

Vale ressaltar que a empresa não esclarece ao usuário o fato de que dados cadastrais e registros de conexão possuem tratamento jurídico diferenciado. Neste sentido, é importante que a empresa informe claramente que registros de conexão somente podem ser entregues mediante ordem judicial, segundo o Marco Civil da Internet. No que se refere a dados cadastrais, essa mesma lei autoriza que sejam requisitados sem ordem judicial por autoridades administrativas competentes. Atualmente, entretanto, em face de controvérsia sobre quais são tais “autoridades administrativas competentes”, é imprescindível que a empresa seja transparente acerca de suas próprias interpretações da lei que aplica quando recebe pedidos de quebra de sigilo.

O **parâmetro II**, referente à identificação das autoridades competentes e dos crimes no âmbito

dos quais a requisição ocorrer, não foi considerado atendido. Não foi encontrada menção ao tema nos documentos analisados da Oi Banda Larga.

O **parâmetro III**, referente ao oferecimento de informações sobre dados de geolocalização, não foi considerado cumprido. Não foi encontrada menção ao tema nos documentos analisados da Oi Banda Larga.

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, foi não foi considerado cumprido. A Oi Banda Larga prevê em seus contratos pré e pós-pago que registros de conexão são disponibilizados apenas mediante ordem de um juiz. 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).

Contrato de Adesão à Banda Larga:

11.14. Disponibilizar os registros de conexão e de acesso a aplicações de internet, de forma autônoma ou associado a dados pessoais ou a outras informações que, possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial

Por fim, o **parâmetro V**, relativo à existência de protocolos específicos sobre entrega de dados ao estado, não foi atendido. Em nossas buscas, nenhum documento como esse pôde ser localizado.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

Nesta categoria, a Oi Banda Larga obteve **estrela cheia**, tendo atendido a ambos os 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, e não localizamos quaisquer ações nesse sentido.

Na fase de interação com as empresas, tivemos acesso à contestação elaborada pela Oi, com outras empresas de telefonia, contra a Lei Estadual nº 20.089/2019, do Estado do Paraná, que impõe às operadoras de telefonia, fixa ou móvel, a obrigatoriedade de garantirem a identificação das chamadas telefônicas, sob pena de serem autuadas nos termos da norma²¹. Na ação, as empresas argumentam que a lei viola frontalmente o direito constitucional ao sigilo de dados, previsto no art. 5º, X e XII da CF/88.

²¹ Processo nº 0001787-36.2020.8.16.0004. Poder Judiciário do Estado do Paraná.

A propositura da ação contra a Lei nº 20.089/2019 do Estado do Paraná demonstra uma preocupação com o direito à privacidade e ao sigilo dos dados e, por isso, o parâmetro foi considerado atendido.

Por fim, o **parâmetro II**, referente à contestação de pedidos abusivos, foi considerado atendido. Realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado de São Paulo e no portal “Jusbrasil”, em ambos os casos pelos termos “Oi S/A E sigilo E quebra” e por acórdãos publicados entre 01/08/2020 e 21/06/2021, e foi localizada uma ação nesse sentido: [HC 2020.0000746961/TJSP](#), no Tribunal de Justiça de São Paulo. Na ação, a empresa questiona uma ordem de uma autoridade policial que requisitava o fornecimento de senhas de acesso, pelo prazo de 06 meses, de qualquer dado telefônico por ele requerido. A empresa questiona a generalidade do pedido e solicita que sejam identificados os usuários ou terminais telefônicos alvos das medidas, bem como que seja apontada a qual investigação criminal tal ordem estaria vinculada.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Direta de Inconstitucionalidade (ADI) 5642²², da ACEL, não foram consideradas, já que não registraram movimentações.

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 sigilo 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 Oi Banda Larga obteve **½ estrela**, pois atendeu ao parâmetro II.

O **parâmetro I**, relativo ao posicionamento em geral da empresa, não 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.

²² 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.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido.

Em seu Relatório de Sustentabilidade, a empresa afirma (p. 51) ter participado da discussão de diversos projetos de lei no âmbito federal, entre eles o PL 2630/2020, que trata sobre fake news, e o PL 3477/2020, que trata sobre garantia de acesso à Internet, com fins educacionais, aos alunos e professores da educação básica pública. Ainda que seja positiva a inserção dessa informação, não encontramos dados, em sites oficiais ou na mídia, que confirmem a participação, em nome próprio, da empresa.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial²³; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020²⁴; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética²⁵; entre outras.

A empresa participou do Congresso intitulado LGPD – Desafios Enfrentados desde a sua Entrada em Vigor, organizada pela IBRASPD, o Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados. A empresa participou do painel “CISO e DPO – Pandemia dos megavazamentos, como lidar com esse cenário e atender o direito do titular”, na pessoa da Fernanda Vaqueiro, CISO da Oi, no dia 01 de setembro de 2021²⁶.

No entanto, vale ressaltar que a Oi foi uma das empresas notificadas pelo Procon, no início de 2021, pelo suposto vazamento de dados de mais de 100 milhões de clientes. Em resposta, a empresa informou apenas:

A Oi entende que não é objeto de questionamentos no episódio, já que não se verifica nenhum indício de vazamento de dados de seus clientes.²⁷

²³ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

²⁴ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

²⁵ TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

²⁶ <https://www.ibraspd.org/webinar-registration>.

²⁷ O VALOR. Oi e TIM dizem que não detectaram vazamentos de dados de clientes. 17 de fevereiro de 2021. Disponível em: <https://valor.globo.com/empresas/noticia/2021/02/17/oi-e-tim-dizem-que-no-detectaram-vazamentos-de-dados-de-clientes.html>

No entanto, não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. Por isso, a resposta da empresa foi considerada excessivamente genérica.

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

Resultado: 

Nesta categoria, a Oi Banda Larga obteve **estrela vazia**, pois não atendeu a nenhum dos parâmetros

Os **parâmetros I ao IV**, relativos à publicação de relatórios de transparência em português, acessibilidade, periodicidade do relatório e informações sobre pedidos de acesso a dados, não foram considerados atendidos. A empresa publica Relatórios de Sustentabilidade; no entanto, o documento não traz informações significativas sobre privacidade e proteção de dados.

Na página 49 do Relatório de Sustentabilidade 2020, há a informação de que em 2020 foram recebidas 2.438 reclamações pelos canais da Anatel sobre utilização indevida de dados cadastrais. Em 2019, esse número era de 1.220 e em 2018 de 684. Segundo a empresa, esse aumento dos números se deve a “alterações nos dados cadastrados pela Anatel, que começou a valer em novembro de 2019; mas quando essas reclamações foram analisadas, encontrou-se um cenário em que 76% das reclamações apresentaram outros motivos, como restrição a mailing de telemarketing, pedidos de cadastros, contestação de fatura, estorno de conta e cancelamento de produto ou serviço” (p. 49).

No entanto, a empresa não publica estatísticas de pedidos, nem discrimina as autoridades responsáveis ou os fundamentos que apresentam e, por isso, o parâmetro não foi considerado atendido.

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

OI MÓVEL

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Oi Móvel obteve **estrela cheia**, pois atendeu, integralmente, ao parâmetro I, III e V, e atendeu parcialmente ao parâmetro II

Ressaltamos, no entanto, que o parâmetro III, 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 Oi Móvel atendeu ao **parâmetro I**, pois atendeu a todos os sub-parâmetros.

O *sub-parâmetro (a)*, referente aos dados coletados, foi considerado cumprido. Em seu Aviso de Privacidade, a empresa informa:

COMO A OI COLETA DADOS PESSOAIS?

Diretamente com você, por exemplo, na aquisição de serviços e produtos ou durante nossos processos seletivos;

Automaticamente, quando, por exemplo, você navega em nossos sites ou aplicativos.

Através de algum parceiro, caso, por exemplo, você já possua um vínculo com o terceiro.

Em seu Aviso de Privacidade, a empresa informa e exemplifica as categorias de dados pessoais coletados:

CATEGORIA DE DADO PESSOAL

DADOS DE CADASTRO E CONTRATO: Nome, número de CPF, número de RG, número de passaporte, filiação, endereço (físico ou e-mail), número de telefone celular e residencial, número ICCID (cartão SIM), data de nascimento, nacionalidade e profissão.

DADOS FINANCEIROS: Informações da fatura, como histórico, datas de pagamento, valores em aberto ou pagamentos recebidos, informações do cartão de crédito ou débito, conta bancária, entre outros.

DADOS DE LOCALIZAÇÃO E TRÁFEGO: Dados de localização aproximada, quando você tiver ativado a funcionalidade de localização do Sistema de Posicionamento Global (GPS) ou coletados por antenas ERB (Estações Rádio Base), número de telefone de ligações efetuadas ou recebidas, bem como respectivo tempo de duração, número de telefone relacionados ao envio e recebimento de SMS, uso e quantidade dos pacotes ou da conexão de dados, navegação em Wi-Fi, informações do perfil de consumo.

DADOS DE NAVEGAÇÃO NOS SITES E APLICATIVOS DA Oi: Dados de dispositivos e navegação (modelo, data, hora, IP) e cookies.

Em sua Política de Privacidade, a empresa informa de maneira exaustiva os dados de cadastros e contratos, as informações financeiras, os dados de localização, dados sobre uso do site e aplicativos, dados de atendimento, de tráfego e estatísticos coletados.

Que dados a Oi coleta?

Seus dados pessoais tratados e a forma de coleta poderão variar de acordo com os serviços contratados por você ou de acordo com a forma de uso dos seus serviços. Não importa se a coleta for feita a partir da inserção voluntária dos dados por você nas plataformas da Oi, de forma automática quando usa nossos serviços, quando acessa nossos sites ou qualquer outra forma de interação com a Oi.

Coletamos seus dados de cadastro e contrato

- Seu nome, número de CPF, número de RG, número de passaporte, filiação, endereço (físico ou e-mail), número de telefone celular e residencial, número ICCID (cartão SIM), data de nascimento, nacionalidade e profissão.

- Número de CPF, filiação, dados bancários, números de boleto, fatura ou débito em conta e gênero.

- Conteúdo de instrumentos de mandato (procurações) utilizados para ações de contratação ou gestão de contratos de serviços prestados pela Oi e número de telefone comercial.

Coletamos suas informações financeiras

- Informações da fatura, como histórico, datas de pagamento, valores em aberto ou pagamentos recebidos.

- Informações do cartão de crédito ou débito, da conta bancária e outras informações bancárias.

Coletamos seus dados de localização

- Dados de localização aproximada, quando você tiver ativado a funcionalidade de localização que utiliza os dados do Sistema de Posicionamento Global (GPS) ou outra tecnologia, e quando referentes aos sinais identificados pelas estações de base da rede móvel da Oi.

Coletamos seus dados sobre o modo de uso do site e dos aplicativos da Oi

- O histórico sobre o modo de uso e navegação realizada por você nos mais diversos meios e plataformas disponibilizados pela Oi.

Coletamos seus dados de atendimento

As informações prestadas nos serviços de atendimento ao cliente, através de qualquer meio disponibilizado pela Oi.

Coletamos seus dados de tráfego

- A duração das ligações, o uso e a quantidade dos pacotes ou da conexão de dados. Ou como você está usando os dados.
- As informações do perfil de consumo.

Coletamos dados estatísticos

A Oi faz o levantamento de informações de logs de uso para mapear o perfil de tráfego de voz e dados.

O *sub-parâmetro (b)*, referente às situações em que a coleta ocorre, também foi considerado cumprido. Isso porque na seção “Como a Oi Coleta Dados Pessoais” do Aviso de Privacidade (vide trecho acima), informa-se que os dados são coletados na aquisição de serviços e produtos, em processos seletivos; automaticamente quando o titular navega nos sites ou aplicativos da empresa; ou através de parceiros. Na Política de Privacidade, especifica-se a coleta de dados de uso dos produtos e serviços contratados, históricos de chamadas, dados de atendimento, transações de recarga, dentre outros. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

O *sub-parâmetro (c)*, referente à finalidade do tratamento de dados, foi considerado cumprido. Na seção “Para quais finalidades a Oi coleta dados pessoais”, a empresa informa quatro hipóteses de finalidade:

Prestação de Serviços: Se você for um de nossos clientes, como assinante da nossa fibra, vamos precisar coletar seus dados cadastrais, de localização, financeiros, entre outros, para formalizarmos o contrato de prestação de serviços e processarmos os pagamentos.

Processo Seletivo: Se quiser trabalhar com a gente, teremos que coletar informações profissionais, como histórico educacional, profissão, entre outros, para avaliarmos se o seu perfil é compatível com a vaga.

Parceiros: Agora, se você for um de nossos parceiros, necessitamos coletar dados cadastrais das pessoas físicas que vão trabalhar em nossas dependências, para controle de acesso, garantindo assim a segurança de todos os envolvidos na operação.

Cookies: Além disso, como a Oi busca melhorar cada vez mais seus produtos e serviços, podemos utilizar dados de navegação e dados de ativos tecnológicos, como cookies, em nossos sites, para melhorar a performance das páginas na web.

Na Política de Privacidade tais informações são destrinchadas em uma tabela, em que é especificado a finalidade do tratamento, quais são os dados tratados e qual é a sua base legal:

Microsoft Word - OIM005320A - Política de Privacidade.docx 3 / 11

nos baseamos para podermos tratá-los de forma adequada.

| Finalidade do tratamento | Dados tratados | Base legal |
|--|--|---|
| <ul style="list-style-type: none"> Atendimento de solicitações para prestação de serviço. Faturamento e processamento de pagamento dos serviços contratados. Atendimento direto, indireto ou, ainda, através de terceiros autorizados pela Oi. Prestação de serviços de roaming. | <ul style="list-style-type: none"> Dados de cadastro e contrato Informações financeiras Dados de tráfego Dados de atendimento Número ICCID (Cartão SIM) | <ul style="list-style-type: none"> Execução de contrato |
| <ul style="list-style-type: none"> Conduzir o planejamento de negócios. Geração e análise de indicadores, relatórios e previsões. Acompanhamento e análises de desempenhos. Estratégia de comunicação. Estratégia de vendas. Auditoria de qualidade. Gestão de controles. | <ul style="list-style-type: none"> Dados de atendimento Dados estatísticos Informações financeiras Dados de localização Dados de tráfego | <ul style="list-style-type: none"> Legítimo interesse |
| <ul style="list-style-type: none"> Prevenção de fraude, uso fraudulento dos serviços Oi e demais medidas que promovam a segurança do usuário na fruição dos serviços contratados. | <ul style="list-style-type: none"> Dados de cadastro e contrato Informações financeiras Dados de tráfego Dados de localização Número ICCID (Cartão SIM) | <ul style="list-style-type: none"> Prevenção à fraude e à segurança do titular Legítimo interesse |
| <ul style="list-style-type: none"> Inovação e evolução dos serviços, de acordo com o nível de serviço prestado aos usuários. | <ul style="list-style-type: none"> Dados de localização Dados sobre o modo de uso do site e aplicativos Dados de atendimento Dados de tráfego | <ul style="list-style-type: none"> Legítimo interesse |

captura de tela de 19.07.2021.

Microsoft Word - OIM005320A - Política de Privacidade.docx 4 / 11

| | | |
|--|---|---|
| <ul style="list-style-type: none"> Análise de tráfego, criando relatório de gestão de forma agregada e estatístico, visando a melhoria da prestação desses serviços sem que os usuários sejam identificados individualmente. Metodologia analítica ("Big Data Analytics") com foco no conjunto de dados variados para identificação de perfil e comportamento com implementação de medidas rigorosas de segurança, garantindo a proteção dos dados pessoais, tornando-os anonimizados sempre que possível. Aperfeiçoar o uso e a experiência do usuário em nossos serviços. | | |
| <ul style="list-style-type: none"> Publicidade de ofertas, promoções, lançamentos e materiais publicitários ou informativos relativos aos serviços da Oi ou de seus parceiros, bem como de terceiros. Uso de localização e metodologia analítica sobre comportamento de uso, padrões e tendências. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados sobre modo de uso do site e aplicativos Dados de tráfego Dados de localização | <ul style="list-style-type: none"> Legítimo interesse |
| <ul style="list-style-type: none"> Apresentar publicidade mais relevante de seus parceiros ou de terceiros em seus canais. Metodologia analítica ("Big Data Analytics") com foco no conjunto de dados variados para criação de público-alvo segmentado e, sempre que possível, anonimizado. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados sobre modo de uso do site e aplicativos Dados de tráfego Dados de localização | <ul style="list-style-type: none"> Legítimo interesse |
| <ul style="list-style-type: none"> Envio de informações, relatórios e indicadores à Anatel. Envio de informações, relatórios e pareceres ao Procon e demais órgãos e autoridades competentes. Quebra de sigilo telefônico, em determinados casos, quando solicitado por autoridade policial, Ministério Público e ordens judiciais. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados de atendimento Informações financeiras Dados de tráfego Dados de localização | <ul style="list-style-type: none"> Cumprimento de obrigação legal ou regulatória |
| <ul style="list-style-type: none"> Efetuar, exercer ou defender ações judiciais. Resposta a ofícios e cumprimento de liminares. Defesa em processos administrativos, relacionados aos órgãos de defesa do consumidor. | <ul style="list-style-type: none"> Dados de cadastro e contrato Dados de atendimento Informações financeiras Dados de tráfego | <ul style="list-style-type: none"> Exercício regular de direitos |

captura de tela de 19.07.2021.

No mesmo documento, a empresa detalha, também, quais são as bases legais para o tratamento de dados:

As bases legais para tratamento de dados

A Oi poderá realizar o tratamento dos seus dados pessoais amparada nas seguintes bases legais:

- Para a correta execução do contrato ou prestação do serviço contratado, ou até mesmo para eventuais procedimentos preliminares necessários, e também para o atendimento das suas eventuais solicitações.
- Para o cumprimento de obrigação legal ou regulatória.
- No atendimento ao seu legítimo interesse ou ao interesse do Grupo Oi, incluindo, mas não se limitando, ao apoio e promoção de suas atividades e na proteção, em relação aos titulares, do exercício regular de seus direitos ou prestação de serviços que os beneficiem de alguma forma.
- Mediante o fornecimento do seu consentimento, através de manifestação livre, informada e inequívoca, para uma finalidade determinada.
- Para medidas de prevenção à fraude e à sua segurança.
- Para o exercício regular de direitos no âmbito de processos judiciais ou administrativos.
- Para uso compartilhado de dados com a Administração Pública, para o tratamento necessário à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres

A empresa detalha de maneira exaustiva quais são os dados tratados, bem como suas finalidades e base legais especificamente para cada tipo de tratamento de dados. Consideramos positiva a forma como a empresa específica tais informações e, por isso, o sub-parâmetro foi considerado atendido.

O *sub-parâmetro (d)*, referente à forma como se dá a utilização, foi considerado cumprido. Na seção “Saiba mais” do Aviso de Privacidade, a empresa informa como utiliza dados pessoais em portais e nos aplicativos da Oi:

Minha Oi

Na Minha Oi, você consegue visualizar os produtos contratados, acompanhar consumo, saber sobre sua oferta atual, recarregar e ainda ter acesso a outros serviços da Oi. Para que tudo isso seja possível, utilizamos dados pessoais. Por exemplo:

- Para exibir as informações sobre sua oferta, precisamos ter acesso a seus dados pessoais, como número de telefone, além de dados de localização e tráfego.
- Se quiser comprar pacotes, mudar sua oferta ou ainda contratar outros serviços, vamos precisar de seus dados cadastrais, dados de localização e tráfego, além de dados financeiros, para processar pagamentos.
- Agora, se precisar de suporte técnico, podemos utilizar dados cadastrais, dados de localização e tráfego, além de dados de navegação e ativos tecnológicos, a depender de sua necessidade.
- Além disso, podemos utilizar dados cadastrais, dados de localização e tráfego para oferecer novos produtos e medir a qualidade dos nossos serviços.

Técnico Virtual Oi

Através do Técnico Virtual, oferecemos soluções para problemas com a internet banda larga ou fibra, TV por satélite ou telefone fixo. Por esse motivo, utilizamos dados pessoais, como dados cadastrais, dados de localização e tráfego e ainda dados de navegação e dados de ativos tecnológicos a fim de viabilizar a prestação do serviço.

Oi Play

É o serviço de streaming da Oi para você ter acesso a filmes, séries e canais de televisão em um só lugar. Nessa plataforma, podemos usar dados pessoais de diversas formas, como, por exemplo:

- Para efetuar a contratação do serviço, coletamos dados cadastrais, de localização, financeiros, entre outros, para formalizarmos o contrato de prestação de serviços e processarmos os pagamentos.
- Para que você possa acessar o conteúdo dos canais e plataformas, podemos precisar autenticar sua identidade, compartilhando algum dado pessoal, como, por exemplo, CPF, com a plataforma parceira.
- Ainda, podemos utilizar dados de navegação e dados de ativos tecnológicos, como cookies, com o objetivo de melhorar a performance do nosso portal e corrigir eventuais erros.

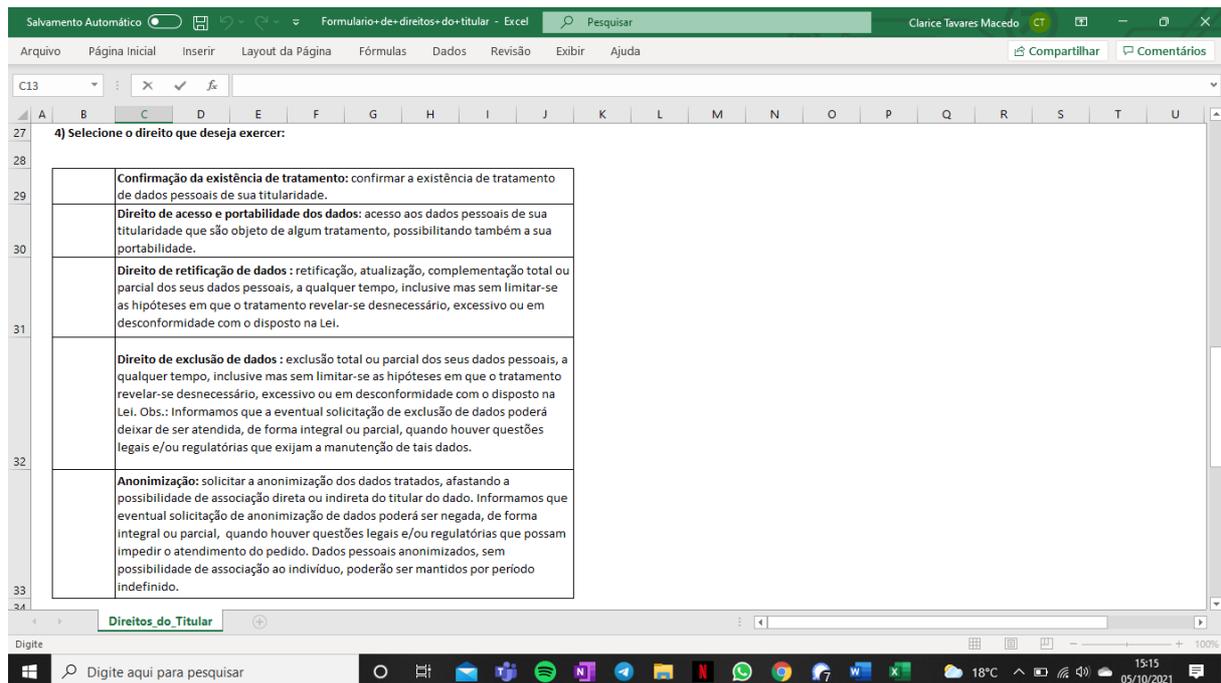
Na seção “As bases legais para o tratamento de dados” da Política de Privacidade (vide trecho acima), a empresa detalha como se dá a utilização, especificando que os dados são utilizados “para a correta execução do contrato ou prestação do serviço contratado”, “para o exercício regular de direitos no âmbito de processos judiciais ou administrativos”, “para uso compartilhado de dados com a Administração Pública” etc. Considerou-se que tais informações são capazes de detalhar a forma de utilização dos dados pessoais.

Por fim, o *sub-parâmetro (e)*, relativo à informação quanto aos direitos dos titulares e meios para exercício desses direitos, foi considerado atendido. Em seu Portal de Privacidade, na seção “Direito dos titulares”, a empresa informa um e-mail para o exercício desses direitos previstos na LGPD. A Oi fornece um canal específico para o titular dos dados, para o representante de um titular de dados e para colaboradores ou ex-colaboradores.

Direitos dos titulares

Agora, se quiser exercer algum dos direitos previstos na LGPD, baixe o arquivo XLSX através de um dos links abaixo e o encaminhe para o e-mail PP-PrivacidadeDireitoTitular@oi.net.br

Na seção “Quais são meus direitos” a empresa apenas informa genericamente que “a Lei Geral de Proteção de Dados Pessoais estabelece que você, enquanto titular de dados pessoais (dono de suas próprias informações), possui uma série de direitos, como acesso aos dados que possuímos sobre a sua pessoa, correção de informações desatualizadas, entre outros”. Nos formulários para o exercício dos direitos do titular, a empresa especifica e define os direitos elencados pela lei:



Captura de tela do formulário para exercício de direitos. 05 de outubro de 2021

Em sua Política de Privacidade, na seção “Quais são os seus direitos”, a empresa informa quais são os direitos sobre os dados pessoais previstos na Lei Geral de Proteção de Dados (direito de acesso e de confirmação de tratamento, de correção, de eliminação, de objeção, de portabilidade, de anonimização, de pedido de informações e o direito de fornecer ou revogar o consentimento) e informa um e-mail para o exercício desses direitos. Ademais, a empresa informa que, para atender determinadas exigências legais, não pode eliminar ou anonimizar dados que “sejam inerentes à prestação do serviço pela Oi”, a menos que haja determinação judicial para tal.

A Lei Geral de Proteção de Dados (LGPD) confere a você direitos sobre seus dados pessoais, conforme mostramos a seguir.

Direito de acesso e de confirmação de tratamento: você tem o direito de confirmar a existência de tratamento dos seus dados pessoais e também de acesso e requisição de cópia desses dados, ressalvadas as hipóteses de sigilo legal.

Direito de correção: você também tem o direito de solicitar a retificação, atualização ou complementação dos seus dados pessoais.

Direito de eliminação: você pode solicitar a exclusão dos seus dados pessoais, exceto se aplicável

outra hipótese legal que impeça a exclusão ou que torne necessária a continuidade do tratamento.

Direito de objeção: você pode solicitar, temporária ou permanentemente, a interrupção do

tratamento de todos ou alguns dos seus dados pessoais, exceto se aplicável outra hipótese legal que impeça a exclusão ou que torne necessária a continuidade do tratamento.

Direito de portabilidade: você pode pedir seus dados pessoais de forma estruturada, de forma que possam ser transmitidos a outro fornecedor de serviço ou produto, mediante solicitação.

Anonimização: você pode solicitar que seus dados pessoais tratados se tornem anônimos, podendo requerer o bloqueio ou a eliminação daqueles considerados desnecessários ou excessivos para finalidade aplicável ao caso concreto ou na hipótese de eventual tratamento em desacordo com a legislação aplicável. Exceto se aplicável outra hipótese legal que impeça a anonimização, bloqueio ou eliminação desses dados ou que torne necessária a continuidade do seu tratamento.

Informações de compartilhamento: você pode pedir informações sobre entidades públicas ou privadas com as quais seus dados pessoais foram compartilhados para o cumprimento das finalidades previstas nesta Política de Privacidade, com exceção dos casos de sigilo legal.

Consentimento: você também pode fornecer e revogar, a qualquer momento, o consentimento anteriormente dado à Oi mediante manifestação expressa, além de solicitar informações sobre a possibilidade de não fornecer consentimento e sobre as eventuais consequências da negativa.

Você pode exercer esses direitos a qualquer momento. Basta enviar uma mensagem para o e-mail PP-PrivacidadeDireitoTitular@oi.net.br

Você reconhece que os termos dos direitos citados nesta página serão assegurados nos termos legais e regulatórios aplicáveis em cada caso concreto.

Eliminação e anonimização

Para atender determinadas exigências legais estabelecidas pelos órgãos reguladores, com exceção de determinação judicial, não poderão ser eliminados ou anonimizados dados que sejam inerentes à prestação do serviço pela Oi, como dados cadastrais, dados de cobrança, dados de localização e dados de tráfego.

O **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, foi considerado parcialmente atendido, pois a empresa atendeu aos sub-parâmetros (c), (e), (f) e (h) e parcialmente ao sub-parâmetro (g).

O *sub-parâmetro (a)*, referente ao tempo e local de armazenamento dos dados, não foi considerado cumprido. Quanto ao tempo de armazenamento, na seção “Por quanto tempo meus dados são armazenados pela Oi?” do Aviso de Privacidade, a empresa informa que mantém os dados pelo período necessário para cumprimento da finalidade e afirma que armazena os dados de acordo com as normas legais. No entanto, a empresa não especifica quais seriam esses dados ou qual seria a legislação vigente aplicável. Tais informações foram consideradas insuficientes, visto que a empresa não estabelece prazos mínimos ou máximos pelo qual armazena os dados de seus clientes.

POR QUANTO TEMPO MEUS DADOS SÃO ARMAZENADOS PELA OI?

Seus dados ficarão conosco apenas pelo período necessário para o cumprimento de alguma finalidade, como, por exemplo, para prestação de

nossos serviços, atendimento a uma obrigação legal/regulatória, ou para nos ajudar a melhorar nossos produtos. Em qualquer caso, armazenaremos seus dados de acordo com a lei, de forma segura, transparente e por tempo limitado.

Na seção “Retenção e término do tratamento dos dados pessoais” da Política de Privacidade, a empresa informa apenas que os dados poderão ser mantidos após o encerramento do contrato e informa genericamente que “os dados pessoais usados para fornecer uma experiência personalizada a você serão mantidos exclusivamente pelo tempo permitido, de acordo com a legislação vigente” e que os dados são mantidos por tempo “estritamente necessário para o cumprimento de obrigação legal e regulatório após o cumprimento do contrato”. No entanto, a empresa não especifica quais seriam esses dados ou qual seria a legislação vigente aplicável. Tais informações foram consideradas insuficientes, visto que a empresa não estabelece prazos mínimos ou máximos pelo qual armazena os dados de seus clientes.

Retenção e término do tratamento dos dados pessoais

- A Oi poderá manter armazenados os seus dados pessoais após o encerramento de contrato ou o término do serviço contratado por você, conforme se revele estritamente necessário para o cumprimento de obrigação legal ou regulatória a que estejamos sujeitos. Ou ainda para exercício de algum direito da Oi em processo administrativo, judicial ou extrajudicial, sem prejuízo da aplicação das hipóteses mencionadas pelo art. 16 da Lei Geral de Proteção de Dados Pessoais (LGPD).

- Os dados pessoais usados para fornecer uma experiência personalizada a você serão mantidos exclusivamente pelo tempo permitido, de acordo com a legislação vigente. - Seus dados pessoais serão tratados apenas durante o período necessário para o alcance das finalidades pretendidas, conforme estabelecido no item 3 desta Política de Privacidade.

Quanto ao local de armazenamento dos dados, o Aviso de Privacidade e a Política de Privacidade não oferece quaisquer informações sobre o local de armazenamento dos dados. Tais informações também não foram encontradas em nenhum dos contratos da empresa.

Quanto ao *sub-parâmetro (b)*, referente a quando/se os dados são apagados, não foi considerado cumprido. A empresa informa apenas que os dados são armazenados de acordo com a lei e por tempo limitado (vide trecho acima), sem especificar prazos ou quais são as legislações aplicáveis.

Na seção “Eliminação e anonimização”, a empresa prevê que, em razão do cumprimento de exigências legais, determinados dados, como dados cadastrais, dados de cobrança, dados de localização e dados de tráfego, não poderão ser eliminados ou sequer anonimizados. Tal informação diverge da legislação atualmente posta. O Marco Civil da Internet, por exemplo, estabelece prazos mínimos pelos quais os dados devem ser guardados, mas não prevê a proibição de que sejam eliminados. Ainda, a empresa informa apenas, na seção “Retenção e término do tratamento dos dados pessoais” da Política de Privacidade” (vide trecho acima) que mantém os dados armazenados apenas “conforme se revele estritamente necessário para o cumprimento de obrigação legal ou regulatória”, sem prever expressamente o apagamento dos dados.

Eliminação e anonimização

- Para atender determinadas exigências legais estabelecidas pelos órgãos reguladores, com exceção de determinação judicial, não poderão ser eliminados ou anonimizados dados que sejam inerentes à prestação do serviço pela Oi, como dados cadastrais, dados de cobrança, dados de localização e dados de tráfego.

Quanto ao *sub-parâmetro (c)*, referente a quais práticas de segurança observa, considerou-se que foi atendido. Na cláusula 16.11 do Contrato de Serviço Móvel Pessoal Pós Pago, a empresa faz uma menção genérica a respeito da preservação do sigilo dos dados cadastrais e de registros de conexão, sem, no entanto, trazer qualquer informação sobre como esses dados seriam protegidos.

“16.11. A Oi se compromete a respeitar a preservação da intimidade, a vida privada, da honra e a imagem das partes direta ou indiretamente envolvidas no que tange ao sigilo de dados, tanto os cadastrais quanto os referentes aos registros de conexão.” (p. 9)

Em seu Aviso de Privacidade, na seção “Meus dados estão protegidos na Oi?”, a empresa informa:

Na Oi, temos como propósito transformar o ambiente digital, aplicando as melhores tecnologias disponíveis no mercado para garantir segurança das informações que possuímos e fazer jus à confiança que você nos deposita. Quando falamos de dados pessoais, essa preocupação é ainda maior e não medimos esforços para assegurar sua privacidade, por isso, aplicamos e renovamos constantemente nossos protocolos de segurança, além de possuímos regras internas que orientam o armazenamento de dados pessoais em locais seguros, reduzindo a possibilidade de acessos não autorizados ou o vazamento de informações.

Em sua Política de Privacidade, na seção “Segurança da Informação”, a empresa informa:

Segurança da informação

A Oi se compromete a garantir a segurança e a manutenção da proteção dos seus dados pessoais armazenados com a adoção das medidas técnicas e administrativas aptas a proteger os dados pessoais exportados de acessos não autorizados e de situações acidentais ou ilícitas, de acordo com as legislações aplicáveis.

Os colaboradores da Oi têm o compromisso de zelar pela segurança dos seus dados pessoais e de respeitar esta Política de Privacidade, sob pena de sofrerem sanção disciplinar em caso de violação dessas normas.

Esperamos que você também contribua com a segurança, mantendo seus dados pessoais seguros. Ao se cadastrar nas plataformas da Oi, escolha uma senha forte o suficiente para evitar que outras pessoas a adivinhem.

A Oi recomenda que você nunca revele ou compartilhe a sua senha com outras pessoas. Você

é o único responsável por manter a senha confidencial e por qualquer ação realizada através de sua conta nos sites e serviços do Grupo Oi.

As proteções citadas elencadas nesta seção não se aplicam a informações que você tenha escolhido compartilhar em áreas públicas, como fóruns e redes sociais de outras companhias.

A Oi se compromete a divulgar para você e órgãos competentes qualquer incidente de segurança e quais as medidas que serão aplicadas nesse caso.

Em seu Relatório de Sustentabilidade, a empresa detalha as práticas de segurança que observa. Afirma ter a certificação ISO 27001 e afirma utilizar o antivírus chamado Endpoint Security EDR. Essas informações foram consideradas suficientes para o sub-parâmetro.

A Oi possui a certificação ISO 27001, que assegura a qualidade e a confiabilidade do sistema de gestão da Segurança da Informação da Companhia, protegendo as redes de dados dos clientes de todo o país contra possíveis ataques cibernéticos.

Em 2020, para fazer com que empresas públicas ou privadas estivessem menos vulneráveis a ciberataques, entre outros riscos decorrentes do ambiente on-line, a Oi passou a oferecer esses serviços de segurança cibernética como tema de alta prioridade.

Em meio ao aumento de ciberataques ocasionados principalmente por conta do regime de home office adotado pela maioria das empresas, devido às necessidades impostas pela pandemia, a Oi desenvolveu um antivírus chamado Endpoint Security EDR, que combina inteligência artificial e machine learning para bloquear ameaças em tempo real – enquanto o antivírus roda, identifica as novas variantes que vão surgindo e já se adapta para combater a ameaça.

Com base na experiência da Companhia para a proteção de dados de seus clientes e sistemas internos, a Oi, por meio do Oi Soluções, oferece esse serviço e pretende ampliar a sua oferta de projetos de segurança em 2021.

O *sub-parâmetro (d)*, referente a quem tem acesso aos dados, não foi considerado cumprido. Na seção “Meus dados estão protegidos na Oi?” (vide trecho acima), a empresa informa apenas que adota protocolos de segurança para proteger os dados de “acessos não autorizados”, mas não oferece quaisquer informações sobre quem tem acesso aos dados pessoais.

O *sub-parâmetro (e)*, referente aos terceiros com quem os dados são compartilhados, foi considerado atendido. Em seu Aviso de Privacidade, a empresa informa, genericamente, algumas hipóteses de compartilhamento de dados:

A OI COMPARTILHA MEUS DADOS PESSOAIS COM ALGUÉM?

Para a prestação de nossos serviços, a Oi conta com parceiros de negócios que podem ter acesso a alguns de seus dados pessoais. Todos os nossos parceiros passam por um processo de avaliação prévio, de modo que apenas aqueles que compartilham nossos valores participarão de nossas atividades.

Ainda adotamos medidas específicas para garantia da segurança e controle de seus dados pessoais, mesmo quando compartilhados. O compromisso

que estabelecemos com você neste aviso também se estende às pessoas que trabalham conosco. Além de nossos parceiros, podemos compartilhar seus dados com autoridades governamentais, como, por exemplo, autoridades policiais, Ministério Público, Tribunais de Justiça, órgãos de defesa do consumidor, Anatel, entre outros, para cumprimento de alguma obrigação legal, regulatória ou ordem judicial.

Da mesma forma, podemos compartilhar dados pessoais para instituições de proteção ao crédito para reduzir o risco de crédito e o uso fraudulento dos serviços Oi. Seja para onde for, compartilharemos seus dados de acordo com a legislação brasileira e reafirmamos nosso compromisso de transparência com você.

Em sua Política de Privacidade, a empresa informa com quais terceiros compartilha os dados e para quais finalidades:

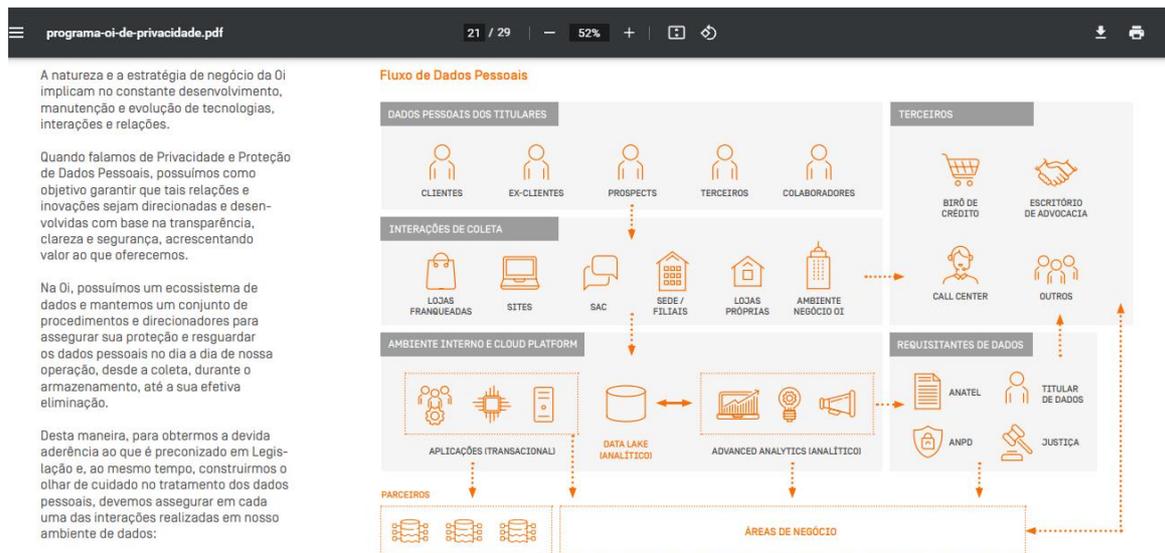
Compartilhamento dos dados

A Oi não compartilha os seus dados pessoais com empresas, organizações ou terceiros, apenas nestes casos abaixo, e sempre de acordo com esta Política de Privacidade e outras medidas de segurança e de confidencialidade adequadas:

- Entre empresas do Grupo Oi para manutenção, promoção e melhoria dos serviços.
- Para parceiros comerciais no desenvolvimento de promoções e ações comerciais conjuntas com a Oi.
- Para prestadores de serviço de marketing, como envio de e-mail marketing, SMS e veiculação de anúncios online.
- Para parceiros de vendas e lojas franqueadas, na colaboração às vendas de produtos e serviços fornecidos pela Oi.
- Para terceiros contratados ou autorizados para cuidados relacionados à execução ou gestão dos serviços Oi, como, por exemplo, prestadores de serviço de suporte técnico e reparo de serviços, análise de dados, consultoria, impressão de faturas, consultas ao sistema de proteção ao crédito e centrais de atendimento ao cliente.
- Para autoridades governamentais, como, por exemplo, autoridades policiais, Ministério Público, Tribunais de Justiça, órgãos de defesa do consumidor ou Anatel, por conta de obrigação legal, regulatória, ordem judicial ou demais solicitações de autoridades com poderes para tanto, para proteger de prejuízos à propriedade ou à segurança do Grupo Oi ou de seus clientes, conforme solicitado ou permitido por lei.
- Para instituições de proteção ao crédito, para reduzir o risco de crédito e o uso fraudulento dos serviços Oi.
- Para terceiros, não previstos aqui, mediante o seu consentimento específico.
- Para agências de cobranças de dívidas, em casos de inadimplência.
- Para terceiros, em razão de reestruturação societária no Grupo Oi.

A Oi solicitará a você o consentimento específico para compartilhar qualquer dado pessoal sensível

Em seu Programa Oi de Privacidade, a empresa apresenta um fluxo de dados em que informa os trajetos que os dados percorrem dentro da empresa, com os titulares e com terceiros:



Captura de tela feita em 06 de outubro de 2021, p. 21.

O fluxo é claro e facilita a comunicação com os usuários. Parabenizamos a empresa pela iniciativa e pela transparência.

Quanto ao *sub-parâmetro (f)*, relativo às finalidades do compartilhamento de dados com terceiros, considerou-se atendido. O Aviso de Privacidade e a Política de Privacidade informa, em algumas hipóteses a finalidade do compartilhamento de dados com terceiros (vide trecho acima), como por exemplo, por obrigação legal, para reduzir o risco de crédito e uso fraudulento. Tais informações foram consideradas suficientes.

Quanto ao *sub-parâmetro (g)*, relativo às hipóteses de transferência internacional de dados, foi considerado parcialmente cumprido. Em seu Aviso de Privacidade, a empresa informa que transfere dados para outros países para armazenamento em nuvem ou para prestação de serviços. A empresa não especifica, no entanto, com quais países, nem em quais hipóteses. No entanto, como houve a preocupação em informar sobre a possibilidade de transferência internacional de dados em seu Aviso de Privacidade, o sub-parâmetro foi considerado parcialmente atendido.

A OI TRANSFERE DADOS PESSOAIS PARA OUTROS PAÍSES?

A internet possibilitou quebrar barreiras geográficas e conectar as pessoas ao redor do mundo e, para que isso aconteça, muitas vezes os dados pessoais circulam entre os países. Como buscamos empregar as melhores tecnologias disponíveis no mercado, em algumas situações, pode haver transferência de dados pessoais para fora do Brasil, como, por exemplo, para armazenamento em nuvem ou se necessário para prestação de um serviço. Em qualquer caso, sempre fazemos isso respeitando a legislação brasileira.

Por fim, quanto ao *sub-parâmetro (h)*, relativo à data da última atualização da política de privacidade, foi considerado cumprido. O Aviso de Privacidade e a Política de Privacidade da empresa apresentam o dia da última atualização, por isso o sub-parâmetro foi considerado atendido. No entanto, vale ressaltar que tal informação não consta nos contratos da empresa. Recomendamos que a prática de informar a última atualização não se limite às políticas de privacidade e que seja aplicado em todos os documentos da empresa.

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. Após pedido de acesso a dados, a empresa respondeu, tempestivamente, à solicitação.

O **parâmetro IV**, que avalia se a empresa promete enviar notificações ao usuário na hipótese de atualização de suas políticas de privacidade, não foi considerado cumprido. Em seu Aviso de Privacidade a empresa apenas informa que o documento poderá ser alterado e recomenda que o titular faça visitas periódicas ao site, sem se comprometer a notificar o usuário.

ESTE AVISO DE PRIVACIDADE PODE MUDAR?

Como a Oi está sempre melhorando seus serviços e produtos, este Aviso de Privacidade pode ser atualizado. Por isso, sugerimos sua visita periódica nesta página.

Em sua Política de Privacidade, a empresa informa que a Oi tem o direito de alterar a política sem aviso prévio e apenas se compromete a divulgar a alteração na página inicial e em outros canais de comunicação, sem, no entanto, prometer enviar notificações aos usuários.

Alterações à política de privacidade

A Oi tem o direito de, quando necessário, sem aviso prévio e com efeitos imediatos, alterar, acrescentar ou revogar, parcial ou totalmente, esta Política de Privacidade, desde que de acordo com a legislação vigente. Recomendamos que você acesse esta página com frequência, ou sempre que tiver dúvidas, para acompanhar qualquer atualização ou mudança em nossa Política de Privacidade. No caso de alterações em nossa Política de Privacidade, divulgaremos imediatamente através de aviso em destaque na página inicial do nosso site e em outros canais de comunicação e relacionamento da Oi com seus clientes.

Na cláusula 7.1.I do contrato pré-pago, a empresa prevê como direito do cliente ser comunicado, previamente, de alterações nas condições do contrato. No entanto, a empresa não informa como o cliente será comunicado, se é por meio de notificação ao cliente ou atualizações no site ou redes sociais.

“7 – Conheça seus direitos e deveres

7.1 Além dos demais direitos previstos em lei, você tem os seguintes direitos:

I. Ser comunicado, antecipadamente, sobre qualquer alteração nas condições de prestação do serviço que afetem você;”

Em virtude da redação ampla da cláusula do contrato e da falta de comprometimento de notificar o cliente no Aviso de Privacidade e na Política de Privacidade, o parâmetro não foi considerado atendido.

Por fim, o **parâmetro V**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado cumprido. Isso porque a Oi dispõe de um Portal de Privacidade com informações claras sobre o tema. O portal pode ser facilmente acessado ao final da página inicial da Oi.



No entanto, a Política de Privacidade da empresa, o documento mais completo e com mais informações sobre as operações de tratamento de dados realizadas pela Oi, não está disponível no Portal de Privacidade. Para acessar o documento é preciso realizar uma busca ativa, por meio da seção “de A a Z”, ao final da página inicial da empresa. Recomenda-se que a Política de Privacidade, em razão do seu detalhamento e importância, esteja mais acessível, preferencialmente, no próprio Portal da empresa.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Oi Móvel obteve $\frac{1}{4}$ de estrela, pois atendeu parcialmente ao parâmetro I

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente atendido. Em seu Aviso de Privacidade e Política de Privacidade, a empresa informa, genericamente, que compartilha dados com autoridades governamentais, como autoridades policiais, Ministério Público, Tribunais de Justiça ou Anatel, para o cumprimento de obrigações legais. No entanto, a empresa não discrimina com quais das autoridades citadas o compartilhamento é realizado sem ordem judicial e quais das autoridades podem ter acesso aos dados apenas mediante autorização judicial.

A OI COMPARTILHA MEUS DADOS PESSOAIS COM ALGUÉM?:

(...) podemos compartilhar seus dados com autoridades governamentais, como, por exemplo, autoridades policiais, Ministério Público, Tribunais de Justiça, órgãos de defesa do consumidor, Anatel, entre outros, para cumprimento de alguma obrigação legal, regulatória ou ordem judicial.

No Contrato de Serviço Móvel Pessoal Pós-Pago, na cláusula 16, a empresa se compromete a fornecer dados cadastrais apenas a autoridades administrativas competentes, sem, no entanto, identificá-las.

CONTRATO SMP POS

16.13. A Oi se compromete a fornecer dados cadastrais, sem a necessidade de prévia ordem judicial, apenas para autoridades administrativas que possuam competência legal para a requisição.

Apesar de a empresa identificar as autoridades em seu Aviso de Privacidade e de se comprometer a fornecer dados cadastrais apenas a autoridades administrativas competentes, a redação das duas cláusulas foi considerada insatisfatória e por isso o parâmetro foi considerado parcialmente cumprido.

Vale ressaltar que a empresa não esclarece ao usuário o fato de que dados cadastrais e registros de conexão possuem tratamento jurídico diferenciado. Neste sentido, é importante que a empresa informe claramente que registros de conexão somente podem ser entregues mediante ordem judicial, segundo o Marco Civil da Internet. No que se refere a dados cadastrais, essa mesma lei autoriza que sejam requisitados sem ordem judicial por autoridades administrativas competentes. Atualmente, entretanto, em face de controvérsia sobre quais são tais “autoridades administrativas competentes”, é imprescindível que a empresa seja transparente acerca de suas próprias interpretações da lei que aplica quando recebe pedidos de quebra de sigilo.

O **parâmetro II**, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, não foi considerado atendido. Não foi encontrada menção ao tema nos documentos analisados da Oi Móvel.

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

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, foi não foi considerado cumprido. A Oi Móvel prevê em seus contratos pré e pós-pago que registros de conexão são disponibilizados apenas mediante ordem de um juiz. 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).

CONTRATO SMP POS

16.12. A Oi se compromete a disponibilizar os registros de conexão e de acesso a aplicações de internet, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial.

Por fim, o **parâmetro V**, relativo à existência de protocolos específicos sobre entrega de dados ao estado, não foi atendido. Em nossas buscas, nenhum documento como esse pôde ser localizado.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado:



Nesta categoria, a Oi Móvel obteve **estrela cheia**, tendo atendido a ambos os 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, e não localizamos quaisquer ações nesse sentido.

Na fase de interação com as empresas, tivemos acesso à contestação elaborada pela Oi, com outras empresas de telefonia, contra a Lei Estadual nº 20.089/2019, do Estado do Paraná, que impõe às operadoras de telefonia, fixa ou móvel, a obrigatoriedade de garantirem a identificação das chamadas telefônicas, sob pena de serem autuadas nos termos da norma²⁸. Na ação, as empresas argumentam que a lei viola frontalmente o direito constitucional ao sigilo de dados, previsto no art. 5º, X e XII da CF/88.

A propositura da ação contra a Lei nº 20.089/2019 do Estado do Paraná demonstra uma preocupação com o direito à privacidade e ao sigilo dos dados e, por isso, o parâmetro foi considerado atendido.

Por fim, o **parâmetro II**, referente à contestação de pedidos abusivos, foi considerado atendido. Realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado de São Paulo e no portal “Jusbrasil”, em ambos os casos pelos termos “Oi S/A E sigilo E quebra” e por acórdãos publicados entre 01/08/2020 e 21/06/2021, e foi localizada uma ação nesse sentido: [HC 2020.0000746961/TJSP](#), no Tribunal de Justiça de São Paulo. Na ação, a empresa questiona uma ordem de uma autoridade policial que requisitava o fornecimento de senhas de acesso, pelo prazo de 06 meses, de qualquer dado telefônico por ele requerido. A empresa questiona a generalidade do pedido e solicita que sejam identificados os usuários ou terminais telefônicos alvos das medidas, bem como que seja apontada a qual investigação criminal tal ordem estaria vinculada.

²⁸ Processo nº 0001787-36.2020.8.16.0004. Poder Judiciário do Estado do Paraná.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Direta de Inconstitucionalidade (ADI) 5642²⁹, da ACEL, não foram consideradas, já que não registraram movimentações.

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 sigilo 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 Oi Móvel obteve $\frac{1}{2}$ **estrela**, pois atendeu ao parâmetro II.

O **parâmetro I**, relativo ao posicionamento em geral da empresa, não 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.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido.

Em seu Relatório de Sustentabilidade, a empresa afirma (p. 51) ter participada da discussão de diversos projetos de lei no âmbito federal, entre eles o PL 2630/2020, que trata sobre fake news, e o PL 3477/2020, que trata sobre garantia de acesso à Internet, com fins educacionais, aos alunos e professores da educação básica pública. Ainda que seja positiva a inserção dessa informação, não encontramos dados, em sites oficiais ou na mídia, que confirmem a participação, em nome próprio, da empresa.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a

²⁹ 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.

oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial³⁰; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020³¹; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética³²; entre outras.

A empresa participou do Congresso intitulado LGPD – Desafios Enfrentados desde a sua Entrada em Vigor, organizada pela IBRASPD, o Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados. A empresa participou do painel “CISO e DPO – Pandemia dos megavazamentos, como lidar com esse cenário e atender o direito do titular”, na pessoa da Fernanda Vaqueiro, CISO da Oi, no dia 01 de setembro de 2021³³.

No entanto, vale ressaltar que a Oi foi uma das empresas notificadas pelo Procon, no início de 2021, pelo suposto vazamento de dados de mais de 100 milhões de clientes. Em resposta, a empresa informou apenas:

A Oi entende que não é objeto de questionamentos no episódio, já que não se verifica nenhum indício de vazamento de dados de seus clientes.³⁴

No entanto, não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. Por isso, a resposta da empresa foi considerada excessivamente genérica.

Nessa categoria, convidamos as empresas, nessa fase de envio e discussão dos resultados preliminares do relatório, a compartilharem conosco outros eventos públicos e participações relevantes que possam ser consideradas para essa categoria.

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

Resultado: 

³⁰ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

³¹ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

³² TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

³³ <https://www.ibraspd.org/webinar-registration>.

³⁴ O VALOR. Oi e TIM dizem que não detectaram vazamentos de dados de clientes. 17 de fevereiro de 2021. Disponível em: <https://valor.globo.com/empresas/noticia/2021/02/17/oi-e-tim-dizem-que-no-detectaram-vazamentos-de-dados-de-clientes.html>

Nesta categoria, a Oi Móvel estrela vazia, pois não atendeu a nenhum dos parâmetros.

Os **parâmetros I ao IV**, relativos à publicação de relatórios de transparência em português, acessibilidade, periodicidade do relatório e informações sobre pedidos de acesso a dados, não foram considerados atendidos. A empresa publica Relatórios de Sustentabilidade; no entanto, o documento não traz informações significativas sobre privacidade e proteção de dados.

Na página 49 do Relatório de Sustentabilidade 2020, há a informação de que em 2020 foram recebidas 2.438 reclamações pelos canais da Anatel sobre utilização indevida de dados cadastrais. Em 2019, esse número era de 1.220 e em 2018 de 684. Segundo a empresa, esse aumento dos números se deve a “alterações nos dados cadastrados pela Anatel, que começou a valer em novembro de 2019; mas quando essas reclamações foram analisadas, encontrou-se um cenário em que 76% das reclamações apresentaram outros motivos, como restrição a mailing de telemarketing, pedidos de cadastros, contestação de fatura, estorno de conta e cancelamento de produto ou serviço” (p. 49).

No entanto, a empresa não publica estatísticas de pedidos, nem discrimina as autoridades responsáveis ou os fundamentos que apresentam e, por isso, o parâmetro não foi considerado atendido.

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

TIM BANDA LARGA

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a TIM Banda Larga obteve **estrela cheia**, tendo atendido integralmente aos parâmetros I, IV e V; e parcialmente ao parâmetro II.

A Tim Banda Larga atende ao **parâmetro I**, referente às informações sobre coleta e finalidade, fornecendo informações claras e completas sobre todos os sub-parâmetros.

O *sub-parâmetro (a)*, referente a quais dados são coletados, foi considerado 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 |
|---|---|--|---|
| 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) | <p>Funcionamento do Site: ativar funcionalidades essenciais, como software antivírus, adaptar o conteúdo ao formato da tela, entre outras funções.</p> <p>Obrigação Legal: cumprir com as obrigações legais de</p> | <p>Legítimo Interesse</p> <p>Cumprimento de Obrigação Legal</p> |
| | | 5 | |
| | | 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 melhorar sua experiência como usuário e atender as | Legítimo |

Captura de tela: 20/07/2021

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; Informações sobre o uso dos Serviços: volume de tráfego na internet; Dados locais (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. Dados do Dispositivo de Acesso (excluindo páginas visitadas).

O *sub-parâmetro (b)*, referente às situações em que a coleta ocorre, foi igualmente considerado 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.

O *sub-parâmetro (c)*, referente à finalidade da coleta de dados, foi igualmente considerado atendido. No mesmo item referenciado acima, a empresa especifica a finalidade da coleta dos diversos dados que aponta. Especifica, por exemplo, as finalidades de “Funcionamento do Site: ativar funcionalidades essenciais, como software antivírus, adaptar o conteúdo ao formato da tela, entre outras funções”, “analytics: compreender o seu comportamento de navegação e como o Site e App está sendo usado, para melhorar sua experiência como usuário e atender as necessidades dos nossos clientes.”, “Marketing: direcionamento de conteúdos e publicidade, nossa e de nossos parceiros, conforme o seu perfil e preferências”, dentre outros.

Além disso, no Contrato de Prestação de Serviços TIM LIVE, a empresa, na cláusula 19, estabelece:

“19.1 As Partes reconhecem que, em razão do presente Contrato, a TIM realizará o tratamento de dados pessoais do CLIENTE na extensão necessária para garantir a adequada prestação dos SERVIÇOS e, em geral, na forma prevista ou de qualquer forma autorizada na legislação aplicável.

O *sub-parâmetro (d)*, referente à forma como se dá a utilização, foi igualmente considerado atendido. Ao especificar as finalidades para as quais trata dados pessoais, conforme item acima, a empresa mostra também exemplos de sua utilização. Por exemplo, ao apontar a finalidade de “marketing”, especifica que os dados serão utilizados para direcionar “conteúdos e publicidade”. Por mostrar situações de uso paralelamente às finalidades, o *sub-parâmetro* foi considerado atendido.

Por fim, o *sub-parâmetro (e)*, referente aos direitos dos titulares e meios para seu exercício, foi igualmente considerado atendido. Em sua Política de Privacidade, no item “Quais são os direitos dos Titulares de Dados”, a empresa apresenta tabela com os direitos e uma explicação de cada um deles, apontando, por exemplo, o “Direito de confirmar a existência de tratamento dos seus dados e de acessá-los”, o “direito de retificação”, “direito de exclusão”, “direito de oposição”, “direito de solicitar anonimização, bloqueio ou eliminação”, “direito à portabilidade”, dentre outros. Além disso, oferece os e-mails da área de Data Protection Officer (DPO) da TIM para exercício dos referidos direitos.

Além disso, no Contrato de Prestação de Serviços TIM LIVE, a empresa, na cláusula 4, estabelece:

4.2. Constituem direitos do CLIENTE:

- (e) a inviolabilidade e ao segredo de sua comunicação, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações e as atividades de intermediação da comunicação dos portadores de deficiência, nos termos da regulamentação;
- (j) o respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora;

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, foi considerado cumprido, pois atende a todos os sub-parâmetros.

O *sub-parâmetro (a)*, referente ao tempo e onde os dados são armazenados, foi considerado cumprido. No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, a empresa detalha alguns prazos legais para manutenção de dados pessoais, bem como os critérios adotados para determinar o período de retenção adequado.

Prazo de Armazenamento

A TIM armazenará e tratará seus Dados Pessoais somente pelo tempo necessário para cumprir as finalidades da coleta, inclusive para fins de cumprimento de quaisquer obrigações legais, regulatórias, contratuais, de prestação de contas, requisição de autoridades competentes ou outras previstas na legislação vigente, como garantir os direitos dos titulares e seus próprios direitos.

Em geral, a título exemplificativo:

- Dados Pessoais cadastrais podem ser mantidos pelo prazo de 5 anos, tendo como referência o Código de Defesa do Consumidor, a contar do término da relação do titular com a TIM;
- Além disso, por obrigação constante no 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, quanto aos aplicativos da TIM, por no mínimo 6 meses;
- por atuar como prestadora de comunicações, de acordo com o estabelecido pela ANATEL, por meio da Resolução nº 738 de 2020, a TIM tem que manter registro dos dados de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada, pelo período de 5 anos.

Após o término dos prazos, os Dados Pessoais serão devidamente eliminados ou anonimizados pela TIM.

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

Não obstante o disposto acima, a política geral da TIM é que nenhum dado pessoal de clientes da TIM deve ficar armazenado por mais de 5 (cinco) anos a contar do término da relação comercial entre um cliente e a TIM. A exceção a essa regra são situações de cumprimento de uma ordem judicial ou administrativa competente (veja a nossa informativa sobre “Compartilhamento de Dados Pessoais em Caso de Investigação”). Lembrando que este é o período máximo, uma vez cumprida sua finalidade e desde que não haja qualquer obrigação legal ou legítimo interesse para sua manutenção por prazo superior.

Quanto ao local de armazenamento, a empresa informa em sua Política de Privacidade, no item “A TIM pode transferir seus Dados para outros países”:

A TIM poderá transferir dados para outros países para fins de armazenamento, por exemplo, em servidores localizados no exterior, com grau de proteção de dados adequado ao previsto nas legislações vigentes. Informamos que seus Dados poderão estar sujeitos à legislação local e às regras pertinentes destes países. Ao interagir conosco, Você concorda com essa transferência internacional de Dados, nos casos em que seja essencial para prestação dos serviços e execução do seu contrato conosco, de acordo com a legislação de proteção de dados.

No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, a empresa informa, com detalhes, os locais de armazenamento de dados pessoais.

Local de Armazenamento

Por fim, os dados armazenados pela TIM ou por fornecedores contratados seguem níveis rígidos e adequados de segurança da informação e consistentes com as práticas do mercado, sempre buscando atender a Lei Geral de Proteção de Dados Pessoais e demais legislações aplicáveis e vigentes. No geral, os dados pessoais são armazenados:

- (i) em servidores de propriedade da TIM, localizados nos estados de São Paulo e Rio de Janeiro;
- (ii) em servidores de terceiros, contratados pela TIM especificamente para serviços de armazenamento de dados (hosting), seguindo controles contratuais para garantir o cumprimento, a Lei Geral de Proteção de Dados; ou
- (iii) em servidores de terceiros, contratados pela TIM para realizar algum serviço específico temporário e que inclui algum tipo de tratamento de dados (por exemplo, uma verificação de fraude). Nesses casos, além dos controles contratuais, limitamos o tratamento ao mínimo necessário e pelo menor tempo possível (por exemplo, em algumas situações o dado é excluído após poucas horas)

Tais informações foram consideradas suficientes para esclarecer ao usuários sobre as práticas adotadas pela empresa para a retenção de dados pessoais.

Quanto ao *sub-parâmetro (b)*, referente a quando/se os dados são apagados, foi considerado cumprido. No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, na seção Prazo de Armazenamento (vide trecho acima), a empresa informa expressamente que, findo os prazos que autorizam a retenção, a TIM deleta ou anonimiza os dados pessoais.

O *sub-parâmetro (c)*, referente às práticas de segurança que a empresa observa, foi considerado atendido. Em seu Relatório de Sustentabilidade 2020, p. 36, 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.

Por esclarecer a norma de segurança utilizada para proteger seus sistemas, e ao prestar algumas informações em relação aos colaboradores e fornecedores que têm acesso aos dados, considerou-se que as informações dadas eram suficientes.

O *sub-parâmetro (d)*, referente a quem tem acesso aos dados, também foi considerado 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.

O *sub-parâmetro (e)*, referente aos terceiros com quem os dados são compartilhados, foi considerado 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. Ao fazermos isso, nós não precisamos revelar a sua

identidade aos nossos parceiros, ou seja, não compartilhamos seus dados com eles nessas situações.

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

A TIM, assim como qualquer grande organização, opera em parceria com uma série de outras empresas que dão suporte no oferecimento de produtos e serviços TIM. Em alguns casos, para que essas empresas possam nos atender e dar o suporte de que precisamos, pode ser necessário compartilhar certos dados pessoais dos nossos clientes com essas empresas. Nossos parceiros e fornecedores somente são autorizados a utilizar os dados pessoais recebidos para os fins específicos para o qual foram contratados, portanto, eles não irão utilizar os seus dados pessoais para outras finalidades, além da prestação de serviços prevista contratualmente. A TIM executa procedimentos preparatórios à contratação de novos parceiros e fornecedores para garantir que, na hipótese em que seja necessário compartilhar dados pessoais com tais empresas, obrigações contratuais de segurança da informação e de proteção de dados pessoais sejam estabelecidas para proteger os dados de nossos clientes.

Tais informações foram consideradas suficientes para informar sobre o compartilhamento.

Quanto ao *sub-parâmetro (f)*, relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi 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.”

Quanto ao *sub-parâmetro (g)*, referente às hipóteses de transferência internacional de dados, foi considerado atendido. Em sua Política de Privacidade, a empresa informa que a TIM poderá transferir dados para outros países.

A TIM poderá transferir dados para outros países para fins de armazenamento, por exemplo, em servidores localizados no exterior, com grau de proteção de dados adequado ao previsto nas legislações vigentes. Informamos que seus Dados poderão estar sujeitos à legislação local e às regras pertinentes destes países. Ao interagir conosco, Você concorda com essa transferência internacional de Dados, nos casos em que seja essencial para prestação dos serviços e execução do seu contrato conosco, de acordo com a legislação de proteção de dados.

No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, a empresa informa de forma detalhada sobre as práticas de transferência internacional e informa os principais países em os dados são armazenados:

Transferências Internacionais

Ao utilizar os serviços de internet da TIM, é possível que o usuário acesse aplicações de terceiros, cujos servidores estão localizados em outros países, e podem capturar as informações de IP e hora de acesso. Isso faz parte da natureza dos serviços de conexão à internet, e é importante que o usuário sempre adote as melhores práticas de segurança quando navega na internet. Além disso, a TIM pode ativamente realizar a transferência internacional de dados pessoais que estão sob seu controle sempre que contratarmos servidores de terceiros, conforme os itens (i) e (ii) acima. Por se tratarem de serviços “cloud”, esses fornecedores podem a todo momento alterar a localização da hospedagem, mas buscamos limitar contratualmente que essas transferências sejam feitas com segurança e para países quem possuem leis que garantem adequadamente a proteção e segurança dos dados pessoais. Não obstante, os principais servidores de terceiros que armazenam dados pessoais sob controle da TIM estão localizados nos seguintes países, além do Brasil:

- AEE (Área Econômica Europeia);
- Califórnia (EUA).

Ainda, quando armazenado em outra localidade, esta é previamente validada e aprovada pelas funções responsáveis.

Tais informações foram consideradas suficientes para fins desta avaliação.

Por fim, quanto ao *sub-parâmetro (h)*, sobre a data da última atualização da política de privacidade, foi considerada atendida. Tanto a Política de Privacidade quanto os contratos contam com a data da última atualização (com exceção do Contrato de prestação de serviço SMP Corporativo, que não tem data de registro).

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendida. O InternetLab realizou um pedido de acesso a dados em 21 de julho de 2021. Em resposta, a TIM informou:

TIM, em conformidade com as disposições legais aplicáveis, deve identificar o solicitante e verificar a existência dos requisitos de legitimidade para atender às solicitações.

Sendo assim, pedimos a gentileza de nos enviar sua solicitação novamente, desta vez acompanhada de documentação necessária (ex.: cópia de um documento de identidade válido), para que possamos fornecer um feedback.

Essa solicitação também visa proteger os titulares da comunicação indevida de seus dados pessoais a terceiros não autorizados.

Atenciosamente,

Data Protection Officer

Após o envio da documentação solicitada pela empresa, a TIM informou, por email, os dados pessoais que possuía sobre o titular, bem como um arquivo Word com as telas comprobatórias dos sistemas em que constam tais dados. Consideramos positiva a exigência de comprovação da titularidade para concessão do acesso aos dados. Por isso, o parâmetro foi considerado atendido.

O **parâmetro IV**, 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 V**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado atendido. A empresa tem um Portal de Privacidade³⁵ com as principais informações de privacidade e proteção de dados. Ainda, a empresa disponibilizou Informativos de Privacidade, em que traz informações detalhadas sobre práticas de privacidade e proteção de dados da empresa.

³⁵ <https://www.tim.com.br/sp/sobre-a-tim/institucional/seguranca/politica-de-privacidade>



Protegemos seus dados e somos transparentes sobre o uso deles

[Sobre a TIM](#) >

O nosso compromisso com Proteção de Dados

Relatório - InternetLab

Projeto de Adequação

Principais ações executadas durante o Projeto de Adequação

Direitos dos Titulares

Sobre a TIM

A TIM S.A. é uma das maiores empresas de telecomunicação do Brasil, além de fazer parte de um grupo multinacional com presença local há mais de 20 anos.

Somos a primeira operadora a ter presença nacional. Com a inovação em nosso DNA, buscamos sempre potencializar a vida de nossos clientes através da tecnologia. Para isso, além de trabalhar na ampliação e melhoria da rede, apostamos em um portfólio completo com telefonia móvel, fixa e internet. Assim, nossos clientes individuais e corporativos estarão sempre conectados.

A transparência é um de nossos pilares. Somos a única empresa do setor de telecomunicações no Novo Mercado da BM&FBOVESPA, reconhecido como nível máximo de governança corporativa. Também fazemos parte do Índice de Sustentabilidade Empresarial (ISE) e do Índice de Carbono Eficiente (ICO2).

Como outro destaque, temos o site [Dados Abertos](#), no qual consumidores

Captura de tela: 08/10/2021.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado:

Nesta categoria, a Tim Banda Larga 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 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 possível 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 prática 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 Banda Larga obteve **estrela cheia**, pois atendeu a ambos os parâmetros.

Quanto ao **parâmetro I**, referente à contestação de legislação, foi considerado atendido. Na fase de engajamento com as empresas, a empresa apresentou a ação, protocolada em conjunto com outras operadoras de telefonia, em que contesta a Lei nº 9.182/2021, do Estado do Rio de Janeiro. A referida legislação institui o alerta obrigatório de crianças e adolescentes desaparecidos pelas companhias de telefonia celular aos seus usuários e dá outras providências. Entre outros argumentos, as empresas afirmam que a lei viola o direito constitucional à privacidade e viola a Lei Geral de Proteção de Dados.

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 S/A E quebra E sigilo”; “TIM S/A E dados pessoais”; e “TIM S/A E privacidade”, e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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.

Nas buscas, foi encontrada no Tribunal de Justiça do Ceará a ação [nº 0830946-86.2014.8.06.0001](#), em que a empresa contesta a competência do Juízo Cível para a quebra do sigilo telefônico. Portanto, o parâmetro foi considerado atendido.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Civil Pública nº 0005292-42.2003.4.03.6110, que questiona, entre outros, a entrega de dados de portas lógicas às

autoridades policiais, e a Ação Direta de Inconstitucionalidade (ADI) 5642³⁶, da ACEL, não foram consideradas, já que não registraram movimentações.

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 sigilo 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 Banda Larga obteve **estrela cheia**, pois atendeu integralmente ao parâmetro I e parcialmente ao parâmetro II.

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.

Durante a fase de engajamento, a empresa enviou ao InternetLab algumas contribuições a consultas públicas. Destacamos aqui a contribuição individual da TIM à tomada de subsídios para regulamentação da aplicação da LGPD para microempresas e empresas de pequeno porte da ANPD, em que a TIM defende que “qualquer medida de flexibilização em favor de agentes econômicos de pequeno porte e/ou startups deve somente alcançar a posição de controlador, na forma definida no artigo 5º, inciso VI, da LGPD, não alcançando aquelas hipóteses em que o agente econômico integra a cadeia de tratamento de dados pessoais na condição de operador (cf. artigo 5º, inciso VII, da LGPD)”.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura

³⁶ 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.

e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial³⁷; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020³⁸; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética³⁹; entre outras.

Em fevereiro de 2021, durante a audiência pública realizada na Câmara dos Deputados sobre a implementação do 5G no Brasil, a empresa, por intermédio de seu vice-presidente de Relações Institucionais, defendeu a construção e financiamento de um centro de excelência de Segurança Brasileiro, com o objetivo de garantir a segurança das redes⁴⁰. Portanto, já que houve o posicionamento público da empresa, o parâmetro foi considerado atendido.

Ainda, em 2021, a TIM incluiu um novo documento em seu Portal de Privacidade, intitulado “Política de Segurança da Informação e Segurança Cibernética”, em que, entre outras coisas, disponibiliza um canal de comunicação específico para casos de segurança. Parabenizamos a empresa pela disponibilização de um documento específico em que informa, com detalhes, sobre práticas de segurança e meios de exercício de direitos.

No entanto, vale ressaltar que a Tim foi uma das empresas notificadas pelo Procon, no início de 2021, pelo suposto vazamento de dados de mais de 100 milhões de clientes. Em resposta, a empresa informou apenas:

“Não identificou a ocorrência de ataque ou vazamento que colocasse em vulnerabilidade dados de seus clientes ou dados próprios”⁴¹.

No entanto, não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. A resposta da empresa foi considerada excessivamente genérica. Contudo, nesta edição do relatório, as respostas relativas ao megavazamento não foram consideradas para fins de pontuação.

Nessa categoria, convidamos as empresas, nessa fase de envio e discussão dos resultados preliminares do relatório, a compartilharem conosco outros eventos públicos e participações relevantes que possam ser consideradas para essa categoria.

³⁷ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

³⁸ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

³⁹ TELESÍNTese. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

⁴⁰ TELESÍNTese. TIM propõe criação de centro de excelência de segurança no Brasil. 10 de fevereiro de 2021. Disponível em: <https://www.telesintese.com.br/tim-defende-centro-de-excelencia-de-seguranca-no-brasil/>

⁴¹ O VALOR. Oi e TIM dizem que não detectaram vazamentos de dados de clientes. 17 de fevereiro de 2021. Disponível em: <https://valor.globo.com/empresas/noticia/2021/02/17/oi-e-tim-dizem-que-no-detectaram-vazamentos-de-dados-de-clientes.html>

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

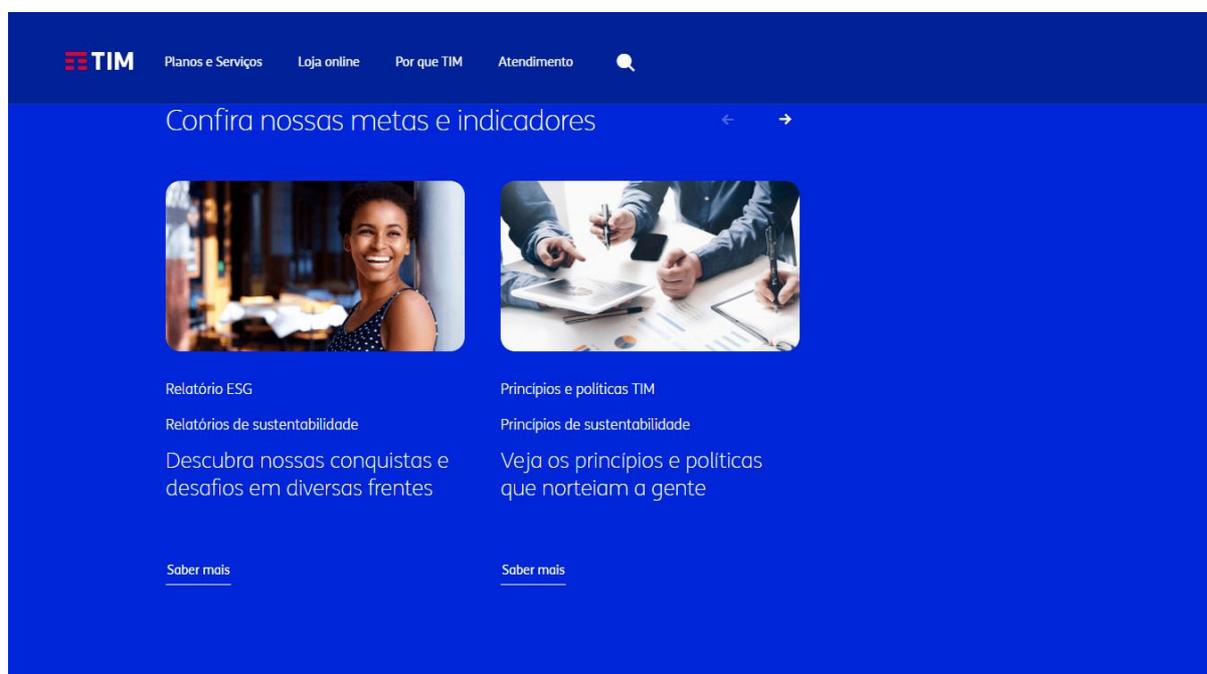
Resultado:



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



Captura de tela de 21.07.2021. Página de sustentabilidade da TIM⁴².

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.

⁴² <https://site.tim.com.br/sp/sobre-a-tim/sustentabilidade>

O **parâmetro IV**, relativo às informações sobre pedidos de acesso a dados, foi considerado atendido. Em seu relatório de transparência, a empresa informa (p. 54):

Em 2020, foram iniciadas 687 ações judiciais relacionadas à privacidade de dados e encerradas 5932, sendo 293 com decisões favoráveis. Nos 300 processos com decisões desfavoráveis à Companhia, houve o pagamento de cerca de R\$ 2 milhões.

No mesmo período, a TIM recebeu 114 ações judiciais relativas à quebra de sigilo telefônico ou telemático e 81 casos foram encerrados. As solicitações à TIM de quebra de privacidade por parte da Justiça, em 2020, somaram mais de 1 milhão conforme segue:

- Interceptações telefônicas: 427 mil
- Dados cadastrais: 391 mil
- Extratos telefônicos: 600

2) Número de clientes cujas informações foram solicitadas (número)

(2) Atualmente não é possível auferir com precisão o número de clientes afetados pelos pedidos de informações, uma vez que autoridades diferentes podem solicitar os mesmos dados em oportunidades diversas. [p. 93]

Vale notar, no entanto, que a redação acima, mesmo que aponte a quantidade de pedidos feitos, afirma que “não é possível auferir com precisão o número de clientes afetados pelos pedidos de informações”, contudo isso já foi feito por outras empresas.

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

TIM MÓVEL

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a TIM Móvel obteve **estrela cheia**, tendo atendido integralmente aos parâmetros I, IV e V; e parcialmente ao parâmetro II.

A Tim Móvel atende ao **parâmetro I**, referente às informações sobre coleta e finalidade, fornecendo informações claras e completas sobre todos os sub-parâmetros.

O *sub-parâmetro (a)*, referente a quais dados são coletados, foi considerado 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 |
|---|---|---|--------------------------------|
| 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 formato da tela, entre outras funções. | Legítimo Interesse |
| | | Obrigação Legal: cumprir com as obrigações legais de | Cumprimento de Obrigação Legal |

5

TIM

DATA DA ÚLTIMA ATUALIZAÇÃO: 12/08/2020.

| | | | |
|--|---|--|----------|
| | 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 melhorar sua experiência como usuário e atender as | | Legítimo |

Captura de tela: 20/07/2021

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; Informações sobre o uso dos Serviços: volume de tráfego na internet; Dados locais (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. Dados do Dispositivo de Acesso (excluindo páginas visitadas).

O *sub-parâmetro (b)*, referente às situações em que a coleta ocorre, foi igualmente considerado 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.

O *sub-parâmetro (c)*, referente à finalidade da coleta de dados, foi igualmente considerado atendido. No mesmo item referenciado acima, a empresa especifica a finalidade da coleta dos diversos dados que aponta. Especifica, por exemplo, as finalidades de “Funcionamento do Site: ativar funcionalidades essenciais, como software antivírus, adaptar o conteúdo ao formato da tela, entre outras funções”, “analytics: compreender o seu comportamento de navegação e como o Site e App está sendo usado, para melhorar sua experiência como usuário e atender as necessidades dos nossos clientes.”, “Marketing: direcionamento de conteúdos e publicidade, nossa e de nossos parceiros, conforme o seu perfil e preferências”, dentre outros.

Além disso, no Contrato de Prestação do Serviço Móvel Pessoal Pós-Pago, a empresa, na cláusula 11, estabelece:

11.1 As Partes reconhecem que, em razão do presente Contrato, a TIM realizará o tratamento de dados pessoais do CLIENTE na extensão necessária para garantir a adequada prestação do SMP e, em geral, na forma prevista ou de qualquer forma autorizada na legislação aplicável.

O *sub-parâmetro (d)*, referente à forma como se dá a utilização, foi igualmente considerado atendido. Ao especificar as finalidades para as quais trata dados pessoais, conforme item acima, a empresa mostra também exemplos de sua utilização. Por exemplo, ao apontar a finalidade de “marketing”, especifica que os dados serão utilizados para direcionar “conteúdos e publicidade”. Por mostrar situações de uso paralelamente às finalidades, o *sub-parâmetro* foi considerado atendido.

Por fim, o *sub-parâmetro (e)*, referente aos direitos dos titulares e meios para seu exercício, foi igualmente considerado atendido. Em sua Política de Privacidade, no item “Quais são os direitos dos Titulares de Dados”, a empresa apresenta tabela com os direitos e uma explicação de cada um deles, apontando, por exemplo, o “Direito de confirmar a existência de tratamento dos seus dados e de acessá-los”, o “direito de retificação”, “direito de exclusão”, “direito de oposição”, “direito de solicitar anonimização, bloqueio ou eliminação”, “direito à portabilidade”, dentre outros. Além disso, oferece os e-mails da área de Data Protection Officer (DPO) da TIM para exercício dos referidos direitos.

Além disso, no Contrato de Prestação do Serviço Móvel Pessoal Pós-Pago, a empresa, na cláusula 4, estabelece:

3.5. São assegurados ao CLIENTE os direitos estabelecidos na regulamentação do SMP e na legislação vigente, tais como:

f) inviolabilidade e sigilo de sua comunicação, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações e ressalvada a hipótese de disponibilização de informações, exclusivamente, para fins estatísticos.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, foi considerado cumprido, pois atende a todos os sub-parâmetros.

O *sub-parâmetro (a)*, referente ao tempo e onde os dados são armazenados, foi considerado cumprido. No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, a empresa detalha algumas prazos legais para manutenção de dados pessoais, bem como os critérios adotados para determinar o período de retenção adequado.

Prazo de Armazenamento

A TIM armazenará e tratará seus Dados Pessoais somente pelo tempo necessário para cumprir as finalidades da coleta, inclusive para fins de cumprimento de quaisquer obrigações legais, regulatórias, contratuais, de prestação de contas, requisição de autoridades competentes ou outras previstas na legislação vigente, como garantir os direitos dos titulares e seus próprios direitos.

Em geral, a título exemplificativo:

- Dados Pessoais cadastrais podem ser mantidos pelo prazo de 5 anos, tendo como referência o Código de Defesa do Consumidor, a contar do término da relação do titular com a TIM;
- Além disso, por obrigação constante no 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, quanto aos aplicativos da TIM, por no mínimo 6 meses;
- por atuar como prestadora de comunicações, de acordo com o estabelecido pela ANATEL, por meio da Resolução nº 738 de 2020, a TIM tem que manter registro dos dados de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada, pelo período de 5 anos.

Após o término dos prazos, os Dados Pessoais serão devidamente eliminados ou anonimizados pela TIM.

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

alcançar os propósitos almejados por outros meios, e os requisitos legais aplicáveis, dentre outros.

Não obstante o disposto acima, a política geral da TIM é que nenhum dado pessoal de clientes da TIM deve ficar armazenado por mais de 5 (cinco) anos a contar do término da relação comercial entre um cliente e a TIM. A exceção a essa regra são situações de cumprimento de uma ordem judicial ou administrativa competente (veja a nossa informativa sobre “Compartilhamento de Dados Pessoais em Caso de Investigação”). Lembrando que este é o período máximo, uma vez cumprida sua finalidade e desde que não haja qualquer obrigação legal ou legítimo interesse para sua manutenção por prazo superior.

Quanto ao local de armazenamento, a empresa informa em sua Política de Privacidade, no item “A TIM pode transferir seus Dados para outros países”:

A TIM poderá transferir dados para outros países para fins de armazenamento, por exemplo, em servidores localizados no exterior, com grau de proteção de dados adequado ao previsto nas legislações vigentes. Informamos que seus Dados poderão estar sujeitos à legislação local e às regras pertinentes destes países. Ao interagir conosco, Você concorda com essa transferência internacional de Dados, nos casos em que seja essencial para prestação dos serviços e execução do seu contrato conosco, de acordo com a legislação de proteção de dados.

No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, a empresa informa, com detalhes, os locais de armazenamento de dados pessoais.

Local de Armazenamento

Por fim, os dados armazenados pela TIM ou por fornecedores contratados seguem níveis rígidos e adequados de segurança da informação e consistentes com as práticas do mercado, sempre buscando atender a Lei Geral de Proteção de Dados Pessoais e demais legislações aplicáveis e vigentes. No geral, os dados pessoais são armazenados:

- (i) em servidores de propriedade da TIM, localizados nos estados de São Paulo e Rio de Janeiro;
- (ii) em servidores de terceiros, contratados pela TIM especificamente para serviços de armazenamento de dados (hosting), seguindo controles contratuais para garantir o cumprimento, a Lei Geral de Proteção de Dados; ou
- (iii) em servidores de terceiros, contratados pela TIM para realizar algum serviço específico temporário e que inclui algum tipo de tratamento de dados (por exemplo, uma verificação de fraude). Nesses casos, além dos controles contratuais, limitamos o tratamento ao mínimo necessário e pelo menor tempo possível (por exemplo, em algumas situações o dado é excluído após poucas horas)

Tais informações foram consideradas suficientes para esclarecer ao usuários sobre as práticas adotadas pela empresa para a retenção de dados pessoais.

Quanto ao *sub-parâmetro (b)*, referente a quando/se os dados são apagados, foi considerado cumprido. No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, na seção Prazo de Armazenamento (vide trecho acima), a empresa informa expressamente que, findo os prazos que autorizam a retenção, a TIM deleta ou anonimiza os dados pessoais.

O *sub-parâmetro (c)*, referente às práticas de segurança que a empresa observa, foi considerado atendido. Em seu Relatório de Sustentabilidade 2020, p. 36, 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.

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.

Por esclarecer a norma de segurança utilizada para proteger seus sistemas, e ao prestar algumas informações em relação aos colaboradores e fornecedores que têm acesso aos dados, considerou-se que as informações dadas eram suficientes.

O *sub-parâmetro (d)*, referente a quem tem acesso aos dados, também foi considerado 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.

O *sub-parâmetro (e)*, referente aos terceiros com quem os dados são compartilhados, foi considerado atendido. Em sua Política de Privacidade, no item “Com quem a TIM compartilha os seus Dados”, a

empresa específica 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. Ao fazermos isso, nós não precisamos revelar a sua identidade aos nossos parceiros, ou seja, não compartilhamos seus dados com eles nessas situações.

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

A TIM, assim como qualquer grande organização, opera em parceria com uma série de outras empresas que dão suporte no oferecimento de produtos e serviços TIM. Em alguns casos, para que essas empresas possam nos atender e dar o suporte de que precisamos, pode ser necessário compartilhar certos dados pessoais dos nossos clientes com essas empresas. Nossos parceiros e fornecedores somente são autorizados a utilizar os dados pessoais recebidos para os fins específicos para o qual foram contratados, portanto, eles não irão utilizar os seus dados pessoais para outras finalidades, além da prestação de serviços prevista contratualmente. A TIM executa procedimentos preparatórios à contratação de novos parceiros e fornecedores para garantir que, na hipótese em que seja necessário compartilhar dados pessoais com tais empresas, obrigações contratuais de segurança da informação e de proteção de dados pessoais sejam estabelecidas para proteger os dados de nossos clientes.

Tais informações foram consideradas suficientes para informar sobre o compartilhamento.

Quanto ao *sub-parâmetro (f)*, relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi 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.”

Quanto ao *sub-parâmetro (g)*, referente às hipóteses de transferência internacional de dados, foi considerado atendido. Em sua Política de Privacidade, a empresa informa que a TIM poderá transferir dados para outros países.

A TIM poderá transferir dados para outros países para fins de armazenamento, por exemplo, em servidores localizados no exterior, com grau de proteção de dados adequado ao previsto nas legislações vigentes. Informamos que seus Dados poderão estar sujeitos à legislação local e às regras pertinentes destes países. Ao interagir conosco, Você concorda com essa transferência internacional de Dados, nos casos em que seja essencial para prestação dos serviços e execução do seu contrato conosco, de acordo com a legislação de proteção de dados.

No documento “Onde e por Quanto tempo a TIM armazena os seus dados”, a empresa informa de forma detalhada sobre as práticas de transferência internacional e informa os principais países em os dados são armazenados:

Transferências Internacionais

Ao utilizar os serviços de internet da TIM, é possível que o usuário acesse aplicações de terceiros, cujos servidores estão localizados em outros países, e podem capturar as informações de IP e hora de acesso. Isso faz parte da natureza dos serviços de conexão à internet, e é importante que o usuário sempre adote as melhores práticas de segurança quando navega na internet. Além disso, a TIM pode ativamente realizar a transferência internacional de dados pessoais que estão sob seu controle sempre que contratarmos servidores de terceiros, conforme os itens (i) e (ii) acima. Por se tratarem de serviços “cloud”, esses fornecedores podem a todo momento alterar a localização da hospedagem, mas buscamos limitar contratualmente que essas transferências sejam feitas com segurança e para países quem possuem leis que garantem adequadamente a proteção e segurança dos dados pessoais. Não obstante, os principais servidores de terceiros que armazenam dados pessoais sob controle da TIM estão localizados nos seguintes países, além do Brasil:

- AEE (Área Econômica Europeia);
- Califórnia (EUA).

Ainda, quando armazenado em outra localidade, esta é previamente validada e aprovada pelas funções responsáveis.

Tais informações foram consideradas suficientes para fins desta avaliação.

Por fim, quanto ao *sub-parâmetro (h)*, sobre a data da última atualização da política de privacidade, foi considerada atendida. Tanto a Política de Privacidade quanto os contratos contam com a data da última atualização (com exceção do Contrato de prestação de serviço SMP Corporativo, que não tem data de registro).

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendida. O InternetLab realizou um pedido de acesso a dados em 21 de julho de 2021. Em resposta, a TIM informou:

TIM, em conformidade com as disposições legais aplicáveis, deve identificar o solicitante e verificar a existência dos requisitos de legitimidade para atender às solicitações.

Sendo assim, pedimos a gentileza de nos enviar sua solicitação novamente, desta vez acompanhada de documentação necessária (ex.: cópia de um documento de identidade válido), para que possamos fornecer um feedback.

Essa solicitação também visa proteger os titulares da comunicação indevida de seus dados pessoais a terceiros não autorizados.

Atenciosamente,

Data Protection Officer

Após o envio da documentação solicitada pela empresa, a TIM informou, por email, os dados pessoais que possuía sobre o titular, bem como um arquivo Word com as telas comprobatórias dos sistemas em que constam tais dados. Consideramos positiva a exigência de comprovação da titularidade para concessão do acesso aos dados. Por isso, o parâmetro foi considerado atendida.

O **parâmetro IV**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, foi considerado atendida. 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 V**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado atendido. A empresa tem um Portal de Privacidade⁴³ com as principais informações de privacidade e proteção de dados. Ainda, a empresa disponibilizou Informativos de Privacidade, em que traz informações detalhadas sobre práticas de privacidade e proteção de dados da empresa.



Protegemos seus dados e somos transparentes sobre o uso deles

Sobre a TIM >

O nosso compromisso com Proteção de Dados

Relatório - InternetLab

Projeto de Adequação

Principais ações executadas durante o Projeto de Adequação

Direitos dos Titulares

Sobre a TIM

A TIM S.A. é uma das maiores empresas de telecomunicação do Brasil, além de fazer parte de um grupo multinacional com presença local há mais de 20 anos.

Somos a primeira operadora a ter presença nacional. Com a inovação em nosso DNA, buscamos sempre potencializar a vida de nossos clientes através da tecnologia. Para isso, além de trabalhar na ampliação e melhoria da rede, apostamos em um portfólio completo com telefonia móvel, fixa e internet. Assim, nossos clientes individuais e corporativos estarão sempre conectados.

A transparência é um de nossos pilares. Somos a única empresa do setor de telecomunicações no Novo Mercado da BM&FBOVESPA, reconhecido como nível máximo de governança corporativa. Também fazemos parte do Índice de Sustentabilidade Empresarial (ISE) e do Índice de Carbono Eficiente (ICO2).

Como outro destaque, temos o selo [Data Aberto](#), no qual consumidores

Captura de tela: 08/10/2021.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ★

Nesta categoria, a Tim Móvel 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 Contrato de Prestação do Serviço Móvel Pessoal Pós-Pago, a empresa, na cláusula 4, estabelece:

3.5. São assegurados ao CLIENTE os direitos estabelecidos na regulamentação do SMP e na legislação vigente, tais como:

⁴³ <https://www.tim.com.br/sp/sobre-a-tim/institucional/seguranca/politica-de-privacidade>

f) inviolabilidade e sigilo de sua comunicação, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações e ressalvada a hipótese de disponibilização de informações, exclusivamente, para fins estatísticos.

No Contrato de Prestação de Serviço SMP Corporativo LA , a empresa informa:

14.10. A TIM dispensará tratamento sigiloso e confidencial aos dados e comunicações do CLIENTE, podendo disponibilizá-los em caso de determinação de autoridade competente.

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 possível 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

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 Móvel obteve **estrela cheia**, pois atendeu a ambos os parâmetros.

O **parâmetro I**, referente à contestação de legislação, foi considerado atendido. Na fase de engajamento com as empresas, a empresa apresentou a ação, protocolada em conjunto com outras operadoras de telefonia, em que contesta a Lei nº 9.182/2021, do Estado do Rio de Janeiro. A referida legislação institui o alerta obrigatório de crianças e adolescentes desaparecidos pelas companhias de telefonia celular aos seus usuários e dá outras providências. Entre outros argumentos, as empresas afirmam que a lei viola o direito constitucional à privacidade e viola a Lei Geral de Proteção de Dados.

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 S/A E quebra E sigilo”; “TIM S/A E dados pessoais”; e “TIM S/A E privacidade”, e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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.

Nas buscas, foi encontrada no Tribunal de Justiça do Ceará a ação [nº 0830946-86.2014.8.06.0001](#), em que a empresa contesta a competência do Juízo Cível para a quebra do sigilo telefônico. Portanto, o parâmetro foi considerado atendido.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Civil Pública nº 0005292-42.2003.4.03.6110, que questiona, entre outros, a entrega de dados de portas lógicas às autoridades policiais, e a Ação Direta de Inconstitucionalidade (ADI) 5642⁴⁴, da ACEL, não foram consideradas, já que não registraram movimentações.

CATEGORIA 4: Postura pública pró-privacidade

Resultado:

Nesta categoria, a TIM Móvel obteve **estrela cheia**, pois atendeu integralmente ao parâmetro I e parcialmente ao parâmetro II.

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.

Durante a fase de engajamento, a empresa enviou ao InternetLab algumas contribuições a consultas públicas. Destacamos aqui a contribuição individual da TIM à tomada de subsídios para regulamentação da aplicação da LGPD para microempresas e empresas de pequeno porte da ANPD, em que a TIM defende que “qualquer medida de flexibilização em favor de agentes econômicos de pequeno porte e/ou startups deve somente alcançar a posição de controlador, na forma definida no artigo 5º, inciso VI, da LGPD, não alcançando aquelas hipóteses em que o agente econômico integra a cadeia de tratamento de dados pessoais na condição de operador (cf. artigo 5º, inciso VII, da LGPD)”.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de

⁴⁴ 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.

seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial⁴⁵; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020⁴⁶; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética⁴⁷; entre outras.

Em fevereiro de 2021, durante a audiência pública realizada na Câmara dos Deputados sobre a implementação do 5G no Brasil, a empresa, por intermédio de seu vice-presidente de Relações Institucionais, defendeu a construção e financiamento de um centro de excelência de Segurança Brasileiro, com o objetivo de garantir a segurança das redes⁴⁸. Portanto, já que houve o posicionamento público da empresa, o parâmetro foi considerado atendido.

Ainda, em 2021, a TIM incluiu um novo documento em seu Portal de Privacidade, intitulado “Política de Segurança da Informação e Segurança Cibernética”, em que, entre outras coisas, disponibiliza um canal de comunicação específico para casos de segurança. Parabenizamos a empresa pela disponibilização de um documento específico em que informa, com detalhes, sobre práticas de segurança e meios de exercício de direitos.

No entanto, vale ressaltar que a Tim foi uma das empresas notificadas pelo Procon, no início de 2021, pelo suposto vazamento de dados de mais de 100 milhões de clientes. Em resposta, a empresa informou apenas:

“Não identificou a ocorrência de ataque ou vazamento que colocasse em vulnerabilidade dados de seus clientes ou dados próprios”⁴⁹.

No entanto, não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. A resposta da empresa foi considerada excessivamente genérica. Contudo, nesta edição do relatório, as respostas relativas ao megavazamento não foram consideradas para fins de pontuação.

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

⁴⁵ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.anatel.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

⁴⁶ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

⁴⁷ TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

⁴⁸ TELESÍNTESE. TIM propõe criação de centro de excelência de segurança no Brasil. 10 de fevereiro de 2021. Disponível em: <https://www.telesintese.com.br/tim-defende-centro-de-excelencia-de-seguranca-no-brasil/>.

⁴⁹ O VALOR. Oi e TIM dizem que não detectaram vazamentos de dados de clientes. 17 de fevereiro de 2021. Disponível em: <https://valor.globo.com/empresas/noticia/2021/02/17/oi-e-tim-dizem-que-no-detectaram-vazamentos-de-dados-de-clientes.ghtml>

Resultado: ★

Nesta categoria, a TIM Móvel obteve **três quartos de estrela**, pois atendeu aos parâmetros I, II, III e 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”.



Captura de tela de 21.07.2021. Página de sustentabilidade da TIM⁵⁰.

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 atendido. Em seu relatório de transparência, a empresa informa (p. 54):

Em 2020, foram iniciadas 687 ações judiciais relacionadas à privacidade de dados e encerradas 5932, sendo 293 com decisões favoráveis. Nos 300

⁵⁰ <https://site.tim.com.br/sp/sobre-a-tim/sustentabilidade>

processos com decisões desfavoráveis à Companhia, houve o pagamento de cerca de R\$ 2 milhões.

No mesmo período, a TIM recebeu 114 ações judiciais relativas à quebra de sigilo telefônico ou telemático e 81 casos foram encerrados. As solicitações à TIM de quebra de privacidade por parte da Justiça, em 2020, somaram mais de 1 milhão conforme segue³ :

- Interceptações telefônicas: 427 mil
- Dados cadastrais: 391 mil
- Extratos telefônicos: 600

2) Número de clientes cujas informações foram solicitadas (número)

(2) Atualmente não é possível auferir com precisão o número de clientes afetados pelos pedidos de informações, uma vez que autoridades diferentes podem solicitar os mesmos dados em oportunidades diversas. [p. 93]

Vale notar, no entanto, que a redação acima, mesmo que aponte a quantidade de pedidos feitos, afirma que “não é possível auferir com precisão o número de clientes afetados pelos pedidos de informações”, contudo isso já foi feito por outras empresas.

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

VIVO BANDA LARGA

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Vivo Banda Larga obteve **estrela cheia**, tendo atendido aos parâmetros I, II e III, e parcialmente ao parâmetro V.

Embora os contratos de telefonia banda larga ofereçam poucas informações sobre as práticas de tratamentos de dados da empresa, constatamos que a maior parte das informações 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.

O sub-parâmetro (a), referente aos dados coletados, foi considerado cumprido. 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 e por meio da sua interação e uso dos canais de informação. Entenda melhor quais informações coletamos:

Dados cadastrais, como por exemplo, 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 23.07.2021

As mesmas informações são repetidas na Política de Privacidade Local da Vivo. Ainda, no Contrato de Adesão de Prestação do Serviço de Telefônico Fixo Comutado, a empresa informa (cláusula 13) sobre a coleta de registros de conexão, nome, dentre outros dados.

O sub-parâmetro (b), referente às situações em que a coleta ocorre, também foi considerado cumprido. Isso porque, mesmo que não haja redação específica para apontar situações onde os dados são coletados, 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 quando se contrata os serviços, por meio da interação com canais de informação, dentre outros. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

O sub-parâmetro (c), referente à finalidade do tratamento de dados, também foi considerado cumprido. No Centro de Privacidade, em “Para que coletamos” a empresa descreve algumas das finalidades, 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 23.07.2021

Ademais, nas cláusulas 5.3 e 13.1 do Contrato de Adesão, a empresa explicita as finalidades da coleta de dados, como seu uso para envio de e-mails, malas diretas, prestação de serviços ou para finalidades de marketing.

5.3 O CLIENTE tem a opção de autorizar ou não a VIVO a enviar-lhe, e-mails, malas diretas, encartes ou qualquer outro instrumento de comunicação ofertando serviços e/ou produtos da VIVO ou empresas a esta relacionada ou parceiras, bem como fornecer a estas os dados cadastrais/pessoais fornecidos para a presente contratação, para a oferta de seus produtos e/ou serviços. Tais permissões podem ser revogadas pelo CLIENTE, a qualquer momento, por meio de solicitação feita à Central de Relacionamento com o CLIENTE.

13.1. Os dados pessoais do CLIENTE recolhidos pela VIVO no âmbito deste Contrato serão tratados na forma da legislação vigente e regulamentação aplicável, exclusivamente com o objetivo de prestação do(s) serviço(s) de telecomunicação (ões) objeto deste Contrato, bem como para análise de perfil do CLIENTE, ou para finalidades de marketing, por forma a (i) garantir a adequação das melhores ofertas de acordo com as necessidades do CLIENTE; e (ii) melhorar a performance dos serviços prestados, podendo ainda os mesmos ser tratados pela VIVO, seus parceiros ou por terceiros por contratados pela VIVO, de forma anonimizada de modo a permitir análise e construção de padrões, comportamentos, escolhas, e consumos para as finalidades aqui previstas.

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. Isso porque fornece indiretamente informações sobre a forma de utilização 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.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercícios desses direitos, também foi considerado atendido. No Centro de Privacidade, em “Exercício dos Direitos”, a empresa lista alguns direitos dos titulares sobre seus dados. Por mais que outros direitos poderiam ter sido mencionados, como o direito à portabilidade e o de revisão de decisão automatizadas, a redação apresentada foi considerada satisfatória. 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.

Deve-se ressaltar que, especificamente quanto ao direito de exclusão dos dados pessoais, a empresa simplesmente afirma “manter os dados pelo tempo necessário” previsto em lei, encaminhando o usuário para a sua Política de Privacidade caso queira saber sobre os “períodos de armazenamento”. A redação dá a entender que o direito de exclusão não pode ser exercido. Idealmente, a empresa deveria ter especificado quais dados podem ser excluídos e quais não, assim como a razão para tal distinção.

O Contrato de Adesão também traz previsões acerca dos direitos dos titulares. A cláusula 5.3, reproduzida acima, garante ao cliente a possibilidade de revogar, a qualquer momento, as permissões concedidas por meio de solicitação no Central de Relacionamento com o Cliente. Ainda, na cláusula 5.1.8., a empresa elenca como direito do cliente a “resposta eficiente e tempestiva pela VIVO às suas reclamações, solicitações de serviços e pedidos de informação”.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, considerou-se, na média, que foi atendido, tendo sido os sub-parâmetros (c) e (d) considerados atendidos, os sub-parâmetros (a), (b), (e), (f), (g) parcialmente atendidos e o parâmetro (h) não atendido.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado parcialmente cumprido. No Centro de Privacidade, em “Tratamento dos Dados” e “Armazenamento dos Dados”, a empresa informa:

Armazenamento dos dados

A Vivo armazena os seus dados durante o relacionamento com você e conforme as finalidades para as quais foram coletados. Além disso, seus dados são mantidos pelo tempo necessário, para cumprimento de obrigações legais e regulatórias, como em caso de ordens judiciais e solicitações de autoridades competentes, sempre em conformidade com a legislação vigente.

Dados como seus registros de conexão (tempo de conexão e IP) são armazenados pelo período mínimo de 1 ano. Registramos conteúdo de provedores de aplicativos, somente daqueles que criamos. Nesse caso, mantemos o registro por no mínimo 6 meses em ambiente controlado e seguro, de acordo com Marco Civil da Internet.

Os seus dados cadastrais (como por exemplo nome completo, endereço, CPF) e os dados de faturamento (documentos fiscais) são armazenados por no mínimo 5 anos, para processos administrativos e judiciais.

Ainda, no Contrato de Adesão, a empresa informa que os dados pessoais são armazenados por 5 anos e que os contratos são mantidos por 10 anos.

13.2 Os dados pessoais do CLIENTE recolhidos pela VIVO no âmbito deste Contrato serão armazenados pela VIVO ou por um terceiro subcontratado pela VIVO pelo prazo de 5 (cinco) anos, sendo os Contratos armazenados pelo prazo de 10 (dez) anos, por forma a garantir o cumprimento das correspondentes obrigações legais aplicáveis, sendo garantido aos CLIENTES que o armazenamento dos seus dados pessoais pela VIVO ou por terceiros subcontratados será efetuada mediante a adoção de medidas de segurança e proteção física e lógica das informações.

As informações sobre tempo de armazenamento foram consideradas satisfatórias, pois são apresentados os prazos de armazenamento detalhados para cada tipo de dado coletado, especificando-se, ainda, quais os prazos máximos de armazenamento. Quanto ao local de armazenamento, a empresa informa, na sua Política de Privacidade da Telefônica:

- A informação é preferencialmente tratada internamente na Telefônica Vivo ou em empresas do Grupo Telefônica, respeitando sempre a legislação vigente do Brasil.
- Em alguns casos a informação pode ser compartilhada com empresas parceiras, das quais são exigidos controles de segurança para proteção das informações.

Considerou-se a redação do trecho acima, por ser excessivamente ampla, insatisfatória. Mesmo que a empresa informe que “a informação é preferencialmente tratada internamente”, não são esclarecidas as hipóteses em que os dados são tratados externamente, quais os países onde são armazenados, quais tipos de dados são armazenados em cada local, dentre outras informações relevantes que poderiam ter sido fornecidas.

O sub-parâmetro (b), referente a quando/se os dados são apagados, considerou-se parcialmente atendido. Isso porque, no mesmo trecho apontado acima, em “Armazenamento dos Dados” no Centro de Privacidade, infere-se que os dados são apagados após o decurso do prazo apontado, mas não há esclarecimento se isso efetivamente ocorre.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, foi considerado atendido. No Relatório de Sustentabilidade de 2020 da empresa (p. 41), a empresa informa alguns dos padrões de segurança que utiliza para garantir a proteção dos usuários, afirmando ter desenvolvido, “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 da Informação”, 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.

O sub-parâmetro (d), referente a quem tem acesso aos dados, também foi considerado atendido, já que a empresa, vide parágrafo acima, afirma que somente pessoas autorizadas, conforme o 'princípio do privilégio mínimo', podem ter acesso aos dados. Mesmo que informações mais detalhadas sobre quais funcionários podem acessar os dados poderiam ter sido fornecidas, a menção ao princípio do privilégio mínimo indica para a existência de padrões mais claros em relação a tais acessos, razão pela qual o sub-parâmetro foi considerado cumprido.

O sub-parâmetro (e), referente aos terceiros com quem os dados são compartilhados, foi considerado parcialmente atendido. A Vivo, no Centro de Privacidade, em "Compartilhamento de Informações", na cláusula 13.4, 13.5 e 13.7 do Contrato de Adesão, e na Cláusula 5 de sua Política de Privacidade Local, a empresa elenca algumas hipóteses de fornecimento de dados a terceiros:

Compartilhamento de informações

Sua informação poderá ser compartilhada para garantir por exemplo, a prestação de serviços contratados por você e em atendimento de obrigações legais e regulatórias. Os dados poderão ser compartilhados com fornecedores, parceiros, empresas do grupo e autoridades, na medida necessária, sempre respeitando a legislação vigente. Mas fique tranquilo, o compartilhamento se dará através da adoção de medidas adequadas, visando a integridade e confidencialidade das informações.

A Vivo pode apoiar estudo de comportamento em eventos que promovam deslocamento de um público em determinada localização ou para determinada situação. Nesse caso, é importante ressaltar que não é possível qualquer forma de individualização dessas informações, que são tratadas de forma agregada.

captura de tela de 23.07.2021

Contrato de Adesão:

13.7 Salvo o disposto nos itens anteriores, não haverá o fornecimento a terceiros de demais dados pessoais, inclusive registros de conexão, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei identificadas na cláusula 13.4 e 13.5 deste Contrato.

As informações acima, mesmo que ofereçam algum guia para quais terceiros têm acesso aos dados, são excessivamente abrangentes. Não determinam quais terceiros podem recebê-los, não traz exemplos de situações em que possa ter havido autorização expressa do usuário, não tendo sido encontrados casos de tais autorizações nos documentos analisados e não determina quais dados e em quais situações são compartilhados. No entanto, por haver preocupação em apontar informações sobre o tema, com um mínimo de detalhamento, o sub-parâmetro foi considerado parcialmente atendido.

O sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi parcialmente atendido. Isso porque as informações trazidas sobre o tema, referenciadas na análise do sub-parâmetro (e) acima, assim como em redação bastante similar na Cláusula 5 de sua Política de Privacidade local, são pouco claras e afirmam somente de forma genérica que os dados podem ser compartilhados "para garantir, por exemplo, a prestação dos serviços contratados por você". 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.

O sub-parâmetro (g), referente às hipóteses de transferência internacional de dados, foi considerado parcialmente atendido. Em seu centro de privacidade, assim como em redação bastante similar na Cláusula 6 de sua Política de Privacidade local, a empresa informa:

Transferência internacional

A Vivo, como parte do Grupo Telefónica pode, em algumas circunstâncias e quando necessário, compartilhar dados pessoais para outras empresas do Grupo. Além disso, seus dados podem ser compartilhados com parceiros e fornecedores com sede em outros países, sempre em conformidade com a legislação aplicável e de acordo com as cláusulas contratuais.

captura de tela de 23.07.2021

As informações acima não esclarecem as hipóteses e situações em que os dados podem ser enviados para fora do país de maneira clara ou exaustiva. No entanto, por haver preocupação em apontar informações sobre o tema, com um mínimo de detalhamento, o sub-parâmetro foi considerado parcialmente atendido.

Por fim, o sub-parâmetro (h), referente à data da última atualização da política de privacidade, não foi atendido. Não há referências a alterações no Centro de Privacidade da Vivo, onde a maior parte das informações sobre privacidade são apresentadas. Além disso, 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”.

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. O InternetLab realizou um pedido de acesso a dados em 21 de julho de 2021 por meio do portal da privacidade da empresa, que, no entanto, resultou em uma mensagem de erro. Após contato com o DPO da empresa, o erro foi corrigido e informações cadastrais do titular puderam ser acessadas por meio do portal.

O **parâmetro IV**, 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, 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 V**, 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:

Centro de Transparência e Privacidade da Vivo

Encontre de forma fácil alguns dos temas importantes que estão em nosso Centro de Transparência



Políticas de Privacidade

Você encontra informações detalhadas sobre o tratamento dos seus dados

[Ver mais](#)



Segurança

Como protegemos as informações fornecidas por você

[Ver mais](#)



Tratamento de Dados

Entenda as finalidades e quais informações coletamos

[Ver mais](#)



captura de tela de 23.07.2021

No entanto, a maior parte de tais informações não são apresentadas nos contratos de internet banda larga da empresa, prática que seria recomendável para que as informações 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 Banda Larga obteve **estrela cheia**, tendo cumprido os parâmetros I, II e V, parcialmente o parâmetro IV e não atendido o III.

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado cumprido. Na página 22 do *Informe de Transparencia en las Comunicaciones 2021* da Telefônica, 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”:

“Intercepción 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 (Ministerio Público) o Comisario de Policía (Autoridad 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.

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

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

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, foi considerado parcialmente cumprido. 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**, relativo à existência de protocolos específicos sobre entrega de dados ao estado, foi considerado atendido. Este ano, 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”. O InternetLab enaltece a criação dessa nova seção, em nosso conhecimento, pouco usual na indústria.



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 receberemos 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.

captura de tela de 23.07.2021

O InternetLab enaltece ainda 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 para que a empresa seja pontuada sem ressalvas, seja em contratos, no Relatório de Sustentabilidade, ou outros materiais.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

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

O **parâmetro I**, referente à contestação de legislação, foi considerado atendido. Na fase de engajamento com as empresas, a empresa apresentou algumas ações nesse sentido. Por exemplo, mencionamos uma ação, protocolada em conjunto com outras operadoras de telefonia, em que se contestam alterações ao Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações - RGC que obrigariam as empresas a fornecerem, a qualquer destinatário de ligações telefônicas, dados pessoais da pessoa que fez a ligação (Ação rescisória no 0802518-50.2020.4.05.0000).

Por fim, o **parâmetro II** foi igualmente considerado atendido. Na fase de engajamento com as empresas, a Vivo apresentou ao InternetLab, com informações sensíveis tarjadas, diversas respostas a ofícios administrativos em que se negou a fornecer dados pessoais a autoridades públicas. Por exemplo, há situações em que negou a entrega de Histórico de Chamadas e Localização de ERBs ao Ministério Público e às Autoridades Policiais, sob a justificativa de ausência da observação do princípio da reserva constitucional de jurisdição.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Civil Pública nº 0005292-42.2003.4.03.6110, que questiona, entre outros, a entrega de dados de portas lógicas às autoridades policiais, e a Ação Direta de Inconstitucionalidade (ADI) 5642⁵¹, da ACEL, não foram consideradas, já que não registraram movimentações.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Vivo Banda Larga obteve **meia estrela**, pois atendeu ao parâmetro I.

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

⁵¹ 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.

oportunidade de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários.

Durante a fase de engajamento com as empresas, a Vivo nos forneceu exemplos de situações nesse sentido. Por exemplo, em artigo de opinião, publicado no portal Poder 360 em setembro de 2021 por Breno Oliveira, diretor jurídico da Telefônica Brasil, defendem-se algumas técnicas de privacidade e formas de se realizar a implementação da LGPD de maneira “bem-sucedida”⁵².

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, não foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere a aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial⁵³; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020⁵⁴; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética⁵⁵; entre outras.

Durante a fase de engajamento, a empresa nos forneceu cópia de suas contribuições à Consulta Pública nº 24 da Anatel, em que defende, principalmente, ampliação do diálogo e da participação do setor privado nas temáticas desenvolvidas pelas CBCs. No entanto, não há, nessa consulta, qualquer menção a técnicas de segurança.

Vale ressaltar que a Vivo sofreu em 2020 um suposto ataque cibernético a seu aplicativo, em que foram vazados diversos dados de clientes⁵⁶, sendo inclusive que chegou a ser processada pelo coletivo Intervezes para obtenção de maiores informações e notificada pela Anatel e pelo Procon⁵⁷. Na fase de engajamento, a empresa nos apresentou as respostas públicas apresentadas ao SENACON quanto ao caso, em que afirma ter avaliado seus sistemas internos e não ter averiguado qualquer incidente de segurança. No entanto, não há menções a melhorias em técnicas de segurança.

Por fim, em geral, perante a mídia, a empresa negou-se a comentar o suposto vazamento e afirmou que “o número de clientes possivelmente impactados por esta ação ilícita é consideravelmente menor do que o divulgado por alguns órgãos da imprensa especializada”⁵⁸. Não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. A resposta da empresa foi considerada excessivamente genérica. Contudo, nesta

⁵² <https://www.poder360.com.br/opiniaio/tecnologia/relatorio-de-conformidade-e-chave-para-adequacao-a-igpd-escreve-breno-oliveira>

⁵³ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

⁵⁴ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

⁵⁵ TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

⁵⁶ <https://tecnoblog.net/320931/vivo-acao-judicial-expor-dados-pessoais-clientes-meu-vivo/>

⁵⁷ <https://tecnoblog.net/313892/anatel-procon-sp-notificam-vivo-dados-expostos-clientes/>

⁵⁸ <https://g1.globo.com/economia/noticia/2021/02/18/operadoras-dizem-que-nao-detectaram-vazamentos-de-dados-de-clientes.ghtml>

edição do relatório, as respostas relativas a tais vazamentos não foram consideradas para fins de pontuação.

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

Resultado: 

Nesta categoria, a Vivo Banda Larga obteve $\frac{3}{4}$ de estrela, pois atendeu aos parâmetros I, II e III e parcialmente ao parâmetro IV.

O **parâmetro I**, relativo à publicação de relatórios de transparência em português, foi considerado atendido. Pelo quinto ano seguido, encontramos a publicação do *Informe de Transparencia en las Comunicaciones de 2021*, do Grupo Telefônica (documento em espanhol), em que há certo detalhamento sobre o conjunto regulatório em cada país no qual o grupo está presente. Além disso, o Relatório de Sustentabilidade 2020 da Vivo, em português, contém informações sobre privacidade e proteção de dados, apontando alguns requisitos de segurança utilizados, princípios da empresa sobre o assunto, alguns links relevantes, dentre outros. Durante a fase de engajamento, a empresa nos mostrou que seu Informe de Transparência havia sido traduzido ao português e publicado em seu centro de privacidade, razão pela qual o parâmetro foi considerado atendido.

O **parâmetro II**, relativo à acessibilidade do relatório de transparência, foi considerado atendido. Isso porque tanto o Relatório de Sustentabilidade quanto o Informe de Transparência em português podem ser encontrados na página principal do centro de privacidade da Vivo.

O **parâmetro III**, relativo à periodicidade do relatório, foi considerado atendido. Nas páginas de ambos 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. No *Informe de Transparencia en las Comunicaciones* (pp. 22 e 23), informa-se que, em 2020, foram feitos 363.125 requerimentos de interceptação e 2.550.060 requerimentos de acesso a metadados. No entanto, em ambos os casos, afirma-se que 0 (zero) pedidos foram rechaçados. Durante a fase de engajamento, a empresa nos esclareceu que um “pedido rechaçado” consistiria em não se ter respondido determinado ofício enviado por uma autoridade pública. A empresa considera que um ofício pedindo acesso a dados pessoais cuja resposta foi negativa, por ter sido respondido, não foi “rechaçado”. Assim, a empresa efetivamente informa, em seu relatório, que respondeu a todos os ofícios. No entanto, buscando maior transparência perante os usuários, seria necessário que houvesse a informação de quantos pedidos foram *negados*, i.e., quantas vezes se considerou que determinado ofício era ilegal, excessivamente genérico etc. Por essa razão, o parâmetro foi considerado parcialmente atendido.

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

VIVO MÓVEL

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Vivo Móvel obteve **estrela cheia**, tendo atendido aos parâmetros I, II e III, e parcialmente ao parâmetro V.

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.

O sub-parâmetro (a), referente aos dados coletados, foi considerado cumprido. 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 contratados por você. Sendo assim, coletamos os dados que você disponibilizou quando contratou os nossos serviços e por meio da sua interação e uso dos canais de informação. Entenda melhor quais informações coletamos:

Dados cadastrais, como por exemplo, 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 23.07.2021

As mesmas informações são repetidas na Política de Privacidade Local da Vivo.

O sub-parâmetro (b), referente às situações em que a coleta ocorre, também foi considerado cumprido. Isso porque, mesmo que não haja redação específica para apontar situações onde os dados são coletados, 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 quando se contrata os serviços, por meio da interação com canais de informação, dentre outros. Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

O sub-parâmetro (c), referente à finalidade do tratamento de dados, também foi considerado cumprido. No Centro de Privacidade, em “Para que coletamos” a empresa descreve algumas das finalidades, 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 23.07.2021

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. Isso porque fornece indiretamente informações sobre a forma de utilização 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.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercícios desses direitos, também foi considerado atendido. No Centro de Privacidade, em “Exercício dos Direitos”, a empresa lista alguns direitos dos titulares sobre seus dados. Por mais que outros direitos poderiam ter sido mencionados, como o direito à portabilidade e o de revisão de decisão automatizadas, a redação apresentada foi considerada satisfatória. 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.

Deve-se ressaltar que, especificamente quanto ao direito de exclusão dos dados pessoais, a empresa simplesmente afirma “manter os dados pelo tempo necessário” previsto em lei, encaminhando o usuário para a sua Política de Privacidade caso queira saber sobre “períodos de armazenamento”. A redação dá a entender que o direito de exclusão não pode ser exercido. Idealmente, a empresa deveria ter especificado quais dados podem ser excluídos e quais não, assim como a razão para tal distinção.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, considerou-se, na média, que foi atendido, tendo sido os sub-parâmetros (c) e (d) considerados atendidos, os sub-parâmetros (b), (e), (f), (g) parcialmente atendidos e os parâmetros (a) e (h) não atendidos.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, não foi considerado atendido. No Centro de Privacidade, em “Tratamento dos Dados” e “Armazenamento dos Dados”, a empresa informa:

Armazenamento dos dados

A Vivo armazena os seus dados durante o relacionamento com você e conforme as finalidades para as quais foram coletados. Além disso, seus dados são mantidos pelo tempo necessário, para cumprimento de obrigações legais e regulatórias, como em caso de ordens judiciais e solicitações de autoridades competentes, sempre em conformidade com a legislação vigente.

Dados como seus registros de conexão (tempo de conexão e IP) são armazenados pelo período mínimo de 1 ano. Registramos conteúdo de provedores de aplicativos, somente daqueles que criamos. Nesse caso, mantemos o registro por no mínimo 6 meses em ambiente controlado e seguro, de acordo com Marco Civil da Internet.

Os seus dados cadastrais (como por exemplo nome completo, endereço, CPF) e os dados de faturamento (documentos fiscais) são armazenados por no mínimo 5 anos, para processos administrativos e judiciais.

captura de tela de 23.07.2021

As informações sobre tempo de armazenamento não foram consideradas satisfatórias, pois não são apresentados os prazos de armazenamento detalhados para cada tipo de dado coletado, nem apontamento dos prazos máximos de armazenamento. Diferentemente do serviço de internet banda larga da Vivo, que aponta os períodos exatos de armazenamento no contrato de adesão aplicável, tais informações não foram localizadas quanto ao serviço de internet móvel. Quanto ao local de armazenamento, a empresa informa, na sua Política de Privacidade da Telefônica:

- A informação é preferencialmente tratada internamente na Telefônica Vivo ou em empresas do Grupo Telefônica, respeitando sempre a legislação vigente do Brasil.
- Em alguns casos a informação pode ser compartilhada com empresas parceiras, das quais são exigidos controles de segurança para proteção das informações.

Considerou-se a redação do trecho acima, por ser excessivamente ampla, insatisfatória. Mesmo que a empresa informe que “a informação é preferencialmente tratada internamente”, não são esclarecidas as hipóteses em que os dados são tratados externamente, quais os países onde são armazenados, quais tipos de dados são armazenados em cada local, dentre outras informações relevantes que poderiam ter sido fornecidas.

O sub-parâmetro (b), referente a quando/se os dados são apagados, considerou-se parcialmente atendido. Isso porque, no mesmo trecho apontado acima, em “Armazenamento dos Dados” no Centro de Privacidade, infere-se que os dados são apagados após o decurso do prazo apontado, mas não há esclarecimento se isso efetivamente ocorre.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, foi considerado atendido. No Relatório de Sustentabilidade de 2020 da empresa (p. 41), a empresa informa alguns dos padrões de segurança que utiliza para garantir a proteção dos usuários, afirmando ter desenvolvido, “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 da Informação”, 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.

O sub-parâmetro (d), referente a quem tem acesso aos dados, também foi considerado atendido, já que a empresa, vide parágrafo acima, afirma que somente pessoas autorizadas, conforme o ‘princípio do privilégio mínimo’, podem ter acesso aos dados. Mesmo que informações mais detalhadas sobre quais funcionários podem acessar os dados poderiam ter sido fornecidas, a menção ao princípio do privilégio mínimo indica para a existência de padrões mais claros em relação a tais acessos, razão pela qual o sub-parâmetro foi considerado cumprido.

O sub-parâmetro (e), referente aos terceiros com quem os dados são compartilhados, foi considerado parcialmente atendido. A Vivo, no Centro de Privacidade, e na Cláusula 5 de sua Política de Privacidade Local, a empresa elenca algumas hipóteses de fornecimento de dados a terceiros:

Compartilhamento de informações

Sua informação poderá ser compartilhada para garantir por exemplo, a prestação de serviços contratados por você e em atendimento de obrigações legais e regulatórias. Os dados poderão ser compartilhados com fornecedores, parceiros, empresas do grupo e autoridades, na medida necessária, sempre respeitando a legislação vigente. Mas fique tranquilo, o compartilhamento se dará através da adoção de medidas adequadas, visando a integridade e confidencialidade das informações.

A Vivo pode apoiar estudo de comportamento em eventos que promovam deslocamento de um público em determinada localização ou para determinada situação. Nesse caso, é importante ressaltar que não é possível qualquer forma de individualização dessas informações, que são tratadas de forma agregada.

captura de tela de 23.07.2021

As informações acima, mesmo que ofereçam algum guia para quais terceiros têm acesso aos dados, são excessivamente abrangentes. Não determinam quais terceiros podem recebê-los, não traz exemplos de situações em que possa ter havido autorização expressa do usuário, não tendo sido encontrados casos de tais autorizações nos documentos analisados e não determina quais dados e em quais situações são compartilhados. No entanto, por haver preocupação em apontar informações sobre o tema, com um mínimo de detalhamento, o sub-parâmetro foi considerado parcialmente atendido.

O sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi parcialmente atendido. Isso porque as informações trazidas sobre o tema, referenciadas na análise do sub-parâmetro (e) acima, assim como em redação bastante similar na Cláusula 5 de sua Política de Privacidade local, são pouco claras e afirmam somente de forma genérica que os dados podem ser compartilhados “para garantir, por exemplo, a prestação dos serviços contratados por você”. 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.

O sub-parâmetro (g), referente às hipóteses de transferência internacional de dados, foi considerado parcialmente atendido. Em seu centro de privacidade, assim como em redação bastante similar na Cláusula 6 de sua Política de Privacidade local, a empresa informa:

Transferência internacional

A Vivo, como parte do Grupo Telefónica pode, em algumas circunstâncias e quando necessário, compartilhar dados pessoais para outras empresas do Grupo. Além disso, seus dados podem ser compartilhados com parceiros e fornecedores com sede em outros países, sempre em conformidade com a legislação aplicável e de acordo com as cláusulas contratuais.

captura de tela de 23.07.2021

As informações acima não esclarecem as hipóteses e situações em que os dados podem ser enviados para fora do país de maneira clara ou exaustiva. No entanto, por haver preocupação em apontar informações sobre o tema, com um mínimo de detalhamento, o sub-parâmetro foi considerado parcialmente atendido.

Por fim, o sub-parâmetro (h), referente à data da última atualização da política de privacidade, não foi atendido. Não há referências a alterações no Centro de Privacidade da Vivo, onde a maior parte das informações sobre privacidade são apresentadas. Além disso, 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”.

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. O InternetLab realizou um pedido de acesso a dados em 21 de julho de 2021 por meio do portal da privacidade da empresa, que, no entanto, resultou em uma mensagem de erro. Após contato com o DPO da empresa, o erro foi corrigido e informações cadastrais do titular puderam ser acessadas por meio do portal.

O **parâmetro IV**, 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, 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 V**, 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:

Centro de Transparência e Privacidade da Vivo

Encontre de forma fácil alguns dos temas importantes que estão em nosso Centro de Transparência



Políticas de Privacidade

Você encontra informações detalhadas sobre o tratamento dos seus dados

[Ver mais](#)



Segurança

Como protegemos as informações fornecidas por você

[Ver mais](#)



Tratamento de Dados

Entenda as finalidades e quais informações coletamos

[Ver mais](#)



captura de tela de 23.07.2021

No entanto, não pôde ser localizado o contrato de prestação de serviços de internet móvel, 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 Móvel obteve **estrela cheia**, tendo cumprido os parâmetros I, II e V, parcialmente o parâmetro IV e não atendido o III.

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, foi considerado cumprido. Na página 22 do *Informe de Transparencia en las Comunicaciones 2021* da Telefônica, 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”:

“Intercepción 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 (Ministerio Público) o Comisario de Policía (Autoridad 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.

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

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

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, foi considerado parcialmente cumprido. 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**, relativo à existência de protocolos específicos sobre entrega de dados ao estado, foi considerado atendido. Este ano, 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”. O InternetLab enaltece a criação dessa nova seção, em nosso conhecimento, pouco usual na indústria.



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 receberemos 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.

captura de tela de 23.07.2021

O InternetLab enaltece ainda 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 para que a empresa seja pontuada sem ressalvas, seja em contratos, no Relatório de Sustentabilidade, ou outros materiais.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: ★

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

O **parâmetro I**, referente à contestação de legislação, foi considerado atendido. Na fase de engajamento com as empresas, a empresa apresentou algumas ações nesse sentido. Por exemplo, mencionamos uma ação, protocolada em conjunto com outras operadoras de telefonia, em que se contestam alterações ao Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações - RGC que obrigariam as empresas a fornecerem, a qualquer destinatário de ligações telefônicas, dados pessoais da pessoa que fez a ligação (Ação rescisória no 0802518-50.2020.4.05.0000).

Por fim, o **parâmetro II** foi igualmente considerado atendido. Na fase de engajamento com as empresas, a Vivo apresentou ao InternetLab, com informações sensíveis tarjadas, diversas respostas a ofícios administrativos em que se negou a fornecer dados pessoais a autoridades públicas. Por exemplo, há situações em que negou a entrega de Histórico de Chamadas e Localização de ERBs ao Ministério Público e às Autoridades Policiais, sob a justificativa de ausência da observação do princípio da reserva constitucional de jurisdição.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Civil Pública nº 0005292-42.2003.4.03.6110, que questiona, entre outros, a entrega de dados de portas lógicas às autoridades policiais, e a Ação Direta de Inconstitucionalidade (ADI) 5642⁵⁹, da ACEL, não foram consideradas, já que não registraram movimentações.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: ★

Nesta categoria, a Vivo Móvel obteve **meia estrela**, pois atendeu ao parâmetro I.

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

⁵⁹ 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.

oportunidade de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários.

Durante a fase de engajamento com as empresas, a Vivo nos forneceu exemplos de situações nesse sentido. Por exemplo, em artigo de opinião, publicado no portal Poder 360 em setembro de 2021 por Breno Oliveira, diretor jurídico da Telefônica Brasil, defendem-se algumas técnicas de privacidade e formas de se realizar a implementação da LGPD de maneira “bem-sucedida”⁶⁰.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, não foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial⁶¹; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020⁶²; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética⁶³; entre outras.

Durante a fase de engajamento, a empresa nos forneceu cópia de suas contribuições à Consulta Pública nº 24 da Anatel, em que defende, principalmente, ampliação do diálogo e da participação do setor privado nas temáticas desenvolvidas pelas CBCs. No entanto, não há, nessa consulta, qualquer menção a técnicas de segurança.

Vale ressaltar que a Vivo sofreu em 2020 um suposto ataque cibernético a seu aplicativo, em que foram vazados diversos dados de clientes⁶⁴, sendo inclusive que chegou a ser processada pelo coletivo Intervezes para obtenção de maiores informações e notificada pela Anatel e pelo Procon⁶⁵. Na fase de engajamento, a empresa nos apresentou as respostas públicas apresentadas ao SENACON quanto ao caso, em que afirma ter avaliado seus sistemas internos e não ter averiguado qualquer incidente de segurança. No entanto, não há menções a melhorias em técnicas de segurança.

Por fim, em geral, perante a mídia, a empresa negou-se a comentar o suposto vazamento e afirmou que “o número de clientes possivelmente impactados por esta ação ilícita é consideravelmente menor do que o divulgado por alguns órgãos da imprensa especializada”⁶⁶. Não foram dadas explicações mais robustas sobre o caso, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. A resposta da empresa foi considerada excessivamente genérica. Contudo, nesta

⁶⁰ <https://www.poder360.com.br/opiniaio/tecnologia/relatorio-de-conformidade-e-chave-para-adequacao-a-igpd-escreve-breno-oliveira>

⁶¹ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

⁶² SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

⁶³ TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

⁶⁴ <https://tecnoblog.net/320931/vivo-acao-judicial-expor-dados-pessoais-clientes-meu-vivo/>

⁶⁵ <https://tecnoblog.net/313892/anatel-procon-sp-notificam-vivo-dados-expostos-clientes/>

⁶⁶ <https://g1.globo.com/economia/noticia/2021/02/18/operadoras-dizem-que-nao-detectaram-vazamentos-de-dados-de-clientes.ghtml>

edição do relatório, as respostas relativas a tais vazamentos não foram consideradas para fins de pontuação.

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

Resultado: 

Nesta categoria, a Vivo Móvel obteve $\frac{3}{4}$ de estrela, pois atendeu aos parâmetros I, II e III e parcialmente ao parâmetro IV.

O **parâmetro I**, relativo à publicação de relatórios de transparência em português, foi considerado atendido. Pelo quinto ano seguido, encontramos a publicação do *Informe de Transparencia en las Comunicaciones de 2021*, do Grupo Telefônica (documento em espanhol), em que há certo detalhamento sobre o conjunto regulatório em cada país no qual o grupo está presente. Além disso, o Relatório de Sustentabilidade 2020 da Vivo, em português, contém informações sobre privacidade e proteção de dados, apontando alguns requisitos de segurança utilizados, princípios da empresa sobre o assunto, alguns links relevantes, dentre outros. Durante a fase de engajamento, a empresa nos mostrou que seu Informe de Transparência havia sido traduzido ao português e publicado em seu centro de privacidade, razão pela qual o parâmetro foi considerado atendido.

O **parâmetro II**, relativo à acessibilidade do relatório de transparência, foi considerado atendido. Isso porque tanto o Relatório de Sustentabilidade quanto o Informe de Transparência em português podem ser encontrados na página principal do centro de privacidade da Vivo.

O **parâmetro III**, relativo à periodicidade do relatório, foi considerado atendido. Nas páginas de ambos 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. No *Informe de Transparencia en las Comunicaciones* (pp. 22 e 23), informa-se que, em 2020, foram feitos 363.125 requerimentos de interceptação e 2.550.060 requerimentos de acesso a metadados. No entanto, em ambos os casos, afirma-se que 0 (zero) pedidos foram rechaçados. Durante a fase de engajamento, a empresa nos esclareceu que um “pedido rechaçado” consistiria em não se ter respondido determinado ofício enviado por uma autoridade pública. A empresa considera que um ofício pedindo acesso a dados pessoais cuja resposta foi negativa, por ter sido respondido, não foi “rechaçado”. Assim, a empresa efetivamente informa, em seu relatório, que respondeu a todos os ofícios. No entanto, buscando maior transparência perante os usuários, seria necessário que houvesse a informação de quantos pedidos foram *negados*, i.e., quantas vezes se considerou que determinado ofício era ilegal, excessivamente genérico etc. Por essa razão, o parâmetro foi considerado parcialmente atendido.

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 Móvel 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 $\frac{3}{4}$ de estrela, pois atendeu integralmente ao parâmetro II, V e parcialmente ao parâmetro I.

A Algar atende parcialmente ao **parâmetro I**. A empresa oferece informações claras e completas sobre os sub-parâmetros (b), (d) e (e); e cumpre parcialmente os sub-parâmetros (a) e (c).

O *sub-parâmetro (a)*, referente aos dados coletados, foi considerado parcialmente cumprido. 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 | <ul style="list-style-type: none"> ● 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. | <ul style="list-style-type: none"> ● 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. |

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.

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.

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 cumprido. 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 finalidade do tratamento de dados, foi considerado parcialmente cumprido. 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 (d)*, referente à forma como se dá a utilização, foi considerado cumprido. 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.”

Por fim, o *sub-parâmetro (e)*, relativo à informação quanto aos direitos dos titulares e meios para exercício desses direitos, foi considerado cumprido. Na Política de Privacidade de Dados Pessoais, bem como na Política de Governança de Dados, a empresa informa quais são os direitos dos titulares (limitação ou anonimização do uso de seus dados pessoais, revogação de consentimento, acesso aos dados etc). A empresa informa também que o exercício do direito dos titulares pode ser realizado através de solicitação ao Encarregado de Dados Pessoais ou por meio do Canal de Atendimento. Os e-mails e contatos são disponibilizados pela empresa:

Privacidade de Dados Pessoais

4.3.1 - Direitos Básicos

O cliente/usuário poderá solicitar ao nosso Encarregado de Dados Pessoais a confirmação da existência de 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 sido 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.

4.4.3 - Canais de Atendimento

Em caso de qualquer dúvida com relação às disposições constantes desta Política, o cliente/usuário poderá entrar em contato por meio dos canais de atendimento:

- Encarregado pelo Tratamento de Dados Pessoais (DPO):
o Alexandre da Silva Simões e-mail: dpo@algartelecom.com.br

Governança de Dados Pessoais

4.11 - Diretrizes de resposta à solicitações e requisições

4.11.1 - Resposta à requisição do titular dos dados pessoais

4.11.1.1 - Os procedimentos de resposta às requisições dos titulares dos dados pessoais serão regidos pelo procedimento de resposta à requisição do titular dos dados pessoais, disponível na biblioteca de documentos da Algar Telecom (<https://book.algarnet.com.br>);

4.11.1.2 - Todos os associados, credenciadas ou prestadores de serviço têm o dever de notificar o encarregado pelo tratamento de dados pessoais, sem demora injustificada, sobre qualquer requisição recebida do titular dos dados pessoais, antes de responder a requisição, buscando, sempre que possível, orientações acerca de melhores práticas na comunicação a ser estabelecida com o titular dos dados pessoais;

4.11.1.3 - Em casos de dúvida e situações específicas, o associado, credenciada ou prestador de serviço deve encaminhar a requisição ao encarregado pelo tratamento de dados pessoais, para que este responda da forma mais adequada perante à legislação específica aplicável e às boas práticas estipuladas internamente ou observadas no mercado.

4.12 Acesso aos dados pessoais pelo titular dos dados pessoais

4.12.1 - O titular dos dados pessoais pode requerer a qualquer momento acesso aos seus dados pessoais, devendo o associado, credenciada ou prestador de serviço da área responsável pelo tratamento assegurar que a identidade do titular dos dados pessoais seja comprovada conforme procedimento de resposta à requisição do titular dos dados pessoais;

4.12.2 - A requisição e posterior acesso aos dados pessoais deve ocorrer, preferencialmente, de modo eletrônico, exceto quando o titular dos dados pessoais expressamente requerer o envio dos dados pessoais de modo físico ou divulgação de modo oral. Podem ser utilizados recursos visuais para tornar as informações ainda mais inteligíveis e de fácil compreensão.

4.13 - Eliminação e/ou bloqueio de tratamento dos dados pessoais por requisição do titular dos dados pessoais

4.13.1 - O titular dos dados pessoais pode requerer a qualquer momento a eliminação e/ou bloqueio do tratamento de seus dados pessoais, devendo o associado, credenciada ou prestador de serviço da área responsável pelo tratamento encaminhar a requisição de eliminação/bloqueio ao encarregado pelo tratamento de dados pessoais para que possam ser adotadas as medidas necessárias conforme indicado no procedimento de resposta à requisição do titular dos dados pessoais;

4.13.2 - Na impossibilidade da eliminação, o titular deve ser informado sobre esta decisão, explicando os motivos pelos quais estes dados pessoais não poderão ser apagados;

4.13.3 - A área de infraestrutura de TI deve estabelecer mecanismos quando da restauração de dados pessoais que impeçam que sejam restauradas ao ambiente lógico os dados pessoais de titular que tenha solicitado sua eliminação.

O **parâmetro II**, 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), (d), (g) e (h); e cumpre parcialmente os sub-parâmetros (e) e (f).

O *sub-parâmetro (a)*, referente ao tempo e local de armazenamento dos dados, foi considerado cumprido. 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 nesse 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”:

4.2 - Armazenamento dos Dados Pessoais e Registros

4.2.1 - Armazenamento dos Dados

Os Dados Pessoais coletados e os registros de atividades são armazenados em ambiente seguro e controlado | prazo mínimo que segue a tabela abaixo:

| 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 Consumidor |
| 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 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.

Captura de tela de 22.07.2021

Quanto ao *sub-parâmetro (b)*, referente a quando/se os dados são apagados, considerou-se que 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 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

9.1 - 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:

- a) Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente;

- b) Adoção de medidas de segurança para proteger os dados pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito;
- c) Armazenamento de modo seguro, controlado e protegido;
- d) Processos de anonimização e pseudonimização, sempre que necessário;
- e) Protocolos de criptografia na transmissão e armazenamento, sempre que necessário;
- f) Registro lógico das operações de tratamento;
- g) Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias;
- h) Transferência à terceiros de modo seguro e contratualmente previsto;
- i) Avaliação de impacto e sistemática à privacidade dos titulares de dados;
- j) Gestão e tratamento adequado de incidentes que envolvam dados pessoais;
- k) 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.

Em seu Relatório de Sustentabilidade, na seção “Segurança da Informação”, a empresa informa:

Temos um ecossistema com sistemas que estão expostos a riscos de cyber segurança. Para mitigar esses riscos, contamos com soluções de proteção contra contaminação intencional ou acidental, malware e antivírus; estrutura para detecção de anomalias em nossa rede interna e externa, cyber ataques e tráfego anômalo; e ferramentas de controle de acesso a dados confidenciais. Em atendimento à Lei 13.709 (Lei Geral de Proteção de Dados Pessoais), foram adequados os processos e políticas da Companhia, reforçada a comunicação para todos os níveis da empresa e implementado sistema de proteção contra vazamento de dados, visando dar cumprimento aos requisitos legais e reforçando o ambiente de segurança cibernética. (p. 40)

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

O *sub-parâmetro (d)*, referente a quem tem acesso aos dados, foi considerado atendido. Em sua Política de Segurança da Informação a empresa informa algumas diretrizes sobre o acesso aos dados por associados da Algar Telecom:

10.1.1 - Associados Algar Telecom

- a) Todo associado deve ter conhecimento de todas as políticas vigentes na empresa, em especial a Política de Segurança da Informação, Código de Conduta Algar, Treinamentos de Conscientização em Segurança da Informação e ser coerente com os mesmos;
- b) Todos os associados devem assinar o Termo de Compromisso e Responsabilidade e Acordo de Confidencialidade no ato de sua admissão ou sempre que solicitado pela empresa;
- c) É vedado a qualquer associado a utilização indevida de informações da empresa e/ou de seus clientes, transmitirem-nas para a concorrência, utilizá-las para benefício próprio e/ou armazenar arquivos e e-mails de forma imprópria;
- d) A Algar Telecom pode receber e armazenar automaticamente informações sobre as atividades de qualquer pessoa que utilize seus recursos, incluindo endereço IP, usuário, aplicativos, tela/página e conversação efetuada dentro ou por meio desta empresa;
- e) Qualquer ID de autenticação (usuário e senha) na rede corporativa ou em aplicativos fornecidos pela Algar Telecom é de uso pessoal e intransferível e cada usuário será responsável pelo armazenamento e uso do mesmo;
- f) Ao final do vínculo empregatício e/ou contratual de associados Algar Telecom, a mesma realizará imediatamente a desativação dos ID's de autenticação utilizados durante o vínculo ou prestação de serviço.

10.1.2 – Fornecedores, Terceiros e Visitantes

- a) É vedado a qualquer pessoa prestadora de serviço utilizar sem autorização ou indevidamente informações da empresa e de seus clientes, transmiti-las

para concorrência, utilizá-las para benefício próprio e/ou armazenar arquivos e e-mails de forma imprópria;

b) Recebendo acesso a qualquer recurso da Algar Telecom, o prestador de serviço estará sujeito às políticas e diretrizes internas da empresa e a todos os critérios estabelecidos pelo “contrato de prestação de serviços” assinado no ato da contratação e, se for o caso, ser penalizado conforme previsto neste documento;

c) Qualquer ID de autenticação (usuário e senha) na rede corporativa ou em aplicativos fornecidos pela Algar Telecom é de uso pessoal e intransferível e cada usuário será responsável pelo armazenamento e uso do mesmo;

d) Ao final do vínculo contratual, o responsável pelo contrato dos prestadores de serviço da Algar Telecom deve garantir que os ID’s de autenticação utilizados durante os trabalhos sejam devidamente desabilitados

Em sua Política de Privacidade, a empresa informa que o acesso aos dados é restrito aos profissionais autorizados pela Algar:

4.1.14 - Acesso à Base de Dados

O acesso aos dados tratados é restrito apenas a profissionais devidamente autorizados pela Algar Telecom, sendo que seu uso, acesso e compartilhamento, quando necessários, estarão de acordo com as finalidades descritas nesta política

O *sub-parâmetro (e)*, 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 (f)*, relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi parcialmente atendido. Isso porque as informações trazidas sobre o tema, referenciadas na análise do sub-parâmetro (e) acima, 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 (g)*, 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.

Por fim, quanto ao *sub-parâmetro (h)*, relativo à data da última atualização da política de privacidade, foi considerado cumprido. A Política de Segurança da Informação, Política de Privacidade e Política de Governança de Dados contam com a data da última atualização (as três foram atualizadas em 17/05/2020). No entanto, vale ressaltar que tal informação não consta nos contratos da empresa. Recomendamos que a prática de informar a última atualização não se limite às políticas de privacidade e que seja aplicado em todos os documentos da empresa.

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, não foi considerado atendido. Ao realizarmos o pedido de acesso a dados através do portal da empresa em 27 de julho de 2021⁶⁷, não obtivemos respostas.

O **parâmetro IV**, 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 Algar mencionava tal possibilidade. Na Política de Privacidade, a empresa recomenda uma consulta periódica dos documentos, pois se reserva no direito de alterar as políticas a qualquer momento.

4.4.2 - Atualização dos Termos

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.algartelem.com.br.

Por fim, o **parâmetro V**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado atendido. A empresa dispõe de uma seção intitulada “Privacidade e Segurança

⁶⁷ Protocolo: 000000024302.20210727

da Informação”, que pode ser acessado no rodapé de seu site⁶⁸, 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
- 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.

⁶⁸ Ver: <https://algartelecom.com.br/politicas/politica-dados.html>

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 **estrela vazia**, pois não atendeu a nenhum 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, e não localizamos quaisquer ações nesse sentido. 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.

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 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) 5642⁶⁹, da ACEL, não foram consideradas, já que não registraram movimentações.

Na fase de engajamento, a empresa nos informou sobre duas ações em que a empresa foi parte por contestação de pedidos abusivos (Processo nº 1009561-39.2019.4.01.3803, TRF-1 e processo nº 11901-75.2016.4.01.3803 1, 1ª Vara Federal de Uberlândia). No entanto, o processo da 1ª Vara Federal de Uberlândia é de 2016, estando fora do escopo temporal do relatório. Quanto ao segundo processo informado pela empresa, na consulta processual realizada no site do Tribunal Regional Federal da 1ª Região, a ação não foi encontrada:

The screenshot shows the website of the Tribunal Regional Federal da Primeira Região (TRF1). The header includes the logo of the Justiça Federal and the text 'TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO (61) 3314-5225'. The breadcrumb trail reads 'Início > Consulta Processual / TRF1 > 1009561-39.2019.4.01.3803'. There are navigation icons for font size and a help icon. The main content area is titled 'Relatório de Indisponibilidade' and features a search options section with a dropdown arrow. A red message box states 'Processo não foi encontrado.' Below this, a timestamp indicates the search was performed on 28/10/2020 at 18:59:40, taking 0.309 seconds. A disclaimer at the bottom of the message box states: 'Este serviço tem caráter meramente informativo, portanto, SEM cunho oficial.' There are 'Login' and 'Quero Conciliar' buttons on the right side of the page.

⁶⁹ 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.

Agradecemos a participação da empresa, no entanto, como a ação não pôde ser encontrada, o parâmetro não foi considerado atendido

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Algar obteve $\frac{1}{2}$ **estrela**, pois atendeu ao parâmetro II.

O **parâmetro I**, relativo ao posicionamento em geral da empresa, não 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.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido. As matérias jornalísticas sobre a Algar diziam respeito à adequação da empresa à LGPD.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial⁷⁰; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020⁷¹; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética⁷²; entre outras. Além de diversas oportunidades para tratar sobre o tema na imprensa e em discussões públicas.

A Algar participou do Congresso intitulado LGPD – Desafios Enfrentados desde a sua Entrada em Vigor, organizada pela IBRASPD, o Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados. A empresa participou do painel “CISO e DPO – Pandemia dos megavazamentos, como lidar com esse

⁷⁰ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

⁷¹ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

⁷² TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

cenário e atender o direito do titular”, na pessoa do Alexandre Simões, no dia 01 de setembro de 2021⁷³. Tal participação foi considerada suficiente para atender ao parâmetro.

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

Resultado:



Nesta categoria, a Algar obteve **estrela vazia**, pois não atendeu a nenhum parâmetro.

Os **parâmetros I a IV** desta categoria, relativos à publicação de relatório de transparência, não foram atendidos. Apesar da empresa publicar anualmente um [Relatório de Sustentabilidade](#), o documento não contém qualquer informação relacionada a pedidos de dados recebidos, atendidos e rechaçados.

As únicas informações sobre dados pessoais que constam no Relatório de Sustentabilidade 2020 estão na seção “Segurança da informação”, que afirma que não houve registro de vazamento de dados no último ano e que explora, brevemente, as ações adotadas pela empresa para a adequação à LGPD. Na seção, a empresa informa que recebeu 92 solicitações (sem especificar de quem seriam as solicitações) que foram atendidas conforme a legislação.

Desde a vigência da legislação não registramos incidentes de Segurança da Informação envolvendo dados pessoais e também não recebemos reclamações fundamentadas sobre violações de privacidade de titulares de dados. As 92 solicitações recebidas em 2020 foram atendidas conforme legislação e dentro do prazo (p. 45).

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.

⁷³ <https://www.ibraspd.org/webinar-registration>.

BRISANET MÓVEL

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Brisanet Móvel obteve **meia estrela**, tendo atendido ao parâmetro III e parcialmente ao parâmetro V.

A Brisanet não atende ao **parâmetro I**, tendo atendido somente ao sub-parâmetro (e) e parcialmente ao sub-parâmetro (b).

O sub-parâmetro (a), referente aos dados coletados, não foi considerado atendido. Em sua Política de Privacidade, a empresa informa:

Os Dados Pessoais podem ser coletados por meio de formulário preenchido por Você, na celebração de contrato com a Brisanet, no aplicativo, nas interações no website por meio de cookies ou em nossas lojas, dentre outros. Neste caso, a Brisanet assume o papel de controlador.

É importante destacar que a Brisanet não trata Dados Pessoais sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização religiosa, filosófica ou política, dado referente à sua saúde ou à sua vida sexual. Os dados biométricos, como, por exemplo, fotos, podem ser coletados exclusivamente com a finalidade de evitar fraudes na prestação do serviço e aumentar a sua própria segurança.

Além disso, no contrato de Serviço Móvel Pessoal Pré-pago, a empresa informa:

2.2. Caberá à BRISANET solicitar ao CLIENTE, previamente à ativação do Serviço Pré-Pago, seus dados pessoais: a) nome completo; b) endereço completo; c) número do registro no Cadastro de Pessoa Física do Ministério da Fazenda (CPF/MF), no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ/MF) ou número do documento de identidade.

As informações acima são referentes às situações em que a coleta ocorre, e fornecem alguns exemplos de dados pessoais coletados, mas é excessivamente genérica, não esclarecendo quais dados efetivamente o titular fornece. Por isso, o parâmetro não foi considerado atendido.

O sub-parâmetro (b), referente às situações em que a coleta ocorre, foi considerado parcialmente cumprido. Isso porque o mesmo trecho apontado acima esclarece as situações em que esta pode ocorrer (por meio de formulário, na celebração de contrato com a Brisanet etc.) 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.

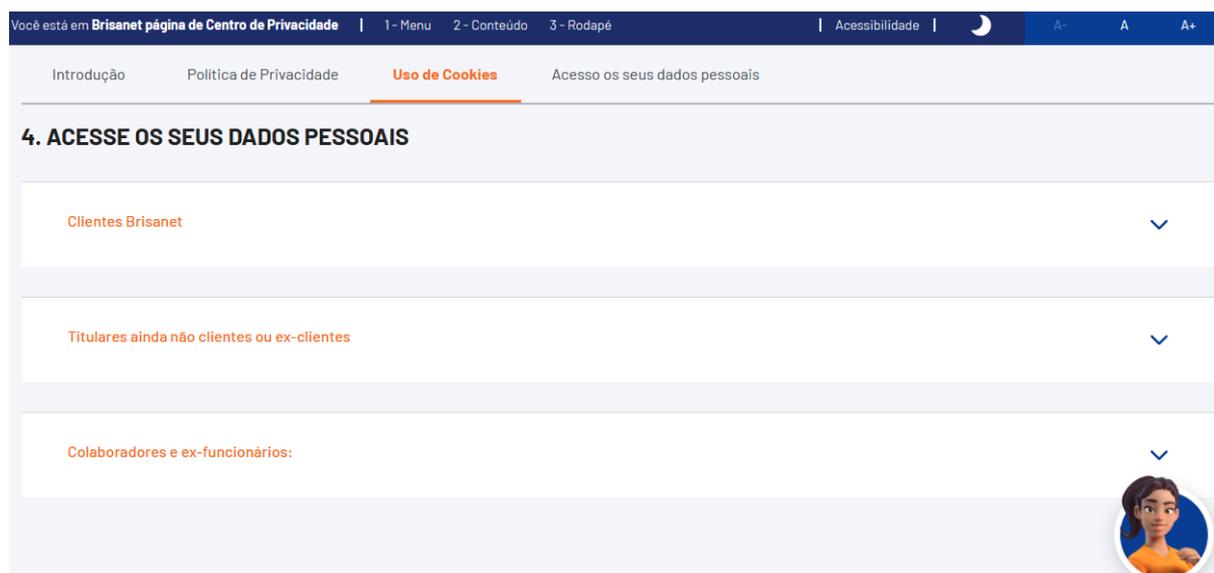
O sub-parâmetro (c), referente à finalidade do tratamento de dados, não foi considerado atendido. Em seus documentos, a Brisenet não informa para quais finalidades trata dados pessoais, informando somente e de forma genérica, (como será avaliado em maiores detalhes abaixo), algumas finalidades do compartilhamento de dados com terceiros.

O sub-parâmetro (d), referente à forma como se dá a utilização, não foi considerado cumprido. Não foram encontrados detalhes sobre hipóteses de uso dos dados nos documentos da Brisenet.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercício desses direitos, foi considerado atendido. Na Política de Privacidade, a empresa informa:

De acordo com a legislação, com relação aos seus Dados Pessoais, Você tem direito a confirmar a existência de tratamento, acessar, corrigir dados incompletos ou desatualizados, bloquear ou eliminar dados desnecessários, portar ou revogar o consentimento para tratamento, quando aplicável. Caso deseje acessar, corrigir ou atualizar os seus Dados Pessoais, Você poderá fazê-lo a qualquer tempo, por meio dos canais e procedimentos informados nesta Política, em nosso website ou aplicativo “Brisacliente”. Para os Dados Pessoais tratados mediante seu consentimento, Você poderá também revê-lo a qualquer momento. Esta ação não afetará a legitimidade do tratamento realizado anteriormente, tampouco prejudicará o tratamento executado com base em outras bases legais.

No Centro de Privacidade, há informações quanto aos meios para exercício destes direitos:



Você está em [Brisenet página de Centro de Privacidade](#) | 1 - Menu 2 - Conteúdo 3 - Rodapé | Acessibilidade | A- A A+

[Introdução](#) [Política de Privacidade](#) [Uso de Cookies](#) [Acesso os seus dados pessoais](#)

4. ACESSE OS SEUS DADOS PESSOAIS

- [Clientes Brisenet](#)
- [Titulares ainda não clientes ou ex-clientes](#)
- [Colaboradores e ex-funcionários:](#)



captura de tela de 23.07.2021

Mesmo que alguns dos direitos da Lei Geral de Proteção de Dados (como o direito de portabilidade ou de revisar decisões automatizadas) não tenham sido mencionados, as informações e o portal disponibilizado foram considerados suficientes para o atendimento do parâmetro.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, não foi considerado atendido. A empresa não fornece informações claras e completas sobre nenhum dos sub-parâmetros.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, não foi considerado cumprido. Não foram encontradas informações quanto ao local de armazenamento, e as informações quanto ao tempo foram consideradas excessivamente genéricas, não fornecendo prazos mínimos ou máximos ou quaisquer maiores detalhamentos:

A Brisanet trata seus Dados Pessoais pelo tempo que durar a prestação dos seus serviços, mas também precisa manter os dados após o término da sua relação contratual para cumprir a lei, como nos casos em que seja necessário fornecer dados às autoridades públicas ou mesmo na realização de defesa em processos judiciais.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, também se considerou que não foi atendido. Não foram localizadas essas informações nos documentos da Brisanet.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, não foi considerado atendido. Não foram localizadas essas informações nos documentos da Brisanet; somente menções genéricas a “armazenamento seguro” das informações dos titulares.

O sub-parâmetro (d), referente a quem tem acesso aos dados, não foi considerado atendido. Em nenhum dos documentos analisados encontramos informações sobre quem tem acesso aos dados, a empresa limita-se a informar genericamente sobre o compartilhamento de dados com terceiros, ponto que será avaliado no sub-parâmetro (e).

O sub-parâmetro (e), referente aos terceiros com quem os dados são compartilhados, não foi atendido. A empresa informa em sua Política de Privacidade:

A Brisanet poderá compartilhar seus Dados Pessoais com parceiros e fornecedores na medida necessária e com o objetivo de garantir a prestação do serviço contratado, para cumprir obrigações regulatórias ou outras previstas na legislação aplicável ou, ainda, para cumprir com qualquer uma das finalidades previstas nesta Política. Neste caso, o compartilhamento se dará por meio da adoção de medidas técnicas e empresariais adequadas, visando a confidencialidade e integridade dos dados.

Mesmo que haja alguma informação sobre o tema, não há informações detalhadas sobre quais “parceiros e fornecedores” receberão os dados, nem maiores especificações sobre quais tipos de parceiros, quais as obrigações regulatórias mencionadas etc.

Quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se também que não foi atendido, já que o trecho acima é, quanto às finalidades do compartilhamento, igualmente excessivamente genérico.

O sub-parâmetro (g), relativo à transferência internacional de dados, não foi considerado atendido. Não foram localizadas essas informações nos documentos da Brisanet.

Por fim, o sub-parâmetro (h), referente à data de última atualização da política de privacidade, foi considerado atendido. Ao fim do sua Política de Privacidade, a empresa aponta a data de sua última atualização.

captura de tela de 23.07.2021

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. O InternetLab realizou um pedido de acesso a dados em 21 de julho de 2021. Em resposta, a empresa informou que não havia, em seus bancos, quaisquer dados atrelados ao titular que fez a solicitação.

O **parâmetro IV**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, não foi considerado atendido. Em sua Política de Privacidade, a empresa afirma explicitamente que “se reserva o direito de alterar a presente Política (...)”, se comprometendo somente “a divulgar em seu website eventuais mudanças realizadas...”

Por fim, o **parâmetro V**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado parcialmente atendido. No rodapé da página inicial do site da Claro, 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 23.07.2021

No entanto, as informações que constam na Política de Privacidade não são apresentadas nos contratos da Brisnet, prática que seria recomendável para que as 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 Brisnet obteve **estrela vazia**, não tendo cumprido nenhum dos parâmetros.

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, não foi considerado cumprido. Em sua Política de Privacidade, a empresa menciona somente genericamente o compartilhamento “para cumprir obrigações regulatórias ou outras previstas na legislação aplicável.”

A Brisnet poderá compartilhar seus Dados Pessoais com parceiros e fornecedores na medida necessária e com o objetivo de garantir a prestação do serviço contratado, para cumprir obrigações regulatórias ou outras previstas na legislação aplicável ou, ainda, para cumprir com qualquer uma das finalidades previstas nesta Política. Neste caso, o compartilhamento se dará por meio da adoção de medidas técnicas e empresariais

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

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

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, também não foi considerado atendido. Não localizamos essas informações nos contratos da Brisanet.

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

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado:



Nesta categoria, a Brisanet Móvel obteve **estrela vazia**, pois não atendeu aos 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, e não localizamos quaisquer ações nesse sentido. 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.

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 “Brisanet S/A E sigilo E quebra” e por acórdãos publicados entre 01/08/2020 e 31/06/2021. Nas buscas, não foram localizadas quaisquer ações nesse 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.

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, não 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.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial⁷⁴; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado pela Anatel em 2020⁷⁵; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética⁷⁶; entre outras.

Em nenhuma dessas ocasiões foram encontrados posicionamentos da Brisagnet.

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

Resultado:



Nesta categoria, a Brisagnet 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 Brisagnet.

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

⁷⁴ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

⁷⁵ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

⁷⁶ TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.

BRISANET BANDA LARGA

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Brisanet Banda Larga obteve **meia estrela**, tendo atendido ao parâmetro III e parcialmente ao parâmetro V.

A Brisanet não atende ao **parâmetro I**, tendo atendido somente ao sub-parâmetro (e) e parcialmente ao sub-parâmetro (b).

O sub-parâmetro (a), referente aos dados coletados, não foi considerado atendido. Em sua Política de Privacidade, a empresa informa:

Os Dados Pessoais podem ser coletados por meio de formulário preenchido por Você, na celebração de contrato com a Brisanet, no aplicativo, nas interações no website por meio de cookies ou em nossas lojas, dentre outros. Neste caso, a Brisanet assume o papel de controlador.

É importante destacar que a Brisanet não trata Dados Pessoais sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização religiosa, filosófica ou política, dado referente à sua saúde ou à sua vida sexual. Os dados biométricos, como, por exemplo, fotos, podem ser coletados exclusivamente com a finalidade de evitar fraudes na prestação do serviço e aumentar a sua própria segurança.

As informações acima são referentes às situações em que a coleta ocorre, e fornecem alguns exemplos de dados pessoais coletados, mas é excessivamente genérica, não esclarecendo quais dados efetivamente o titular fornece. Por isso, o parâmetro não foi considerado atendido.

O sub-parâmetro (b), referente às situações em que a coleta ocorre, foi considerado parcialmente cumprido. Isso porque o mesmo trecho apontado acima esclarece as situações em que esta pode ocorrer (por meio de formulário, na celebração de contrato com a Brisanet etc.) 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.

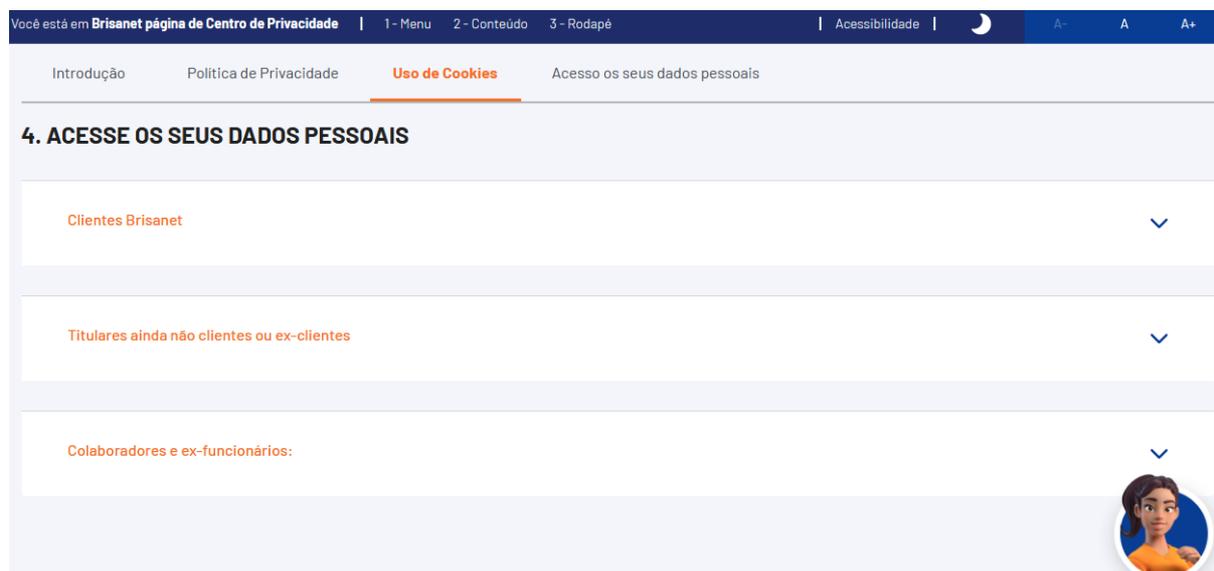
O sub-parâmetro (c), referente à finalidade do tratamento de dados, não foi considerado atendido. Em seus documentos, a Brisanet não informa para quais finalidades trata dados pessoais, informando somente e de forma genérica, (como será avaliado em maiores detalhes abaixo), algumas finalidades do compartilhamento de dados com terceiros.

O sub-parâmetro (d), referente à forma como se dá a utilização, não foi considerado cumprido. Não foram encontrados detalhes sobre hipóteses de uso dos dados nos documentos da Brisanet.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercício desses direitos, foi considerado atendido. Na Política de Privacidade, a empresa informa:

De acordo com a legislação, com relação aos seus Dados Pessoais, Você tem direito a confirmar a existência de tratamento, acessar, corrigir dados incompletos ou desatualizados, bloquear ou eliminar dados desnecessários, portar ou revogar o consentimento para tratamento, quando aplicável. Caso deseje acessar, corrigir ou atualizar os seus Dados Pessoais, Você poderá fazê-lo a qualquer tempo, por meio dos canais e procedimentos informados nesta Política, em nosso website ou aplicativo “Brisacliente”. Para os Dados Pessoais tratados mediante seu consentimento, Você poderá também revê-lo a qualquer momento. Esta ação não afetará a legitimidade do tratamento realizado anteriormente, tampouco prejudicará o tratamento executado com base em outras bases legais.

No Centro de Privacidade, há informações quanto aos meios para exercício destes direitos:



captura de tela de 23.07.2021

Mesmo que alguns dos direitos da Lei Geral de Proteção de Dados (como o direito de portabilidade ou de revisar decisões automatizadas) não tenham sido mencionados, as informações e o portal disponibilizado foram considerados suficientes para o atendimento do parâmetro.

Quanto ao **parâmetro II**, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, não foi considerado atendido. A empresa não fornece informações claras e completas sobre nenhum dos sub-parâmetros.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, não foi considerado cumprido. Não foram encontradas informações quanto ao local de armazenamento, e as informações quanto ao tempo foram consideradas excessivamente genéricas, não fornecendo prazos mínimos ou máximos ou quaisquer maiores detalhamentos:

A Brisnet trata seus Dados Pessoais pelo tempo que durar a prestação dos seus serviços, mas também precisa manter os dados após o término da sua relação contratual para cumprir a lei, como nos casos em que seja necessário fornecer dados às autoridades públicas ou mesmo na realização de defesa em processos judiciais.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, também se considerou que não foi atendido. Não foram localizadas essas informações nos documentos da Brisnet.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, não foi considerado atendido. Não foram localizadas essas informações nos documentos da Brisnet; somente menções genéricas a “armazenamento seguro” das informações dos titulares.

O sub-parâmetro (d), referente a quem tem acesso aos dados, não foi considerado atendido. Em nenhum dos documentos analisados encontramos informações sobre quem tem acesso aos dados, a empresa limita-se a informar genericamente sobre o compartilhamento de dados com terceiros, ponto que será avaliado no sub-parâmetro (e).

O sub-parâmetro (e), referente aos terceiros com quem os dados são compartilhados, não foi atendido. A empresa informa em sua Política de Privacidade:

A Brisnet poderá compartilhar seus Dados Pessoais com parceiros e fornecedores na medida necessária e com o objetivo de garantir a prestação do serviço contratado, para cumprir obrigações regulatórias ou outras previstas na legislação aplicável ou, ainda, para cumprir com qualquer uma das finalidades previstas nesta Política. Neste caso, o compartilhamento se dará por meio da adoção de medidas técnicas e empresariais adequadas, visando a confidencialidade e integridade dos dados.

Mesmo que haja alguma informação sobre o tema, não há informações detalhadas sobre quais “parceiros e fornecedores” receberão os dados, nem maiores especificações sobre quais tipos de parceiros, quais as obrigações regulatórias mencionadas etc.

Quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se também que não foi atendido, já que o trecho acima é, quanto às finalidades do compartilhamento, igualmente excessivamente genérico.

O sub-parâmetro (g), relativo à transferência internacional de dados, não foi considerado atendido. Não foram localizadas essas informações nos documentos da Brisnet.

Por fim, o sub-parâmetro (h), referente à data de última atualização da política de privacidade, foi considerado atendido. Ao fim do sua Política de Privacidade, a empresa aponta a data de sua última atualização.

Você está em **Brisanet página de Política de Privacidade** | 1 - Menu 2 - Conteúdo 3 - Rodapé | Acessibilidade | A- A A+

Tratamento de Dados Pessoais

Direito do Titular dos Dados Pessoais

Utilização de Cookies

Encarregado dos Dados Pessoais - DPO

Disposições Finais

Para ter andamento de sua requisição, certifique-se de observar o procedimento apresentado em nosso website. A Brisanet estabelece medidas de segurança para confirmar sua identidade.

Para clientes ativos, os Dados Pessoais cadastrais podem também ser conferidos diretamente no aplicativo "Brisacliente", o qual é acessado mediante autenticação por senha.

6. DISPOSIÇÕES FINAIS

A Brisanet se reserva o direito de alterar a presente Política para adaptá-la a possíveis modificações de cunho legal, regulatório ou, até mesmo, jurisprudencial, bem como àquelas relativas às práticas comerciais. Em qualquer destes casos, a Brisanet se compromete a divulgar em seu website eventuais mudanças realizadas nesta Política.

Pereiro / Ceará, 18 de setembro de 2020.

captura de tela de 23.07.2021

O **parâmetro III**, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. O InternetLab realizou um pedido de acesso a dados em 21 de julho de 2021. Em resposta, a empresa informou que não havia, em seus bancos, quaisquer dados atrelados ao titular que fez a solicitação.

O **parâmetro IV**, que avalia se a empresa promete enviar notificações ao usuário quando da atualização de suas políticas de privacidade, não foi considerado atendido. Em sua Política de Privacidade, a empresa afirma explicitamente que "se reserva o direito de alterar a presente Política (...)", se comprometendo somente "a divulgar em seu website eventuais mudanças realizadas..."

Por fim, o **parâmetro V**, referente à acessibilidade das informações sobre privacidade e proteção de dados, foi considerado parcialmente atendido. No rodapé da página inicial do site da Claro, 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.

Você está em **Brisanet página de Centro de Privacidade** | 1 - Menu 2 - Conteúdo 3 - Rodapé | Acessibilidade | A- A A+

Centro de privacidade da Brisanet

Introdução | Política de Privacidade | Uso de Cookies | Acesso os seus dados pessoais

1. INTRODUÇÃO

Os dados pessoais de nossos clientes sempre foram tratados pela Brisanet com a devida diligência e segurança, de acordo com as regras existentes no ordenamento legal. Com a entrada em vigor da Lei Geral de Proteção de Dados - Lei nº 13.709/2018 - no último dia 18 de setembro de 2020, o tratamento dos dados pessoais passou a ser disciplinado de forma mais detalhada e foram ampliados os direitos e deveres no que tange à utilização e ao tratamento desses dados.



captura de tela de 23.07.2021

No entanto, não pôde ser localizado o 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.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Brisnet obteve **estrela vazia**, não tendo cumprido nenhum dos parâmetros.

O **parâmetro I**, referente à identificação das autoridades competentes para requisitar dados, não foi considerado cumprido. Em sua Política de Privacidade, a empresa menciona somente genericamente o compartilhamento “para cumprir obrigações regulatórias ou outras previstas na legislação aplicável.”

A Brisnet poderá compartilhar seus Dados Pessoais com parceiros e fornecedores na medida necessária e com o objetivo de garantir a prestação do serviço contratado, para cumprir obrigações regulatórias ou outras previstas na legislação aplicável ou, ainda, para cumprir com qualquer uma das finalidades previstas nesta Política. Neste caso, o compartilhamento se dará por meio da adoção de medidas técnicas e empresariais

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

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

O **parâmetro IV**, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, também não foi considerado atendido. Não localizamos essas informações nos contratos da Brisnet.

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

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

Nesta categoria, a Brisnet Banda Larga obteve **estrela vazia**, pois não atendeu aos 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, e não localizamos quaisquer ações nesse sentido. 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.

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 “Brisanet S/A E sigilo E quebra” e por acórdãos publicados entre 01/08/2020 e 31/06/2021. Nas buscas, não foram localizadas quaisquer ações nesse 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.

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, não 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.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido.

O **parâmetro II**, relativo ao posicionamento da empresa sobre medidas de segurança, foi considerado atendido. Ao longo de 2020 e início de 2021, as empresas provedoras de acesso à Internet tiveram a oportunidade de se manifestar sobre políticas e práticas que promovam a segurança dos dados de seus usuários, como por exemplo: a Consulta Pública nº 24 da Anatel, sobre a reavaliação da estrutura e regimento interno das Comissões Brasileiras de Comunicações - CBC, cujo art. 2º, IV dispõe sobre as ações da Comissão no que se refere à Aspectos políticos relacionados à Segurança Cibernética e à Inteligência Artificial⁷⁷; o regulamento de Segurança Cibernética para o setor de Telecom, aprovado

⁷⁷ ANATEL. Regulamento das Comissões Brasileiras de Comunicações vai a consulta pública. 6 de maio de 2021. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regulamento-das-comissoes-brasileiras-de-comunicacoes-vai-a-consulta-publica>.

pela Anatel em 2020⁷⁸; a proposta da Anatel de criação de um grupo de cooperação em segurança cibernética⁷⁹; entre outras.

Em nenhuma dessas ocasiões foram encontrados posicionamentos da Brisanet.

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.

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

⁷⁸ SEGINFO. Anatel aprova regulamento de Segurança Cibernética para o setor de Telecom. 22 de dezembro de 2020. Disponível em: <https://seginfo.com.br/2020/12/22/anatel-aprova-regulamento-de-seguranca-cibernetica-para-o-setor-de-telecom/>.

⁷⁹ TELESÍNTESE. Anatel pode criar grupo de cooperação em cibersegurança. 18 de novembro de 2020. Disponível em: <https://www.telesintese.com.br/anatel-pode-criar-grupo-de-cooperacao-em-ciberseguranca/>.