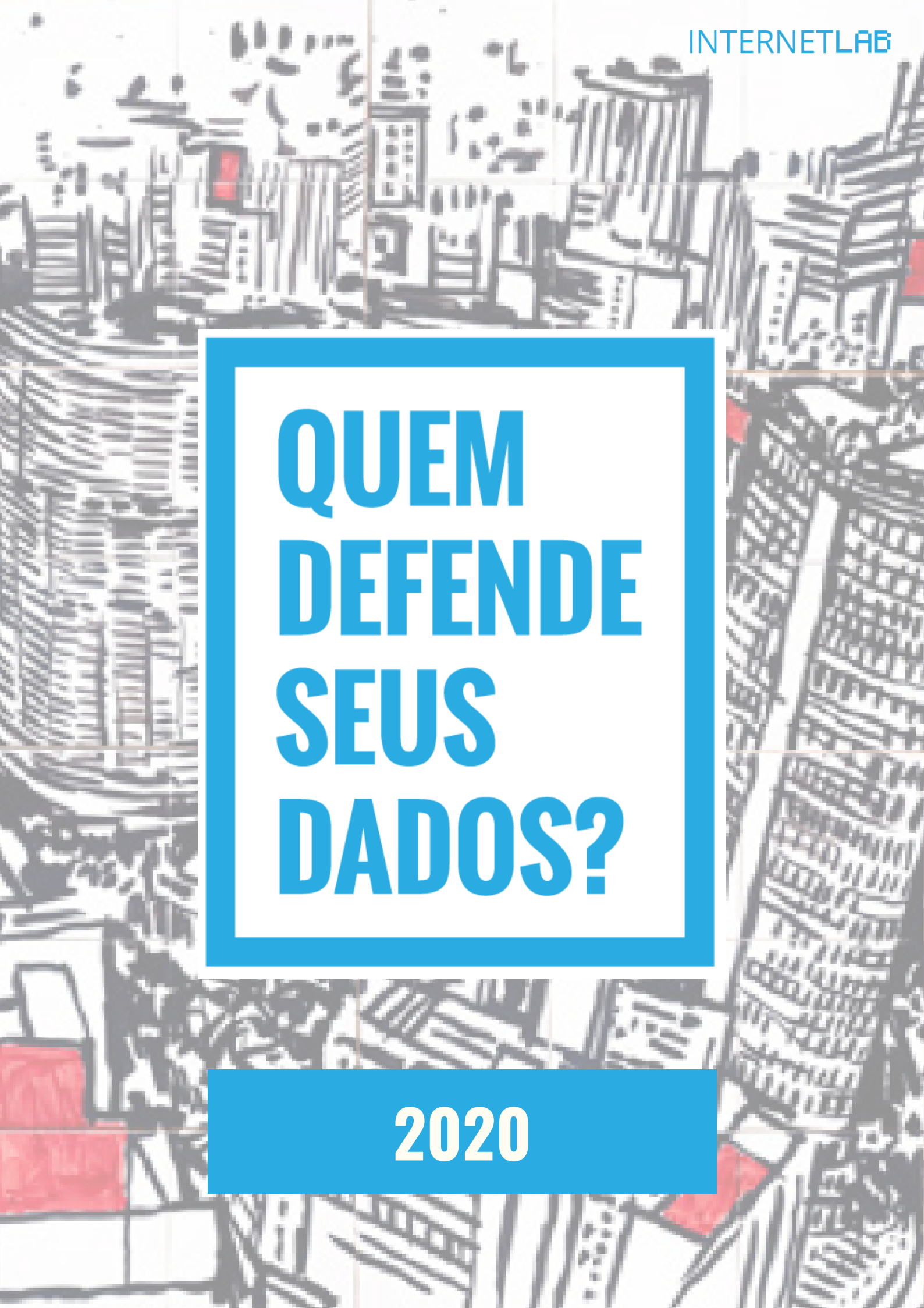
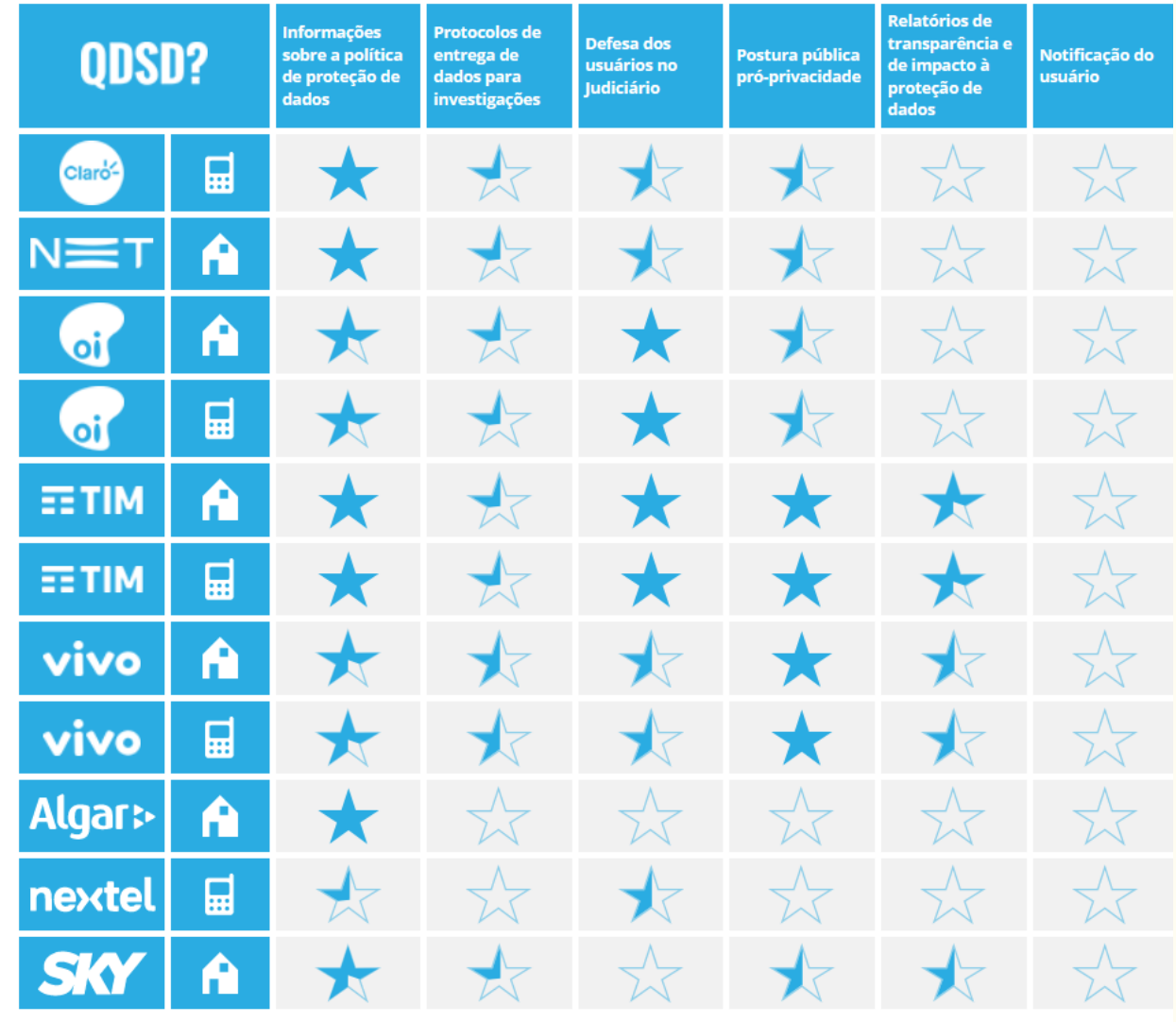

INTERNETLAB
QUEM DEFENDE SEUS DADOS?
2020

2020

RESULTADO GERAL



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.

Esta é a quinta edição do projeto "Quem Defende Seus Dados?", versão brasileira do “Who has your back?”. Desde 2015, o projeto "Who Has Your Back?", desenvolvido pela EFF nos Estados Unidos, vem se expandindo para outros países ao redor do mundo, especialmente os da América Latina. 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 documento, apresentamos a metodologia e os resultados de nossa análise em 2020. Neste ano, diante da entrada em vigor da Lei Geral de Proteção de Dados, de modificações nos entendimentos e práticas sobre privacidade e proteção de dados, e da pandemia de COVID-19, promovemos uma das maiores revisões de parâmetros de avaliação já feitas no Quem Defende Seus Dados.

Valorizamos nessa edição, 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 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, os posicionamentos da empresa em relação à privacidade dos usuários na pandemia de COVID-19, dentre outros.

Em sua quinta edição, o projeto avaliou as seguintes empresas (independentemente de pertencerem ao mesmo grupo econômico): Oi banda larga fixa e móvel; Vivo banda larga fixa e móvel, TIM banda larga fixa e móvel, NET, Claro, Nextel, Algar e Sky.

2020

METODOLOGIA

Cada empresa foi avaliada a partir de 6 categoriais, 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 de privacidade.

Para esta avaliação, foram analisados os contratos de prestação de serviço, relatórios de sustentabilidade e demais documentos disponíveis nos websites das empresas até 05/06/2020. 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 2019 e julho de 2020.

Com os resultados preliminares em mãos, entramos em contato com as empresas, solicitando que nos enviassem comentários, críticas ou documentos sobre os métodos e os resultados obtidos (setembro de 2020). Finalmente, dialogamos com as empresas que se manifestaram e, a partir de seus comentários, ajustamos, quando pertinente, o seu desempenho.

Com base nas respostas obtidas, atribuímos as seguintes notas: A. 1 estrela cheia; B. ¾ de estrela; C. ½ estrela; D. ¼ de estrela; E. Nenhuma estrela.

Uma estrela cheia significa que a empresa atende a todos os parâmetros em determinada categoria, enquanto a atribuição de nenhuma estrela significa que a companhia não atendeu a nenhum parâmetro.

Destacamos que, em vista das consideráveis mudanças, buscamos incentivar as empresas com avaliações que elevem sua nota geral. Especificamente, 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.

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

Mais recentemente, a Lei Geral de Proteção de Dados Pessoais reiterou e aprofundou estes marcos normativos e o respeito à transparência como princípio norteador da proteção de dados. Previu, assim, o direito do titular de dados pessoais a informações claras, adequadas e ostensivas sobre o tratamento de seus dados, especialmente no que diz respeito à finalidade específica, forma e duração do tratamento, à identificação e contato do controlador, ao eventual compartilhamento de dados e a respectiva finalidade, às responsabilidades dos agentes que realizarão o tratamento (LGPD, art. 9° 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. 7° 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.

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 (e) com quais terceiros e (f) para quais finalidades os dados são compartilhados.

[Respostas a solicitações de direitos] A empresa processou e satisfez, 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.

2020

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 demandam de provedores de conexão o fornecimento de informações que extrapolam a definição do art. 5, VI, do MCI, alcançando, por exemplo, o número da porta lógica de origem dos IPs. O MCI, 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 MCI, determina que a autoridade administrativa deve indicar no pedido o fundamento legal de competência 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 essas 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 STF, em decorrência da ação direta de inconstitucionalidade (ADI 5642) proposta em janeiro de 2017 pela a Associação Nacional das Operadoras de Celular (ACEL), por violarem os art. 5º, incisos X e XII da Constituição, ao permitirem uma interpretação, segundo a qual em alguns casos seria dispensável a ordem judicial para acesso aos dados de localização. Além disso, há outra controvérsia no que diz respeito à temporalidade dos dados locacionais que podem ser exigidos: a despeito de possível violação à privacidade e às normativas de proteção de dados, segundo algumas interpretações, somente o acesso a dados de localização em tempo real dependeria de 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.

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. Por se tratar de matéria sob controvérsia jurídica, a questão se desdobra em parâmetros que discriminam diferentes níveis de proteção, clareza e comprometimento quanto ao acesso a dados para investigações.

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 no prazo de 12 (doze) horas, entregar os dados 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

2020

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 diante de pedidos considerados abusivos.

Neste último caso, consideramos o disposto no Decreto nº 8.771/2016, que estabelece a necessidade de indicação do fundamento legal da competência da autoridade requerente e 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.

[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 os 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

2020

A empresa se posicionou publicamente em defesa da privacidade e da proteção de dados, fortalecendo a cultura de proteção a esses direitos no Brasil? Essa categoria levou em consideração a postura adotada pelas empresas no contexto da pandemia de COVID-19.

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 que tenham abordado leis, projetos de lei e políticas públicas que impactam usuários da rede, assim como seu posicionamento na mídia comum e especializada.

Neste ano, observamos ainda a postura adotada pelas empresas especificamente diante das medidas do setor público em resposta à pandemia do novo coronavírus, muitas delas dependentes da colaboração dos provedores de conexão. São exemplos dessas iniciativas os acordos que viabilizaram o monitoramento de deslocamento populacional para estimar a adesão às medidas de distanciamento social e a edição da Medida Provisória nº 954/2020 para o compartilhamento de informações cadastrais de usuários de linhas telefônicas com o Instituto Brasileiro de Geografia e Estatística (IBGE).

Avaliamos, nesse contexto, o comprometimento das empresas com a defesa dos direitos de seus usuários, manifesto em seu posicionamento em consultas públicas, debates ou na mídia, a respeito de tais iniciativas. Consideramos apenas a participação feitas 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, e defendeu concretamente a aprovação de normas ou adoção de técnicas que aumentem a proteção conferida aos usuários dos seus serviços?

[Posicionamento no contexto "COVID-19"] A empresa se posicionou em nome próprio, em consultas públicas, debates, ou na mídia, a favor de técnicas ou práticas que promovem a proteção de seus usuários diante de tentativas excepcionais de coleta de dados durante a pandemia de COVID-19, fornecendo informações acerca das medidas efetivamente tomadas nesse contexto?

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.

2020

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 elementos, 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 é uma prática corrente. No Brasil, ao contrário, é 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 concessões de acesso a 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 usuário.

Ressalta-se que também foi considerada a acessibilidade e publicidade dos relatórios de transparência. Por isso, somente relatórios escritos ou traduzidos para língua portuguesa foram considerados. Ademais, são melhor avaliados os relatórios facilmente acessíveis nas páginas principais das empresas.

A Lei Geral de Proteção de Dados Pessoais prevê, por fim, a elaboração 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 Autoridade Nacional de Proteção de Dados Pessoais pode determinar a elaboração de relatório de impacto (art. 10, §3°; art. 32 e art. 38).

Além da elaboração, a publicação de relatórios de impacto à proteção de dados é considerada uma boa prática, para os fins deste relatório, por reforçar o compromisso com a transparência e viabilizar uma prestação de contas da empresa acerca de suas práticas na gestão de dados pessoais.

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

2020

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 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. De acordo com o CPP, 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, §3°).

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.

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.

Diante disso, 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, alguns provedores 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 proibido 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 ampla 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. Mesmo no âmbito de processos criminais, 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, por 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.

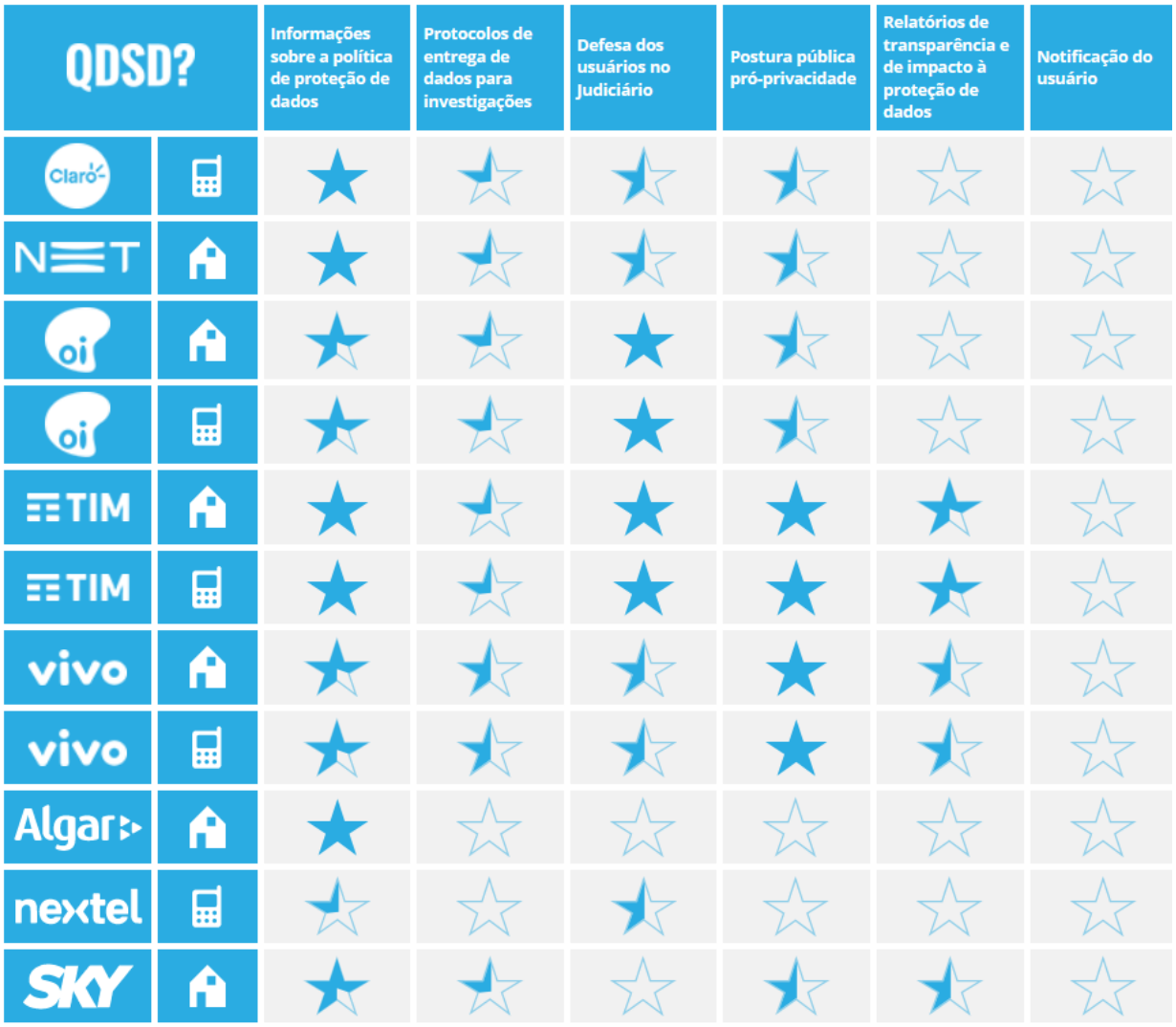
Padrões de desempenho

★ O provedor de Internet atende ao parâmetro.

☆ O provedor de Internet não atende ao parâmetro.

2020

RESULTADOS



CLARO

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a CLARO obteve estrela cheia, tendo atendido os 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 sua Política de Privacidade, a empresa informa:

> "Informações Cadastrais
> Boa parte dos nossos serviços exige que você tenha um cadastro único com uma conta de usuário, permitindo assim, o seu acesso a todos os serviços da Claro.
> Quando você faz o seu cadastro, solicitamos: seu nome, o seu CPF, o seu RG, a sua data de nascimento, a informação de gênero e seus dados de contato, como telefone e e-mail.
>
> Perfil de Consumo
> Com o objetivo de aprimorar a sua experiência na Claro, estamos continuamente efetuando melhorias na rede, ampliando e personalizando ofertas de produtos e serviços, enviando alertas ou notificações. Para esses objetivos, a Claro poderá coletar informações de seu perfil de consumo, como: localização, recursos, dispositivos utilizados, navegação, ofertas contratadas ou pesquisadas, informações fornecidas enquanto utiliza os serviços, assim como a duração e a frequência das suas atividades".

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 "Informações Cadastrais" e "Perfil de Consumo" (vide trecho acima), informa-se que a empresa coleta informações no momento do cadastro e "enquanto utiliza os serviços".

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 seção "Perfil de Consumo" da Política de Privacidade da Claro (vide trecho acima), a empresa informa que a coleta de dados tem como objetivo "aprimorar a sua experiência na Claro", personalização de ofertas,

realização de melhorias na rede e envio de alertas e notificações. Ainda, na seção "Sobre o tratamento de dados pessoais", a empresa fornece informações detalhadas sobre as finalidades do tratamento dos dados:

> "A Claro poderá realizar o tratamento de dados pessoais coletados para as seguintes finalidades:
> Com o objetivo de garantir a sua segurança na identificação, autenticação e autorização de acesso aos nossos produtos e serviços;
> Para o melhor atendimento de suas solicitações e resolução de suas dúvidas;
> Para manter os seus dados atualizados para que possamos contatar você sempre que for preciso, seja por telefone, e-mail, SMS, mala direta ou por outros meios de comunicação;
> Para aprimorar a sua experiência na navegação em nossos sites, aplicativos e serviços;
> Para uso em estatísticas, estudos, pesquisas e levantamentos sobre suas atividades e comportamentos ao utilizar os nossos sites, aplicativos e serviços;
>
> Para divulgar os nossos serviços e os de nossos parceiros, e comunicar as novidades, funcionalidades e outras informações que possam ser relevantes para aperfeiçoar nosso relacionamento;
> Para que nos preservemos em nossos direitos e obrigações relativos à utilização dos nossos sites, aplicativos e serviços;
> Para que possamos disponibilizar a você conteúdos relevantes e enviar, por exemplo, informações sobre sua fatura, seu consumo, seu pacote e promoções, além de outras facilidades;
> Para o envio de comunicações que você concordou em receber.
> A Claro, como proprietária, é responsável por sua própria base de dados, e pode utilizar as informações dentro do limite e propósito de seu ramo de atuação. A Claro poderá ainda utilizar informações de forma anonimizada, com o objetivo de aprimorar e personalizar continuamente os serviços que prestamos a você."

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. Na seção "Quais dados a Claro coleta e como usa?" de sua Política de Privacidade, a Claro detalha, 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 tráfego "são fundamentais para mensurar a qualidade dos nossos serviços, para que você possa entender a fatura e ainda para seu próprio controle", que dados bancários são utilizados "somente para efetuar a cobrança pelos serviços de telecomunicações ou outros serviços que você tenha contratado através da Claro", dentre outros.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercícios desses direitos, também foi considerado atendido. Na Política de Privacidade, há a seção "Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais", em que a empresa informa sobre a existência desses quatro direitos, por mais que não mencione todos os previstos na legislação atual. A empresa informa, também, os meios para o exercício destes direitos: a central de atendimento e o Fale Conosco da Claro.

> "Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais
> Nos comprometemos, em toda hipótese, com os padrões (...) de controle e segurança, respeitando os padrões exigidos.
> Você, cliente Claro, possui os seguintes direitos, a respeito de seus dados pessoais:
> De correção de dados que possam estar incompletos, incorretos ou desatualizados;
> Você poderá cancelar o consentimento dado à Claro, a qualquer momento. Para isso, é só entrar em contato com a central de atendimento ou com o canal que disponibilizamos, o Fale Conosco Claro;
> A Claro manterá as suas informações armazenadas pelo período exigido pelas leis existentes."

Além disso, em seu Contrato de Prestação de Serviços de acesso à internet Pré-pago, afirma:

> "8.1 Além dos direitos já previstos neste Contrato, são assegurados ao ASSINANTE os direitos estabelecidos no Regulamento do SMP e na Lei no 12.965/2014, tais como: a) Recebimento gratuito, mediante solicitação, do relatório detalhado do tráfego de dados utilizado, relativo ao prazo máximo de 6 (seis) meses anteriores ao seu pedido, desde que esteja com o cadastro devidamente atualizado perante a CLARO; h) inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; i) inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; m) exclusão definitiva de seus dados pessoais que tiver fornecido a determinada aplicação de internet; n) publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet."

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

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado parcialmente cumprido. Na sua Política de Privacidade, na seção

"Por quanto tempo a Claro trata seus dados?", a empresa informa os prazos de armazenamento detalhados para cada tipo de dado coletado. No entanto, quanto aos dados cadastrais e de faturamento, a Claro informa apenas o prazo mínimo pelo qual os armazena. Ainda que seja positivo que a empresa estabeleça um prazo mínimo, a ausência de informações sobre o período máximo pelo qual a empresa armazena os dados de seus clientes acaba por tornar demasiado impreciso tal período de tempo.

> "Por quanto tempo a Claro trata seus dados?
> 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 dos prazos que observamos são os seguintes:
> 1. Conexão à internet: a Claro armazenará os registros de conexão pelo prazo de um ano, e não guardará os registros de acesso a funcionalidades de internet;
> 2. Funcionalidades de internet: nos aplicativos próprios da Claro, os registros de acesso a funcionalidades serão armazenados por seis meses;
> 3. Dados cadastrais e de faturamento serão armazenados no mínimo por cinco anos."

Quanto ao local de armazenamento, a empresa informa nas seções "Por quanto tempo a Claro trata seus dados?" e "Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais" que os dados são processados nos datacenters da Claro, em servidores de terceiros contratados ou em "nuvens". Tais informações foram consideradas excessivamente genéricas, fornecendo poucas informações consistentes sobre o local de armazenamento.

> Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais
> Armazenamos os seus dados pessoais em local seguro. Muitas vezes em nossos próprios servidores, de terceiros contratados ou na "nuvem", sempre com o objetivo de melhorar nossos processos.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, não foi considerado atendido. Isso porque a empresa informa apenas o tempo mínimo de armazenamento dos dados.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, foi considerado atendido. Na Política de Privacidade, a empresa se compromete a seguir padrões de segurança e controle, sem especificar neste documento, no entanto, quais são as práticas adotadas.

> "Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais

> Nos comprometemos, em toda hipótese, com os padrões (...) de controle e segurança, respeitando os padrões exigidos."

Apesar da informação genérica da Política de Privacidade, a empresa apresenta mais informações sobre as práticas de segurança adotadas nos Sustainability Report 2018 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. Sobre o sistema, a América Móvil afirma:

> "*This is a system that manages information security within a company to efficiently safeguard important data, both financial and confidential, minimizing the risk of illegal or non-permitted access by third parties*."

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 seguinte.

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

> "Com quem a Claro compartilha dados?
> 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 que deverão observar certos cuidados, como a segurança dos seus dados. Veja quais são esses terceiros:
> 1. Empresas de *Call Center* – para que possamos realizar atendimento.
> 2. Empresas de Serviços Técnicos – para que os clientes de TV tenham seus serviços instalados ou mantidos.
> 3. Empresas que possuem pacotes de conteúdo comercializados nos canais de vendas da Claro e que precisam de algumas informações para ativarem os conteúdos e assinaturas.
> 4. Empresas de Crédito e Cobrança – para que possam realizar cobranças das faturas em aberto.
> 5. Agentes Autorizados – empresas que vendem produtos e serviços com a marca Claro, que muitas vezes são a porta de entrada dos clientes.
> 6. Parceiros de Televendas – para que façam ofertas de produtos e serviços a você, por ligações ou SMS, consultando antes se você chegou a pedir para não ser chamado.
> 7. Companhia Seguradora – a Claro recebe propostas de seguros de aparelhos celulares e compartilha seus dados com a seguradora e a corretora para fins de cobertura do

> seguro e também com terceiro para fins de cobrança do prêmio na fatura.
> 8. Empresas que operam plataformas e aplicações de recarga.
> 9. Setor público, no atendimento a fiscalizações do nosso órgão regulador e mediante requisições de autoridades policiais ou decisões judiciais.
> 10. Parceiro que faz tratamento de dados coletados dos aplicativos NET-Claro-Wi-Fi, Minha Claro e Claro Banca, como descrito mais acima."

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.

Por fim, quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi atendido, em vista dos detalhamentos de cada compartilhamento conforme trecho acima.

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. Isso porque, aproximadamente um mês depois de ter sido feito o referido pedido de acesso aos dados, por meio do e-mail dpo@claroatendimento.com.br, somente uma resposta genérica foi recebida:

> "Informamos que a política de privacidade da Claro pode ser consultada no Portal de Privacidade disponível em nosso site, no rodapé da página, esclarecemos que através do nosso site, o (a) cliente pode consultar e receber de forma automática as informações sobre os Direitos de Privacidade dos seus dados, bem como exercer os direitos de consentimento/revogação de uso de seus dados sempre que quiser.
>
> Dessa forma, pedimos que acesse o site Claro www.claro.com.br, acessar no rodapé da página o Portal de Privacidade (área logada) e escolher as opções desejadas em seus direitos de privacidade.
>
> Para não clientes da Claro, a solicitação também pode ser feita diretamente em nosso site.
>
> Por fim, informamos que a Claro já atua em conformidade com a proteção de dados de seus clientes, trabalhando

> apenas com os dados que precisa e se dedicando para protegê-los."

Nossas tentativas de acesso aos dados por meio do referido portal, no entanto, não foram frutíferas, e novas tentativas de contato pelo e-mail acima mencionado não foram respondidas.

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 se compromete a informar o usuário em eventuais modificações do documento, prevendo, inclusive, o cancelamento do consentimento para o tratamento dos dados pessoais, caso o cliente discorde das alterações.

> "Alterações na política de privacidade
> A Claro se reserva o direito de modificar esta Política de Privacidade a qualquer momento e sempre mantendo-a atualizada e disponível no site. Nesses casos, você, nosso cliente, será informado sobre as alterações realizadas, ficando você autorizado, caso venha a discordar das alterações, a cancelar o seu consentimento para tratamento dos dados pessoais."

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 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.

No entanto, as informações que constam na Política de Privacidade não são apresentadas nos contratos da Claro, 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 Claro obteve ¼ de estrela, tendo apenas cumprido parcialmente o parâmetro I.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente cumprido, pois a empresa informa apenas que se compromete a fornecer dados cadastrais a autoridades competentes, sem, no entanto, identificá-las. Em sua Política de Privacidade, a empresa informa que "em caso de pedidos judiciais, a Claro pode compartilhar seus dados pessoais com as autoridades legais, sempre obedecendo as leis existentes na época da solicitação", sem mencionar quais seriam essas autoridades. A empresa afirma, apenas, que poderá compartilhar dados com instituições de Proteção ao Crédito:

> Política de Privacidade
> "Sobre compartilhamento de dados pessoais
> Em caso de pedido judicial, a Claro pode compartilhar seus dados pessoais com as autoridades legais, sempre obedecendo as leis existentes na época da solicitação;
> Podemos enviar a instituições de Proteção ao Crédito informações específicas de nossos clientes com o objetivo de reduzir o risco de crédito e proteger pessoas e empresas de possíveis situações enganosas e fraudulentas;"

De maneira semelhante, em seu Código de Ética, a empresa afirma que as transmissões de dados só são realizadas seguindo "pedidos legais das autoridades competentes", sem, no entanto, identificá-las.

> Código de Ética
> "É estritamente proibido interferir nas comunicações ou transmissões realizadas por nossos clientes, como ouvir, manipular ou monitorar conversas, interferir em transmissões de dados ou revelar a existência ou o conteúdo das comunicações do cliente, exceto nos casos exigidos por lei e/ou seguindo pedidos legais das autoridades competentes.
> Qualquer pedido ou demanda de informações confidenciais por uma autoridade governamental deve ser encaminhado ao nosso Departamento Jurídico, para que sejam tomadas

> todas as medidas adequadas para sua proteção e assegure que todos os requisitos aplicáveis sejam cumpridos."

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."

No entanto, por mais que a empresa afirme que forneça dados apenas nas hipóteses previstas em lei e seguindo pedidos de autoridades legais, ela não identifica quais são as autoridades ou as hipóteses legais. A previsão de compartilhamento com instituições de Proteção ao Crédito é restrita, já que não menciona expressamente outras circunstâncias em que a empresa entrega dados de seus clientes.

Além disso, 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. Recomendamos que a empresa faça a distinção entre dados cadastrais e registros de conexão e identifique quais são as autoridades competentes. Diante disso, o parâmetro foi considerado apenas parcialmente atendido.

O parâmetro II, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, não foi considerado atendido. Como mencionado no parâmetro anterior, a empresa menciona em seu Código de Ética apenas que não interfere nas comunicações ou transmissões de dados, exceto "nos casos exigidos por lei e/ou seguindo pedidos legais das autoridades competentes", sem discriminar quais seriam os dispositivos legais aplicáveis ou quais seriam as autoridades competentes. Em virtude dessa falta de informações, o parâmetro não foi considerado atendido.

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 Claro.

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 foi encontrada menção ao tema nos documentos analisados da Claro.

Por fim, o parâmetro V, relativo à existência de protocolos específicos sobre entrega de dados ao estado, também 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 obteve meia estrela, pois atendeu ao parâmetro I.

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.

No entanto, na fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o Tribunal Regional Federal da 5ª região (TRF5). Nela, as empresas Claro, Vivo, TIM e Oi, mediante atuação pelo Sinditelebrasil (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal) questionaram a tentativa de alteração do Regulamento Geral de Direitos do Consumidor (RGC) pela Agência Nacional de Telecomunicações (Anatel), que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

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) 5642, da Associação Nacional das Operadoras Celulares (ACEL), não foram consideradas, já que não registraram movimentações.

Por fim, para averiguação do parâmetro II, referente à contestação de pedidos abusivos, realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado de São Paulo e no portal "Jusbrasil", em ambos os casos pelos termos "claro E sigilo E quebra" e "claro s.a. E sigilo E quebra" nos acórdãos publicados entre 01/08/2019 e 31/07/2020. 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 Claro obteve meia 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. O adiamento da entrada em vigor da Lei Geral de Proteção de Dados (LGPD) é um exemplo nesse sentido.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido. Durante as discussões no Congresso Nacional relativas ao adiamento da LGPD, além disso, não foi encontrada qualquer participação da Claro por meio de comunicados de imprensa, participação das discussões no congresso etc.

Em nossas buscas, foi localizada a notícia, divulgada pelo portal Olhar Digital, que afirmava que em novembro de 2019, houve uma falha de segurança no portal de serviços "Minha Claro Residencial" que expôs os dados pessoais (nome completo, endereço, data de nascimento, CPF, e-mail e números de telefone) dos clientes da operadora. De acordo com a reportagem, mais de 8 milhões de clientes tiveram seus dados expostos.

Em nota enviada ao portal, a Claro afirmou:

> "A Claro informa que investe constantemente em políticas e procedimentos de segurança, adotando medidas rígidas para evitar ações indevidas contra seus clientes. Sobre o fato relatado, a empresa esclarece que identificou e corrigiu rapidamente, no dia 14 de novembro, a eventual vulnerabilidade na aplicação Minha Claro Residencial e não foi identificado nenhum prejuízo aos clientes. A Claro segue padrões rígidos, que são revistos periodicamente, com mecanismos de segurança de forma a sempre garantir a privacidade de seus clientes."

A redação foi considerada excessivamente genérica e insatisfatória para os fins desse relatório.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido. Em sua Política de Privacidade, no item “A Claro, seus dados e a COVID-19”, a empresa informa:

> “A Claro, seus dados e a COVID-19
> A Claro, de forma a contribuir com soluções que pudessem aliviar um pouco os impactos da pandemia, faz parte de duas iniciativas:
> Os “mapas de calor”:
> Primeira informação importante: a Claro não identifica você e não monitora seu deslocamento. A Claro simplesmente faz a contagem da quantidade de linhas vinculadas a cada antena à noite e durante o dia, tanto para confirmar se há isolamento como se há aglomeração em alguns pontos.
> O Push do Bem: A Claro disponibilizou, para vários pequenos negócios, a possibilidade de que se cadastrem neste link. A Claro faz publicidade dessas ofertas, se o compartilhamento de geolocalização estiver autorizado por você nos apps NET-Claro Wi-Fi, Minha Claro e Claro Banca. Com isso, a Claro dá a oportunidade para que você compre de um comércio local e incentiva negócios para esses empresários”.

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

Resultado:

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

Os parâmetros I ao IV, relativos ao 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.

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 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 os parâmetros I, II, IV e V.

Embora os contratos da Net Vírtua não ofereçam informações substanciais sobre as práticas de tratamentos de dados da empresa, constatamos que algumas informações estão disponíveis no Código de Ética e na Política de Privacidade da empresa.

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 sua Política de 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 informa:

> "Informações Cadastrais
> Boa parte dos nossos serviços exige que você tenha um cadastro único com uma conta de usuário, permitindo assim, o seu acesso a todos os serviços da Claro.
> Quando você faz o seu cadastro, solicitamos: seu nome, o seu CPF, o seu RG, a sua data de nascimento, a informação de gênero e seus dados de contato, como telefone e e-mail.
>
> Perfil de Consumo
> Com o objetivo de aprimorar a sua experiência na Claro, estamos continuamente efetuando melhorias na rede, ampliando e personalizando ofertas de produtos e serviços, enviando alertas ou notificações. Para esses objetivos, a Claro poderá coletar informações de seu perfil de consumo, como: localização, recursos, dispositivos utilizados, navegação, ofertas contratadas ou pesquisadas, informações fornecidas enquanto utiliza os serviços, assim como a duração e a frequência das suas atividades".

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 "Informações Cadastrais" e "Perfil de Consumo" (vide trecho acima), informa-se que a empresa coleta informações no momento do cadastro e "enquanto utiliza o serviço".

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, considerado atendido. Na seção "Perfil de Consumo" da Política de Privacidade da Claro (vide trecho acima), a empresa informa que a coleta de dados tem como objetivo "aprimorar a sua experiência na Claro", personalização de ofertas, realização de melhorias na rede e envio de alertas e notificações. Ainda, na seção "Sobre o tratamento de dados pessoais", a empresa fornece informações detalhadas sobre as finalidades do tratamento dos dados:

> "A Claro poderá realizar o tratamento de dados pessoais coletados para as seguintes finalidades:
> Com o objetivo de garantir a sua segurança na identificação, autenticação e autorização de acesso aos nossos produtos e serviços;
> Para o melhor atendimento de suas solicitações e resolução de suas dúvidas;
> Para manter os seus dados atualizados para que possamos contatar você sempre que for preciso, seja por telefone, e-mail, SMS, mala direta ou por outros meios de comunicação;
> Para aprimorar a sua experiência na navegação em nossos sites, aplicativos e serviços;
> Para uso em estatísticas, estudos, pesquisas e levantamentos sobre suas atividades e comportamentos ao utilizar os nossos sites, aplicativos e serviços;
>
> Para divulgar os nossos serviços e os de nossos parceiros, e comunicar as novidades, funcionalidades e outras informações que possam ser relevantes para aperfeiçoar nosso relacionamento;
> Para que nos preservemos em nossos direitos e obrigações relativos à utilização dos nossos sites, aplicativos e serviços;
> Para que possamos disponibilizar a você conteúdos relevantes e enviar, por exemplo, informações sobre sua fatura, seu consumo, seu pacote e promoções, além de outras facilidades;
> Para o envio de comunicações que você concordou em receber.
> A Claro, como proprietária, é responsável por sua própria base de dados, e pode utilizar as informações dentro do limite e propósito de seu ramo de atuação. A Claro poderá ainda utilizar informações de forma anonimizada, com o objetivo de aprimorar e personalizar continuamente os serviços que prestamos a você."

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. Na seção "Quais dados a Claro coleta e como usa?" de sua Política de Privacidade, a Claro/NET detalha, 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 tráfego "são fundamentais para mensurar a qualidade dos nossos serviços, para que você possa entender a fatura e ainda para seu próprio controle", que dados bancários são utilizados "somente para efetuar a cobrança pelos serviços de telecomunicações ou outros serviços que você tenha contratado através da Claro", dentre outros.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercícios desses direitos, também foi considerado atendido. Na Política de Privacidade, há a seção "Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais", em que a empresa informa sobre a existência desses quatro direitos, por mais que não mencione todos os previstos na legislação atual. A empresa informa, também, os meios para o exercício de seus direitos: central de atendimento e Fale Conosco da Claro.

> "Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais
> Nos comprometemos, em toda hipótese, com os padrões (...) de controle e segurança, respeitando os padrões exigidos.
> Você, cliente Claro, possui os seguintes direitos, a respeito de seus dados pessoais:
> De correção de dados que possam estar incompletos, incorretos ou desatualizados;
> Você poderá cancelar o consentimento dada à Claro, a qualquer momento. Para isso, é só entrar em contato com a central de atendimento ou com o canal que disponibilizamos, o Fale Conosco Claro;
> A Claro manterá as suas informações armazenadas pelo período exigido pelas leis existentes."

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

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado parcialmente cumprido. Na sua Política de Privacidade, na seção "Por quanto tempo a Claro trata seus dados?", a empresa informa os prazos de armazenamento detalhados para cada tipo de dado coletado. No entanto, quanto aos dados cadastrais e de faturamento, a empresa informa apenas o prazo mínimo pelo qual armazena os dados. Ainda que seja positivo que a empresa estabeleça um prazo mínimo, a ausência de informações sobre o período máximo pelo qual a empresa armazena os dados de seus clientes acaba por tornar demasiado impreciso período de tempo pelo qual os dados são armazenados.

> "Por quanto tempo a Claro trata seus dados?

> 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 dos prazos que observamos são os seguintes:
> 1. Conexão à internet: a Claro armazenará os registros de conexão pelo prazo de um ano, e não guardará os registros de acesso a funcionalidades de internet;
> 2. Funcionalidades de internet: nos aplicativos próprios da Claro, os registros de acesso a funcionalidades serão armazenados por seis meses;
> 3. Dados cadastrais e de faturamento serão armazenados no mínimo por cinco anos."

Quanto ao local de armazenamento, a empresa informa nas seções "Por quanto tempo a Claro trata seus dados?" e "Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais" que os dados são processados nos datacenters da Claro, em servidores de terceiros contratados ou em "nuvens". Tais informações foram consideradas excessivamente genéricas, fornecendo poucas informações consistentes sobre o local de armazenamento.

> <u>Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais</u>
> Armazenamos os seus dados pessoais em local seguro. Muitas vezes em nossos próprios servidores, de terceiros contratados ou na "nuvem", sempre com o objetivo de melhorar nossos processos.

O sub-parâmetro (b), referente a quando/se os dados são apagados, não foi considerado atendido. Isso porque a empresa informa apenas o tempo mínimo de armazenamento dos dados.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, foi considerado atendido. Na Política de Privacidade, a empresa se compromete a seguir padrões de segurança e controle, sem especificar neste documento, no entanto, quais são as práticas adotadas.

> <u>"Sobre os direitos de acessar, corrigir, cancelar e contestar informações pessoais</u>
> Nos comprometemos, em toda hipótese, com os padrões ("modelos" para não repetir "padrões") de controle e segurança, respeitando os padrões exigidos."

Apesar da informação genérica da Política de Privacidade, a empresa apresenta mais informações sobre as práticas de segurança adotadas nos Sustainability Report 2018 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. Sobre o sistema, a América Móvil afirma:

> “This is a system that manages information security within a company to efficiently safeguard important data, both financial and confidential, minimizing the risk of illegal or non-permitted access by third parties.”

O sub-parâmetro (d), referente a quem tem acesso aos dados, também 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 atendido. A empresa informa, na seção “Com quem a Claro compartilha dados?” de sua Política de Privacidade, o seguinte:

> “Com quem a Claro compartilha dados?
> 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 que deverão observar certos cuidados, como a segurança dos seus dados. Veja quais são esses terceiros:
> 1. Empresas de Call Center – para que possamos realizar atendimento.
> 2. Empresas de Serviços Técnicos – para que os clientes de TV tenham seus serviços instalados ou mantidos.
> 3. Empresas que possuem pacotes de conteúdo comercializados nos canais de vendas da Claro e que precisam de algumas informações para ativarem os conteúdos e assinaturas.
> 4. Empresas de Crédito e Cobrança – para que possam realizar cobranças das faturas em aberto.
> 5. Agentes Autorizados – empresas que vendem produtos e serviços com a marca Claro, que muitas vezes são a porta de entrada dos clientes.
> 6. Parceiros de Televendas – para que façam ofertas de produtos e serviços a você, por ligações ou SMS, consultando antes se você chegou a pedir para não ser chamado.
> 7. Companhia Seguradora – a Claro recebe propostas de seguros de aparelhos celulares e compartilha seus dados com a seguradora e a corretora para fins de cobertura do seguro e também com terceiro para fins de cobrança do prêmio na fatura.
> 8. Empresas que operam plataformas e aplicações de recarga.
> 9. Setor público, no atendimento a fiscalizações do nosso órgão regulador e mediante requisições de autoridades policiais ou decisões judiciais.

> 10. Parceiro que faz tratamento de dados coletados dos aplicativos NET-Claro-Wi-Fi, Minha Claro e Claro Banca, como descrito mais acima."

Por fim, quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi atendido.

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. Aproximadamente um mês depois de ter sido feito o referido pedido de acesso aos dados, por meio do e-mail dpo@claroatendimento.com.br, somente uma resposta genérica foi recebida:

> "Informamos que a política de privacidade da Claro pode ser consultada no Portal de Privacidade disponível em nosso site, no rodapé da página, esclarecemos que através do nosso site, o (a) cliente pode consultar e receber de forma automática as informações sobre os Direitos de Privacidade dos seus dados, bem como exercer os direitos de consentimento/revogação de uso de seus dados sempre que quiser.
>
> Dessa forma, pedimos que acesse o site Claro (www.claro.com.br), acessar no rodapé da página o Portal de Privacidade (área logada) e escolher as opções desejadas em seus direitos de privacidade.
>
> Para não clientes da Claro, a solicitação também pode ser feita diretamente em nosso site.
>
> Por fim, informamos que a Claro já atua em conformidade com a proteção de dados de seus clientes, trabalhando apenas com os dados que precisa e se dedicando para protegê-los.".

Nossas tentativas de acesso aos dados por meio do referido portal, no entanto, não foram frutíferas, e novas tentativas de contato pelo e-mail acima mencionado não foram respondidas.

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 se compromete a informar o usuário de eventuais modificações do documento, prevendo, inclusive, o cancelamento do consentimento para o tratamento dos dados pessoais, caso o cliente discorde das alterações.

> "Alterações na política de privacidade
> A Claro se reserva o direito de modificar esta Política de Privacidade a qualquer momento e sempre mantendo-a

atualizada e disponível no site. Nesses casos, você, nosso cliente, será informado sobre as alterações realizadas, ficando você autorizado, caso venha a discordar das alterações, a cancelar o seu consentimento para tratamento dos dados pessoais."

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 Net, 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 28.07.2020

No entanto, as informações que constam na Política de Privacidade não são apresentadas nos contratos da Net, 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 Net obteve ¼ de estrela, tendo apenas cumprido parcialmente o parâmetro I.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente cumprido, pois a empresa informa apenas que se compromete a fornecer dados cadastrais a autoridades competentes, sem, no entanto, identificá-las. Em sua Política de Privacidade, a empresa informa que "em caso de pedidos judiciais, a Claro pode compartilhar seus dados pessoais com as autoridades legais, sempre obedecendo as leis existentes na época da solicitação", sem mencionar quais seriam essas autoridades. A empresa afirma, apenas, que poderá compartilhar dados com instituições de Proteção ao Crédito:

> Política de Privacidade
> "Sobre compartilhamento de dados pessoais
> Em caso de pedido judicial, a Claro pode compartilhar seus dados pessoais com as autoridades legais, sempre obedecendo as leis existentes na época da solicitação;
> Podemos enviar a instituições de Proteção ao Crédito informações específicas de nossos clientes com o objetivo de reduzir o risco de crédito e proteger pessoas e empresas de possíveis situações enganosas e fraudulentas;"

De maneira semelhante, em seu Código de Ética, a empresa afirma que as transmissões de dados só são realizadas seguindo "pedidos legais das autoridades competentes", sem, no entanto, identificá-las.

> Código de Ética
> "É estritamente proibido interferir nas comunicações ou transmissões realizadas por nossos clientes, como ouvir, manipular ou monitorar conversas, interferir em transmissões de dados ou revelar a existência ou o conteúdo das comunicações do cliente, exceto nos casos exigidos por lei e/ou seguindo pedidos legais das autoridades competentes.
> Qualquer pedido ou demanda de informações confidenciais por uma autoridade governamental deve ser encaminhado ao nosso Departamento Jurídico, para que sejam tomadas todas as medidas adequadas para sua proteção e assegure que todos os requisitos aplicáveis sejam cumpridos."

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

> Contrato de prestação de serviço de comunicação multimídia (SCM) Net Vírtua
> 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.

No entanto, por mais que a empresa afirme que forneça dados apenas nas hipóteses previstas em lei e seguindo pedidos de autoridades legais, ela não identifica quais são as autoridades ou as hipóteses legais. A previsão de compartilhamento com instituições de Proteção ao Crédito é insuficiente, já que não menciona expressamente outras circunstâncias em que a empresa entrega dados de seus clientes.

Além disso, 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. Diante disso, o parâmetro foi considerado apenas parcialmente atendido.

O parâmetro II, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, não foi considerado atendido. Como mencionado no parâmetro anterior, a empresa menciona em seu Código de Ética apenas que não interfere nas comunicações ou transmissões de dados, exceto "nos casos exigidos por lei e/ou seguindo pedidos legais das autoridades competentes", sem discriminar quais seriam os dispositivos legais aplicáveis, quais crimes ou quais seriam as autoridades competentes. Em virtude dessa falta de informações, o parâmetro não foi considerado atendido.

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 Net.

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

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

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

Nesta categoria, a Net obteve meia estrela, pois atendeu ao parâmetro I.

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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas Claro, Vivo, TIM e Oi, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

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 ADI 5642, da ACEL, não foram consideradas, já que não registraram movimentações.

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 "net E sigilo E quebra" e "claro s.a. E sigilo E quebra" e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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 NET obteve meia 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 chance de se manifestar sobre políticas públicas e projetos de lei que afetam a privacidade dos usuários. O adiamento da entrada em vigor da LGPD é um exemplo nesse sentido.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido. Durante as discussões no Congresso Nacional relativas ao adiamento da LGPD, além disso, não foi encontrada qualquer participação da NET por meio de comunicados de imprensa, participação das discussões no congresso etc.

Em nossas buscas, foi localizada a notícia, divulgada pelo portal Olhar Digital, que afirmava que em novembro de 2019, houve uma falha de segurança no portal de serviços "Minha Claro Residencial", utilizado por clientes do serviço de banda larga NET, que expôs os dados pessoais (nome completo, endereço, data de nascimento, CPF, e-mail e números de telefone) dos clientes da operadora. De acordo com a reportagem, mais de 8 milhões de clientes tiveram seus dados expostos.

Em nota enviada ao portal, a Claro afirmou:

> "A Claro informa que investe constantemente em políticas e procedimentos de segurança, adotando medidas rígidas para evitar ações indevidas contra seus clientes. Sobre o fato relatado, a empresa esclarece que identificou e corrigiu rapidamente, no dia 14 de novembro, a eventual vulnerabilidade na aplicação Minha Claro Residencial e não foi identificado nenhum prejuízo aos clientes. A Claro segue padrões rígidos, que são revistos periodicamente, com mecanismos de segurança de forma a sempre garantir a privacidade de seus clientes."

A redação foi considerada excessivamente genérica e insatisfatória para os fins desse relatório, já que não defendeu concretamente a aprovação de normas ou adoção de técnicas que pudessem fazer frente ao ocorrido.

Localizamos também uma notícia segundo a qual a Vivo, a Net e Oi teriam compartilhado, entre si, “dados pessoais de cidadãos sem cobertura específica para alavancar o número de clientes atendidos”. De acordo com a reportagem, do portal Tecmundo, a suspeita advém de relatos de usuários que, após contatarem uma das empresas e receberem negativa quanto à cobertura em sua área, foram contatados pelas outras empresas para oferecendo outros planos de internet, relatos esses confirmados por atendentes de telemarketing da empresa. Em sua resposta ao portal, a NET afirmou:

> “A NET esclarece que cumpre rigorosamente todas as leis e normas estabelecidas pela Agência Nacional de Telecomunicações (ANATEL) em relação ao atendimento de seus clientes e dos interessados em adquirir os produtos que comercializa. No entanto, está buscando mais detalhes para apurar o caso específico mencionado pelo TecMundo"

No entanto, não foram dadas explicações para os relatos dos usuários ou das confirmações pelos atendentes, nem foram defendidos concretamente medidas

que pudessem fazer frente às alegações. Por isso, a resposta da empresa foi considerada excessivamente genérica.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido. Em sua Política de Privacidade, no item "A Claro, seus dados e a COVID-19", a empresa informa:

> "A Claro, seus dados e a COVID-19
> A Claro, de forma a contribuir com soluções que pudessem aliviar um pouco os impactos da pandemia, faz parte de duas iniciativas:
> Os "mapas de calor":
> Primeira informação importante: a Claro não identifica você e não monitora seu deslocamento. A Claro simplesmente faz a contagem da quantidade de linhas vinculadas a cada antena à noite e durante o dia, tanto para confirmar se há isolamento como se há aglomeração em alguns pontos.
> O Push do Bem: A Claro disponibilizou, para vários pequenos negócios, a possibilidade de que se cadastrem neste link. A Claro faz publicidade dessas ofertas, se o compartilhamento de geolocalização estiver autorizado por você nos apps NET-Claro Wi-Fi, Minha Claro e Claro Banca. Com isso, a Claro dá a oportunidade para que você compre de um comércio local e incentiva negócios para esses empresários".

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

Resultado: ☆

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

Os parâmetros I ao IV, relativos ao 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.

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 ¾ de estrela, pois atendeu aos parâmetros I e V e parcialmente aos parâmetros II e IV.

A Oi atende ao parâmetro I, tendo cumprido todos os sub-parâmetros.

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

> Que dados coletamos:
> Coletamos seus dados quando você os informa de forma voluntária. Mas também automaticamente, quando acessa nossos sites, usa nossos serviços ou interage com a gente. Por exemplo, coletamos dados como nome, e-mail, endereço, gênero, nacionalidade e números de telefone e de documentos, entre outros. Mas também informações financeiras, como dados bancários, números de boleto e informações do seu cartão de crédito ou débito.
>
> Além dessas informações, dados de atendimento, estatísticos, de consumo dos seus planos, de localização (quando você ativa o GPS no seu celular) e a forma como você usa o nosso site e os aplicativos também são coletados pela Oi.

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

> 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 “Que dados coletados” do Portal de Privacidade (vide trecho acima), informa-se que os dados são coletados ao acessar o site, nos usos dos serviços da empresa, ao ativar o GPS do celular e pelo uso do site e dos aplicativos. Na Política de Privacidade, especifica-se a coleta de dados de uso dos produtos e serviços contratados, históricos de chamada, dados de atendimento, transações de recarga, 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, foi considerado cumprido. Na seção “Por que motivo usamos seus dados pessoais” do Portal de Privacidade, a empresa informa que coleta os dados para “prestar os serviços que você contratou”. Informa também que utiliza os dados para prevenir fraudes, criar ofertas de acordo com o perfil do cliente e “aperfeiçoar” a experiência do usuário, tanto no site quanto nos aplicativos.

POR QUE MOTIVO USAMOS SEUS DADOS PESSOAIS

Na maioria das vezes, para poder prestar os serviços que você contratou. Mas também para melhorar constantemente a qualidade de nossos produtos, prevenir fraudes, criar ofertas de acordo com o seu perfil e aperfeiçoar a sua experiência quando usa o nosso site ou aplicativos.

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.

Finalidade do tratamento	Dados tratados	Base legal
• 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.	• Dados de cadastro e contrato • Informações financeiras • Dados de tráfego • Dados de atendimento • Número ICCID (Cartão SIM)	• Execução de contrato
• 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.	• Dados de atendimento • Dados estatísticos • Informações financeiras • Dados de localização • Dados de tráfego	• Legítimo interesse
• Prevenção de fraude, uso fraudulento dos serviços Oi e demais medidas que promovam a segurança do usuário na fruição dos serviços contratados.	• Dados de cadastro e contrato • Informações financeiras • Dados de tráfego • Dados de localização • Número ICCID (Cartão SIM)	• Prevenção à fraude e à segurança do titular • Legítimo interesse
• Inovação e evolução dos serviços, de acordo com o nível de serviço prestado aos usuários.	• Dados de localização • Dados sobre o modo de uso do site e aplicativos • Dados de atendimento • Dados de tráfego	• Legítimo interesse

captura de tela de 26.10.2020.

• 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.		
• 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.	• Dados de cadastro e contrato • Dados sobre modo de uso do site e aplicativos • Dados de tráfego • Dados de localização	• Legítimo interesse
• 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.	• Dados de cadastro e contrato • Dados sobre modo de uso do site e aplicativos • Dados de tráfego • Dados de localização	• Legítimo interesse
• 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.	• Dados de cadastro e contrato • Dados de atendimento • Informações financeiras • Dados de tráfego • Dados de localização	• Cumprimento de obrigação legal ou regulatória
• Efetuar, exercer ou defender ações judiciais. • Resposta a ofícios e cumprimento de liminares. • Defesa em processos administrativos, relacionados aos órgãos de defesa do consumidor.	• Dados de cadastro e contrato • Dados de atendimento • Informações financeiras • Dados de tráfego	• Exercício regular de direitos

captura de tela de 26.10.2020.

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. Consideramos positiva que a forma como a empresa específica tais informações.

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. 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 exercícios desses direitos, também foi considerado atendido. 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 LGPD (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.

A Oi Banda Larga atende parcialmente ao parâmetro II, tendo atendido ao sub-parâmetro (e), e parcialmente ao sub-parâmetro (c).

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, não foi considerado cumprido. Quanto ao tempo de armazenamento, a empresa informa, na seção "retenção e término do tratamento dos dados pessoais" da Política de Privacidade, apenas que os dados são mantidos por tempo "estritamente necessário para o cumprimento de obrigação legal e regulatório após o cumprimento do contrato", sem fornecer, no entanto, maiores informações. A empresa não estabelece prazos mínimos ou máximos pelo qual a empresa 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, 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 não estabelece de maneira clara quando os dados são apagados. 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.

Quanto ao sub-parâmetro (c), referente a quais práticas de segurança a empresa observa, considerou-se que foi parcialmente atendido. Na cláusula 11.3 do

Contrato de Adesão à Banda Larga, 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. Em seu Relatório de Sustentabilidade (p. 31), a empresa afirma que as ações de segurança aplicadas às informações dos clientes são baseadas em "normas legais aplicáveis" e "padrões de tecnologia da rede e conscientização da equipe".

> "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."
>
> "Ações de segurança das informações de clientes trafegadas na Companhia são baseadas nas normas legais aplicáveis e buscam definir padrões de tecnologia da rede e de conscientização da equipe, principalmente, nas áreas de negócio, tecnologia da informação e engenharia.
> O fluxo de aprovações avaliará a necessidade de o usuário ter acesso ou não ao grupo de informações trafegadas. A gestão da segurança da informação garante os requisitos mínimos de segurança em pesquisa e desenvolvimento de produtos, bem como nos testes anteriores à entrada em produção, e atua na disponibilização de informações de clientes (p. 31)."

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.

Tais informações constantes nos dois documentos são demasiado vagas e trazem poucas garantias aos clientes sobre as práticas adotadas pela empresa. A empresa não informa, por exemplo, quais padrões de segurança adota, quais protocolos segue, se utiliza criptografia na transferência dos dados pessoais dos dispositivos dos usuários ou quais são os princípios de segurança da informação que segue. No entanto, por haver preocupação em mencionar o tema, o parâmetro foi considerado parcialmente atendido.

O sub-parâmetro (d), referente a quem tem acesso aos dados, não foi considerado cumprido. Na seção "Segurança da informação" (vide trecho acima), a empresa informa apenas que adota medidas 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 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

Por fim, quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se atendido. A Política de Privacidade informa a finalidade de algumas hipóteses de compartilhamento de dados (vide trecho acima), como por exemplo, por obrigação legal, para reduzir o risco de crédito e uso fraudulento, em casos de inadimplência e em razão de reestruturação societária.

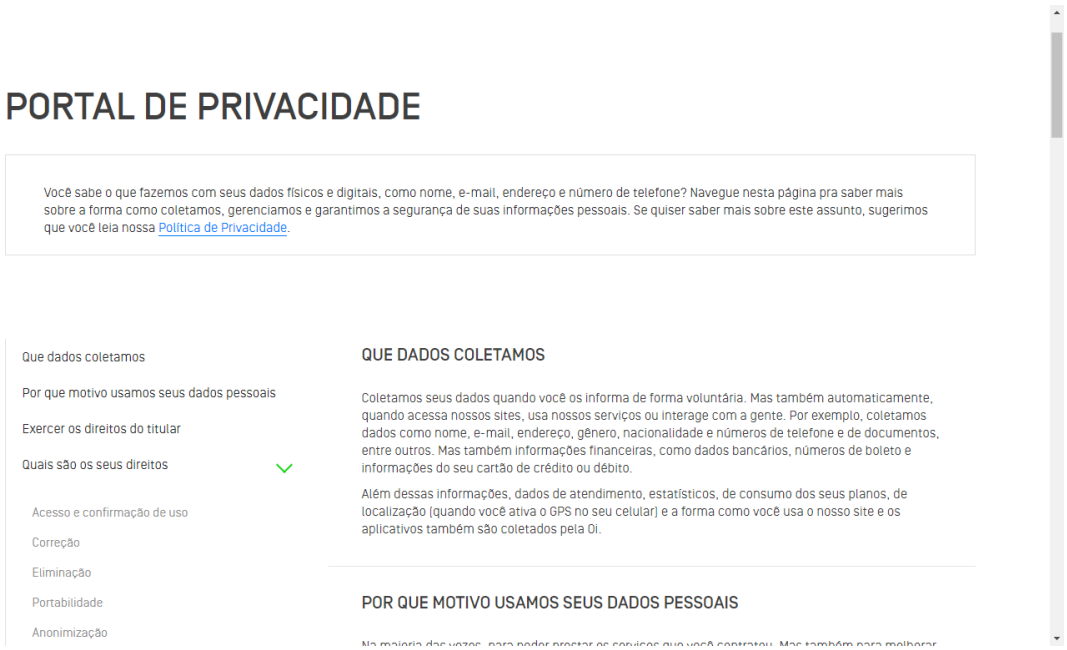
O parâmetro III, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, não foi considerado cumprido. Em solicitação feita pelo e-mail ouvidoria@oi.net.br, obtivemos como resposta da empresa que "a operadora não fornece dados pessoais, por vias normais", que esse pedido era atendido apenas mediante pedido judicial.

O parâmetro IV, que avalia se a empresa promete enviar notificações ao usuário na hipótese de atualização de suas políticas de privacidade, foi considerado parcialmente atendido. Em sua Política de Privacidade a empresa afirma que caso de alterações no documento, a empresa divulgará "imediatamente através de aviso em destaque na página inicial" do site e em outros canais de comunicação. Ainda que a empresa não se comprometa a enviar notificações ao usuário, consideramos positivo o esforço de comunicação e, por isso, o parâmetro foi considerado parcialmente atendido. No entanto, ressaltamos que é recomendado que a empresa envie notificações ao usuário na hipótese de atualização de suas políticas, visto que o encargo de se manter atualizado não pode recair apenas no usuário.

> 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.

Por fim, o parâmetro V, referente à acessibilidade das informações sobre privacidade e proteção de dados, também foi considerado cumprido. Isso porque a Oi dispõe de um Portal de Privacidade, mencionado acima, com informações claras sobre o tema. O portal pode ser facilmente acessado no final da página inicial da Oi.



captura de tela de 26.10.2020

As informações do Portal de Privacidade encontram-se mais detalhadas na Política de Privacidade da empresa. Importante ressaltar, no entanto, que as informações sobre o compartilhamento de dados pessoais não constam no Portal de Privacidade, estando restritas à Política de Privacidade. Recomendamos que tais dados estejam presentes, também, no Portal, para fins de uma maior transparência.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Oi Banda Larga obteve ¼ de estrela, pois atendeu parcialmente aos parâmetros I e IV.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente cumprido. No Contrato de Adesão à Banda Larga, na cláusula 11, que dispõe sobre as obrigações da Oi, a

empresa se compromete a fornecer dados cadastrais apenas a autoridades administrativas competentes

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

Em sua Política de Privacidade, a empresa afirma compartilhar dados com autoridades governamentais, como "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". 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. Apesar de a empresa identificar as autoridades, a redação foi considerada insatisfatória e por isso o parâmetro foi considerado parcialmente cumprido.

> Política de privacidade:
> 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:
> - 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

Ainda, 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 ou na Política de Privacidade.

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 ou na Política de Privacidade.

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. A Oi Banda Larga prevê no contrato 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).

> "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 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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas Oi, Vivo, TIM e Claro, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do

comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a Ação Direta de Inconstitucionalidade (ADI) 5642, da ACEL, não foram tomadas em consideração nessa versão, já que não registraram movimentações.

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 01/08/2019 e 31/07/2020, e foram localizadas duas ações nesse sentido: o HC 2205750-04.2019.8.26.0000, no Tribunal de Justiça de São Paulo, e HC 5575105.48.2019.8.09.0000, no Tribunal de Justiça do Estado de Goiás. Em ambas ações, a empresa questiona ordens judiciais para senha de acesso, dados cadastrais, registros de conexão e dados de localização, genéricas e carentes fundamentação idôneas a específicas. 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.

Em fase de engajamento, a empresa informou ao InternetLab — com a devida supressão dos dados pessoais das partes — processos em que a empresa contestou pedido de quebra de sigilo de dados que afetaria usuários que não tinham nenhuma relação com os fatos investigados.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Oi Banda Larga obteve ½ de 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. O adiamento da entrada em vigor da LGPD é um exemplo nesse sentido.

Em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido. Durante as discussões no Congresso Nacional relativas ao adiamento da LGPD, além disso, não foi encontrada qualquer participação da Oi por meio de comunicados de imprensa, participação das discussões no congresso etc.

Na fase de engajamento, a Oi informou ao InternetLab algumas iniciativas da empresa, noticiadas publicamente, para adequação à LGPD (1, 2, 3, 4). Ainda que o esforço para a adequação à Lei seja positivo, a postura não foi considerada satisfatória para a avaliação do parâmetro. Isto porque a atuação da empresa foi restrita ao cumprimento legal, não assumindo uma postura claramente pró-privacidade ou defendendo concretamente a aprovação de normas ou adoção de técnicas que aumentem a proteção dos usuários, para além do que já está previsto em lei.

Vale ressaltar, ainda, que em seu Relatório de Sustentabilidade, a Oi afirma que, em parceria com a SindiTelebrasil, participou da discussão de projetos de lei no âmbito federal e também em medidas provisórias que dispõe sobre proteção de dados. No entanto, não menciona em quais foram os projetos de lei ou quais foram os posicionamentos adotados pela empresa e, em nossas buscas, não encontramos nenhum documento ou notícia que indique a participação da empresa nessas discussões.

> Discussões importantes sobre a legislação federal do setor de telecomunicações aconteceram em 2018. Em parceria com o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal (SindiTelebrasil), participamos da discussão de diversos projetos de lei no âmbito federal, entre eles: (...) Medidas Provisórias de interesse do setor de telecomunicações, especialmente aquelas que trataram de matéria tributária e da proteção de dados pessoais. (p. 39)

Ademais, também foi localizada notícia segundo a qual a Vivo, a Net e Oi teriam compartilhado, entre si, "dados pessoais de cidadãos sem cobertura específica para alavancar o número de clientes atendidos". De acordo com a reportagem, do portal Tecmundo, a suspeita advém de relatos de usuários que, após contatarem uma das empresas e receberem negativa quanto à cobertura em sua área, foram contatados pelas outras empresas para oferecendo outros planos de internet, relatos esses confirmados por atendentes de telemarketing da empresa. Em sua resposta ao portal, a Oi afirmou:

> "A Oi informa que segue a Legislação vigente em relação aos serviços de telemarketing e que preserva o sigilo dos dados pessoais de seus clientes. A companhia acrescenta que vai averiguar o caso relatado pelo veículo".

No entanto, não foram dadas explicações para os relatos dos usuários ou das confirmações pelos atendentes, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. Por isso, a resposta da empresa foi considerada excessivamente genérica e insatisfatória para os fins desse relatório.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido.

A Oi, bem como demais empresas de telecomunicações, comprometeu-se a fornecer os dados de geolocalização das linhas móveis ao Ministério da Ciência, Tecnologia, Inovação e Comunicação (MCTIC). Em uma seção do site criada especificamente para tratar das medidas adotadas pela empresa no enfrentamento da pandemia de COVID-19, a Oi afirma que os dados fornecidos ao MCTIC visam apenas o combate à pandemia e os dados serão organizados de forma agregada e anônima, nos termos da LGPD e do Marco Civil da Internet. Vale ressaltar, no entanto, que a empresa não especifica quais foram as práticas e técnicas de segurança adotadas para garantir a anonimização dos dados compartilhados.

> "As principais operadoras de telefonia móvel, atuando em parceria, estão oferecendo ao MCTIC uma solução única de dados para monitorar mobilidade populacional, deslocamentos, pontos de aglomeração e identificar situações de concentração de pessoas e risco de contaminação pelo novo coronavírus. As operadoras - Algar Telecom, Claro, Oi, Tim e Vivo - vão fornecer os dados de mobilidade originados pelos celulares nas redes móveis ao MCTIC, que possui uma sala de acompanhamento do tema e poderá disponibilizar as informações a todas as esferas do poder público. Os dados fornecidos visam exclusivamente o combate ao covid-19.
>
> Nessa solução, os dados estarão em nuvem pública (Data Lake) e organizados de forma agregada, estatísticos e anônima, de acordo com as normas da Lei Geral de Proteção de Dados (LGPD) e do Marco Civil da Internet. As operadoras desenvolverão ainda aplicativos e casos de uso para auxiliar os órgãos públicos no mapeamento da evolução da epidemia do novo coronavírus. A iniciativa poderá evoluir também para convidar outras empresas, universidades e startups para participar, agregando mais dados anonimizados e estatísticos ao Data Lake, ou até para o desenvolvimento de outros aplicativos e casos de uso."

Ademais, a empresa também se posicionou acerca da Medida Provisória 954/2020, que obrigava as empresas de telecomunicações a compartilharem dados de seus clientes com o Instituto Brasileiro de Geografia e Estatística (IBGE), "para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19)". A eficácia da MP, contudo, foi suspensa pelo Supremo Tribunal Federal no julgamento das ADIs 6.387, 6.388, 6.389, 6.390 e 6.393.
Em um evento organizado pela TeleTime e Mobile Time, "As telecomunicações em tempos de incertezas: quatro perspectivas", o Oi defendeu a entrega de dados ao IBGE mediante assinatura de termos de responsabilidade:

> “Vamos ter que entregar ao IBGE, mas mediante a assinatura de algum termo de responsabilidade. Mesmo com a MP, a gente entende que deveria haver um recibo, e a partir daí, toda a instrução de uso e, depois, destruição da informação. (...) O que é público, já fornecemos. O que é privado, e neste caso é de forma massiva, está advindo por meio de ato de força da MP, e a gente ainda não tem desfecho disso. É uma informação recente, e tem o prazo de sete dias, apesar de alguns outros fatores correndo paralelamente”

Enaltecemos a postura do Oi pela participação na discussão sobre a MP 954/2020 e consideramos que as declarações no evento, bem como as informações que constam no site da empresa, configuram uma postura pública pró-privacidade no contexto da pandemia de COVID-19.

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, a cada dois anos, Relatórios de Sustentabilidade; no entanto, o documento não traz informações significativas sobre privacidade e proteção de dados.

Na página 31 do Relatório de Sustentabilidade 2018, consta a informação de que em 2018 foram recebidas 694 reclamações pelos canais da Anatel sobre utilização indevida de dados cadastrais. Em 2017 esse número era de 819 e em 2016 de 983. Na página 62, a empresa afirma que o número total de queixas comprovadas relativas à violação de privacidade e perda de dados de clientes foi de 31 casos.

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 ¾ de estrela, pois atendeu aos parâmetros I e V e parcialmente aos parâmetros II e IV. Embora os contratos de telefonia ofereçam poucas informações sobre as práticas de tratamentos de dados da empresa, constatamos que algumas informações estão disponíveis Portal de Privacidade, no website da Oi e na Política de privacidade.

A Oi atende ao parâmetro I, tendo cumprido todos os sub-parâmetros.

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

> Que dados coletamos:
> Coletamos seus dados quando você os informa de forma voluntária. Mas também automaticamente, quando acessa nossos sites, usa nossos serviços ou interage com a gente. Por exemplo, coletamos dados como nome, e-mail, endereço, gênero, nacionalidade e números de telefone e de documentos, entre outros. Mas também informações financeiras, como dados bancários, números de boleto e informações do seu cartão de crédito ou débito.
>
> Além dessas informações, dados de atendimento, estatísticos, de consumo dos seus planos, de localização (quando você ativa o GPS no seu celular) e a forma como você usa o nosso site e os aplicativos também são coletados pela Oi.

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

> 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 “Que dados coletados” do Portal de Privacidade (vide trecho acima), informa-se que os dados são coletados ao acessar o site, nos usos dos serviços da empresa, ao ativar o GPS do celular e pelo uso do site e dos aplicativos. Na Política de Privacidade, especifica-se a coleta de dados de uso dos produtos e serviços contratados, históricos de chamada, dados de atendimento, transações de recarga, 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, foi considerado cumprido. Na seção “Por que motivo usamos seus dados pessoais” do Portal de Privacidade, a empresa informa que coleta os dados para “prestar os serviços que você contratou”. Informa também que utiliza os dados para prevenir fraudes, criar ofertas de acordo com o perfil do cliente e “aperfeiçoar” a experiência do usuário, tanto no site quanto nos aplicativos.

2020

POR QUE MOTIVO USAMOS SEUS DADOS PESSOAIS
Na maioria das vezes, para poder prestar os serviços que você contratou. Mas também para melhorar constantemente a qualidade de nossos produtos, prevenir fraudes, criar ofertas de acordo com o seu perfil e aperfeiçoar a sua experiência quando usa o nosso site ou aplicativos.

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

Finalidade do tratamento	Dados tratados	Base legal
• 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.	• Dados de cadastro e contrato • Informações financeiras • Dados de tráfego • Dados de atendimento • Número ICCID (Cartão SIM)	• Execução de contrato
• 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.	• Dados de atendimento • Dados estatísticos • Informações financeiras • Dados de localização • Dados de tráfego	• Legítimo interesse
• Prevenção de fraude, uso fraudulento dos serviços Oi e demais medidas que promovam a segurança do usuário na fruição dos serviços contratados.	• Dados de cadastro e contrato • Informações financeiras • Dados de tráfego • Dados de localização • Número ICCID (Cartão SIM)	• Prevenção à fraude e à segurança do titular • Legítimo interesse
• Inovação e evolução dos serviços, de acordo com o nível de serviço prestado aos usuários.	• Dados de localização • Dados sobre o modo de uso do site e aplicativos • Dados de atendimento • Dados de tráfego	• Legítimo interesse

captura de tela de 26.10.2020.

• 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.		
• 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.	• Dados de cadastro e contrato • Dados sobre modo de uso do site e aplicativos • Dados de tráfego • Dados de localização	• Legítimo interesse
• 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.	• Dados de cadastro e contrato • Dados sobre modo de uso do site e aplicativos • Dados de tráfego • Dados de localização	• Legítimo interesse
• 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.	• Dados de cadastro e contrato • Dados de atendimento • Informações financeiras • Dados de tráfego • Dados de localização	• Cumprimento de obrigação legal ou regulatória
• Efetuar, exercer ou defender ações judiciais. • Resposta a ofícios e cumprimento de liminares. • Defesa em processos administrativos, relacionados aos órgãos de defesa do consumidor.	• Dados de cadastro e contrato • Dados de atendimento • Informações financeiras • Dados de tráfego	• Exercício regular de direitos

captura de tela de 26.10.2020.

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. Consideramos positiva que a forma como a empresa específica tais informações.

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. 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 exercícios desses direitos, também foi considerado atendido. 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.

A Oi Banda Larga atende parcialmente ao parâmetro II, tendo atendido ao sub-parâmetro (e), e parcialmente ao sub-parâmetro (c).

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, não foi considerado cumprido. Quanto ao tempo de armazenamento, a empresa informa, na seção "retenção e término do tratamento dos dados pessoais" da Política de Privacidade, apenas que os dados são mantidos por tempo "estritamente necessário para o cumprimento de obrigação legal e regulatório após o cumprimento do contrato", sem, no entanto, fornecer maiores informações. A empresa não estabelece prazos mínimos pelo qual a empresa 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, 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 não estabelece de maneira clara quando os dados são apagados. 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.

Quanto ao sub-parâmetro (c), referente a quais práticas de segurança observa, considerou-se que foi parcialmente 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. Em seu Relatório de Sustentabilidade (p. 31), a empresa afirma que as ações de segurança aplicadas às informações dos clientes são baseadas em "normas legais aplicáveis" e "padrões de tecnologia da rede e conscientização da equipe".

> "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."
>
> "Ações de segurança das informações de clientes trafegadas na Companhia são baseadas nas normas legais aplicáveis e buscam definir padrões de tecnologia da rede e de conscientização da equipe, principalmente, nas áreas de negócio, tecnologia da informação e engenharia.
> O fluxo de aprovações avaliará a necessidade de o usuário ter acesso ou não ao grupo de informações trafegadas. A gestão da segurança da informação garante os requisitos mínimos de segurança em pesquisa e desenvolvimento de produtos, bem como nos testes anteriores à entrada em produção, e atua na disponibilização de informações de clientes (p. 31)."

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.

Tais informações constantes nos dois documentos são demasiado vagas e trazem poucas garantias aos clientes sobre as práticas adotadas pela empresa. A empresa não informa, por exemplo, quais padrões de segurança adota, quais protocolos segue, se utiliza criptografia na transferência dos dados pessoais dos dispositivos dos usuários ou quais são os princípios de segurança da informação que segue. No entanto, por haver preocupação em mencionar o tema, o parâmetro foi considerado parcialmente atendido.

O sub-parâmetro (d), referente a quem tem acesso aos dados, não foi considerado cumprido. Na seção "Segurança da informação" (vide trecho acima), a empresa informa apenas que adota medidas 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 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

Por fim, quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se atendido. A Política de Privacidade informa, algumas hipóteses a finalidade com compartilhamento de dados (vide trecho acima), como por exemplo, por obrigação legal, para reduzir o risco de crédito e uso fraudulento, em casos de inadimplência e em razão de reestruturação societária.

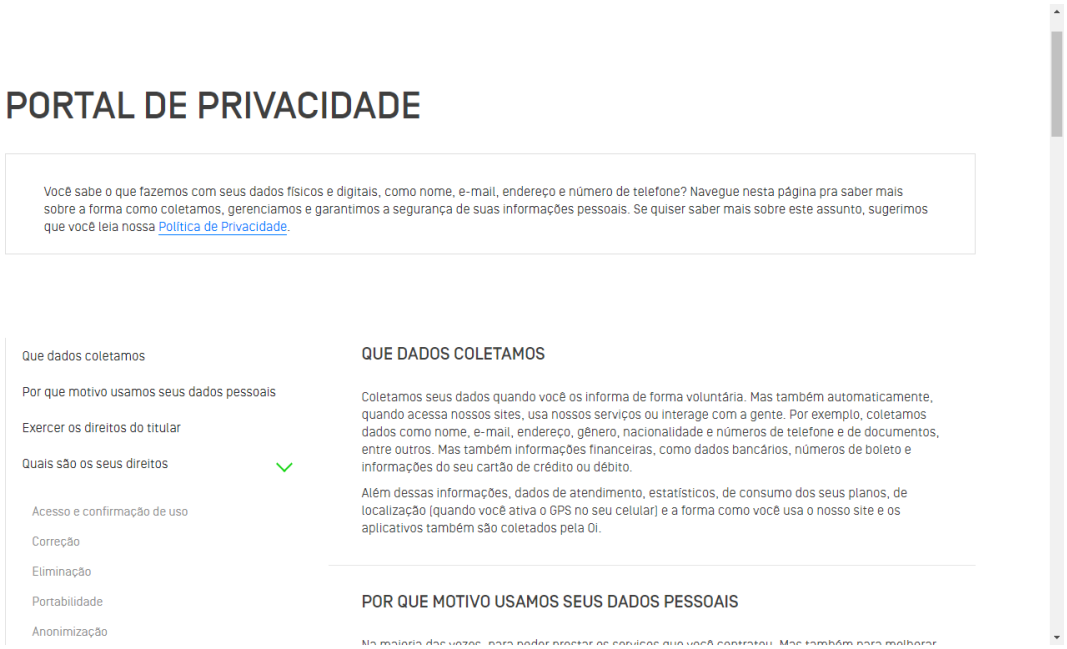
O parâmetro III, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, não foi considerado cumprido. Em solicitação feita pelo e-mail ouvidoria@oi.net.br, obtivemos como resposta da empresa que “a operadora não fornece dados pessoais, por vias normais”, e que esse pedido era atendido apenas mediante pedido judicial.

O parâmetro IV, que avalia se a empresa promete enviar notificações ao usuário na hipótese de atualização de suas políticas de privacidade, foi considerado parcialmente atendido. Em sua Política de Privacidade a empresa afirma que caso de alterações no documento, a empresa divulgará “imediatamente através de aviso em destaque na página inicial” do site e em outros canais de comunicação. Ainda que a empresa não se comprometa a enviar notificações ao usuário, consideramos positivo o esforço de comunicação e, por isso, o parâmetro foi considerado parcialmente atendido. No entanto, ressaltamos que é recomendado que a empresa envie notificações ao usuário na hipótese de atualização de suas políticas, visto que o encargo de se manter atualizado não pode recair apenas no usuário.

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.

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, mencionado acima, com informações claras sobre o tema. O portal pode ser facilmente acessado ao final da página inicial da Oi.



captura de tela de 26.10.2020.

As informações do Portal de Privacidade encontram-se mais detalhadas na Política de Privacidade da empresa. Importante ressaltar, no entanto, que as informações sobre o compartilhamento de dados pessoais não constam no Portal de Privacidade, estando restritas à Política de Privacidade. Recomendamos que tais dados estejam presentes, também, no Portal, para fins de uma maior transparência.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

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

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente atendido. No Contrato de Serviço Móvel Pessoal Pós-Pago, na cláusula 16, a empresa se compromete a fornecer dados cadastrais apenas a autoridades administrativas competentes.

> "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."

Em sua Política de Privacidade, a empresa afirma compartilhar dados com autoridades "governamentais", como "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". 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. Apesar de a empresa identificar as autoridades, a redação foi considerada insatisfatória e por isso o parâmetro foi considerado parcialmente cumprido.

> "Política de privacidade:
> 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:
> - 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."

Ainda, 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 ou na Política de Privacidade.

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 ou na Política de Privacidade.

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. 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). No entanto, por diferenciar a entrega de registros de conexão e de acesso a aplicações de internet, o parâmetro foi considerado parcialmente cumprido.

> "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, pois atendeu aos dois 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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas Oi, Vivo, TIM e Claro, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido

regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

Ações consideradas nas versões anteriores do Quem Defende Seus Dados, como a ADI 5642, da ACEL, não foram consideradas, já que não registraram movimentações.

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 01/08/2019 e 31/07/2020, e foram localizadas duas ações nesse sentido: o HC 2205750-04.2019.8.26.0000, no Tribunal de Justiça de São Paulo, e HC 5575105.48.2019.8.09.0000, no Tribunal de Justiça do Estado de Goiás. Em ambas ações, a empresa questiona ordens judiciais para senha de acesso, dados cadastrais, registros de conexão e dados de localização, genéricas e carentes fundamentação idôneas a específicas. 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.

Em fase de engajamento, a empresa informou ao InternetLab — com a devida supressão dos dados pessoais das partes — processos em que a empresa contestou pedidos de quebra de sigilo de dados que afetariam usuários que não tinham nenhuma relação com os fatos investigados.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Oi Móvel obteve ½ de 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. O adiamento cogitado para a entrada em vigor da LGPD é um exemplo nesse sentido.

Em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido. Durante as discussões no Congresso Nacional relativas ao adiamento da LGPD,

além disso, não foi encontrada qualquer participação da Oi por meio de comunicados de imprensa, participação das discussões no congresso etc.

Na fase de engajamento, a Oi informou ao InternetLab algumas iniciativas da empresa, noticiadas publicamente, para adequação à LGPD (1, 2, 3, 4). Ainda que o esforço para a adequação à Lei seja extremamente positivo, a postura não foi considerada satisfatória para a avaliação do parâmetro. Isto porque a atuação da empresa foi restrita ao cumprimento legal, não defendendo concretamente a aprovação de normas ou adoção de técnicas que aumentem a proteção dos usuários, para além do que já está previsto em lei.

Vale ressaltar, ainda, que em seu Relatório de Sustentabilidade, a Oi afirma que, em parceria com a SindiTelebrasil, participou da discussão de projetos de lei no âmbito federal e também em medidas provisórias que dispõem sobre proteção de dados. No entanto, não menciona em quais foram os projetos de lei ou quais foram os posicionamentos defendidos pela empresa e, em nossas buscas, não encontramos nenhum documento ou notícia que indique a participação da empresa nessas discussões.

> Discussões importantes sobre a legislação federal do setor de telecomunicações aconteceram em 2018. Em parceria com o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal (SindiTelebrasil), participamos da discussão de diversos projetos de lei no âmbito federal, entre eles: (...) Medidas Provisórias de interesse do setor de telecomunicações, especialmente aquelas que trataram de matéria tributária e da proteção de dados pessoais. (p. 39)

Ademais, também foi localizada notícia segundo a qual a Vivo, a Net e Oi teriam compartilhado, entre si, “dados pessoais de cidadãos sem cobertura específica para alavancar o número de clientes atendidos”. De acordo com a reportagem, do portal Tecmundo, a suspeita advém de relatos de usuários que, após contatarem uma das empresas e receberem negativa quanto à cobertura em sua área, foram contatados pelas outras empresas para oferecendo outros planos de internet, relatos esses confirmados por atendentes de telemarketing da empresa. Em sua resposta ao portal, a Oi afirmou:

> “A Oi informa que segue a Legislação vigente em relação aos serviços de telemarketing e que preserva o sigilo dos dados pessoais de seus clientes. A companhia acrescenta que vai averiguar o caso relatado pelo veículo”.

No entanto, não foram dadas explicações para os relatos dos usuários ou das confirmações pelos atendentes, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. Por isso, a resposta da empresa foi considerada excessivamente genérica e insatisfatória para os fins desse relatório.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido.

A Oi, bem como demais empresas de telecomunicações, comprometeu-se a fornecer os dados de geolocalização das linhas móveis ao MCTIC. Em uma seção do site criada especificamente para tratar das medidas adotadas pela empresa no enfrentamento da pandemia de COVID-19, a Oi afirma que os dados fornecidos ao MCTIC visam apenas o combate à pandemia e os dados serão organizados de forma agregada e anônima, nos termos da LGPD e do Marco Civil da Internet. Vale ressaltar, no entanto, que a empresa não especifica quais foram as práticas e técnicas de segurança adotadas para garantir a anonimização dos dados compartilhados.

> "As principais operadoras de telefonia móvel, atuando em parceria, estão oferecendo ao MCTIC uma solução única de dados para monitorar mobilidade populacional, deslocamentos, pontos de aglomeração e identificar situações de concentração de pessoas e risco de contaminação pelo novo coronavírus. As operadoras - Algar Telecom, Claro, Oi, Tim e Vivo - vão fornecer os dados de mobilidade originados pelos celulares nas redes móveis ao MCTIC, que possui uma sala de acompanhamento do tema e poderá disponibilizar as informações a todas as esferas do poder público. Os dados fornecidos visam exclusivamente o combate ao covid-19.
>
> Nessa solução, os dados estarão em nuvem pública (Data Lake) e organizados de forma agregada, estatísticos e anônima, de acordo com as normas da Lei Geral de Proteção de Dados (LGPD) e do Marco Civil da Internet. As operadoras desenvolverão ainda aplicativos e casos de uso para auxiliar os órgãos públicos no mapeamento da evolução da epidemia do novo coronavírus. A iniciativa poderá evoluir também para convidar outras empresas, universidades e *startups* para participar, agregando mais dados anonimizados e estatísticos ao Data Lake, ou até para o desenvolvimento de outros aplicativos e casos de uso."

Ademais, a empresa também se posicionou acerca da Medida Provisória 954/2020 que obrigava as empresas de telecomunicações a compartilharem dados de seus clientes com o IBGE, "para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19)". A eficácia da MP, contudo, foi suspensa pelo Supremo Tribunal Federal no julgamento das ADIs 6.387, 6.388, 6.389, 6.390 e 6.393.

No evento organizado pela TeleTime e MobileTime, "As telecomunicações em tempos de incertezas: quatro perspectivas", a Oi defendeu a entrega de dados ao IBGE mediante assinatura de termos de responsabilidade:

> “Vamos ter que entregar ao IBGE, mas mediante a assinatura de algum termo de responsabilidade. Mesmo com a MP, a gente entende que deveria haver um recibo, e a partir daí, toda a instrução de uso e, depois, destruição da informação. (...) O que é público, já fornecemos. O que é privado, e neste caso é de forma massiva, está advindo por meio de ato de força da MP, e a gente ainda não tem desfecho disso. É uma informação recente, e tem o prazo de sete dias, apesar de alguns outros fatores correndo paralelamente”

Enaltecemos a postura do Oi pela participação na discussão sobre a MP 954/2020 e consideramos que as declarações no evento, bem como as informações que constam no site da empresa, configura uma postura pública pró-privacidade, no contexto da pandemia de COVID-19.

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

Resultado:

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

Os parâmetros I ao IV, relativo 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, a cada dois anos, Relatórios de Sustentabilidade; no entanto, o documento não traz informações significativas sobre privacidade e proteção de dados.

Na página 31 do Relatório de Sustentabilidade 2018, há a informação de que em 2018 foram recebidas 694 reclamações pelos canais da Anatel sobre utilização indevida de dados cadastrais. Em 2017 esse número era de 819 e em 2016 de 983. Na página 62, a empresa afirma que o número total de queixas comprovadas relativas à violação de privacidade e perda de dados de clientes foi de 31 casos.

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 a todos os parâmetros.

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, no item "Que tipo de Dados e com qual finalidade a TIM trata", a empresa especifica a origem, o tipo de dado coletado, a finalidade e a base legal de tratamento de diversos dados pessoais processados por ela. Dentre outros, informa 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: e-mail, 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 locacionais (país, cidade e estado) de onde ocorreu o acesso ou onde a ligação está ocorrendo; registros de telefonia e de envio de SMS e MMS; desempenho da rede e da infraestrutura de telecomunicações Dados sobre pagamento: números e dados de cartão de crédito, transações de recargas, informações bancárias necessárias para prestação de serviços; informações de crédito para os sistemas de tarifação e emissão de faturas. 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 Os dados dos Clientes TIM serão utilizados apenas para prestação do Serviço de Comunicação Multimídia, serviços acessórios a este Contrato e melhoria dos serviços."

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, considerou-se que foi atendido, tendo sido somente o sub-parâmetro (a) considerado parcialmente atendido e os sub-parâmetros (c), (d), (e) e (f) cumpridos.

O sub-parâmetro (a), referente a por quanto tempo e onde os dados são armazenados, foi considerado parcialmente cumprido. Em sua Política de

Privacidade, no item “Por quanto tempo os Dados serão armazenados”, a empresa estabelece:

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

Ainda que seja positivo que a empresa estabeleça um prazo mínimo, a ausência de informações sobre o período máximo pelo qual são armazenados alguns dados acaba por tornar demasiado imprecisa a disposição. Além disso, mesmo com os detalhamentos sobre o processo decisório para determinação do tempo de retenção, poucas informações concretas são oferecidas.

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.”

Mesmo que haja alguma informação sobre o fato de os dados pessoais poderem ser tratados fora do Brasil, não são fornecidas informações claras e completas sobre o local de seu armazenamento. Em vista disso e das questões apontadas quanto ao tempo de armazenamento, o sub-parâmetro foi considerado parcialmente atendido.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, não foi considerado foi atendido. Isso porque, no mesmo trecho apontado

acima, em “Por quanto tempo os Dados serão armazenados” na Política de Privacidade, a empresa informa apenas o período mínimo de armazenamento, sem apontar expressamente a hipóteses e em quanto tempo os dados são apagados.

O sub-parâmetro (c), referente às práticas de segurança que a empresa observa, foi considerado atendido. Em seu Relatório de Sustentabilidade 2019, p. 46, a empresa esclarece:

> “Na TIM, a gestão da segurança e privacidade dos dados dos clientes é realizada em acordo com a norma ISO 27001, padrão para sistema de gestão da segurança da informação (ISMS – Information Security Management System) e tem como requisitos mandatórios os seguintes pontos:
> • Somente colaboradores autorizados têm permissão para acessar as informações de cadastro e dados de comunicação dos clientes, e em situações específicas;
> • Fornecedores – incluindo os prestadores de Serviço de Valor Agregado (VAS) – assinam contratos com cláusula de confidencialidade e privacidade dos dados dos clientes.”

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, vide parágrafo acima, 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. A TIM Banda Larga, em seu Contrato de Prestação de Serviços TIM LIVE, estabelece que:

> “19.3 O CLIENTE autoriza a TIM a reter os seus dados e transmiti-los para empresas do GRUPO TIM, além de instituições financeiras, empresas de cartão de crédito e parceiros comerciais com a finalidade de prestar o serviço, criar e disponibilizar novas ofertas e serviços ao CLIENTE.”

Além disso, 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.

Por fim, 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."

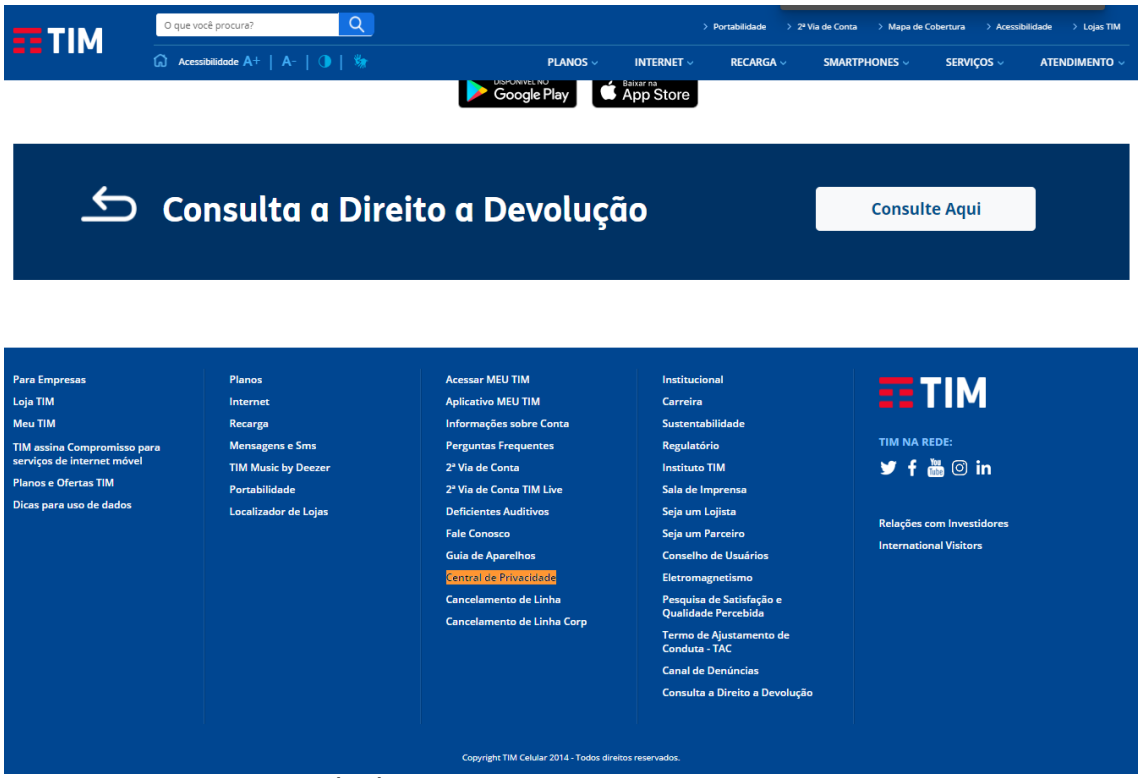
O parâmetro III, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. Por meio de e-mail a dpo.consumer@timbrasil.com.br, um integrante do InternetLab conseguiu acesso a seus dados cadastrais básicos, como nome, CPF, data de nascimento etc. O InternetLab ressalta que dados pessoais vão além das informações de natureza principalmente cadastral que foram compartilhadas, e que o efetivo cumprimento ao direito de acesso aos dados pelo seu titular envolveria o compartilhamento de outras e mais detalhadas informações. No entanto, nessa edição do Quem Defende Seus Dados, por termos obtido sucesso no contato e na averiguação de funcionamento do canal de contato com a empresa, tal parâmetro foi considerado atendido.

Independentemente disso, o InternetLab enaltece o procedimento de exercício do direito de acesso aos dados, que contou com verificação da identidade do titular solicitante, de forma a resguardar sua privacidade e a segurança de suas informações.

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: "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 igualmente considerado atendido. Isso porque a Central de Privacidade da TIM é de acesso relativamente fácil: em sua página principal, na barra final, há um link para esse ambiente.



captura de tela de 29/10/2020. Página inicial da TIM.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ☆

Nesta categoria, a Tim Banda Larga obteve um quarto de estrela, tendo cumprido parcialmente o parâmetro I.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente cumprido. No Contrato de Prestação de Serviços da TIM Live, a empresa esclarece:

> "19.2 A TIM dispensa tratamento sigiloso e confidencial aos dados e comunicações do CLIENTE, podendo disponibilizá-los aos órgãos e autoridades competentes, quando solicitados, inclusive para prevenir e reprimir atos ilícitos, conforme legislação aplicável."

Além disso, em seu Relatório de Sustentabilidade 2019 (p. 46):

> “Dados cadastrais e de comunicações telefônicas são compartilhados apenas com autoridades, de acordo com a legislação brasileira, e para o cumprimento de obrigações judiciais de quebra de sigilo telefônico e telemático.”

A empresa não identifica as autoridades às quais entende ser devida a entrega de dados cadastrais sem ordem judicial. No entanto, por prometer cumprir com a legislação na disponibilização de “dados e comunicações” às “autoridades competentes”, o parâmetro foi considerado parcialmente cumprido. Recomendamos que a empresa identifique de forma expressa quais são as autoridades competentes a quem ela entrega dados sem ordem judicial.

Além disso, 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 Tim Banda Larga.

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 Tim Banda Larga.

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 foi encontrada menção ao tema nos documentos analisados da Tim Banda Larga.

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 Tim Banda Larga obteve estrela cheia, pois atendeu a ambos 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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas TIM, Vivo, Claro e Oi, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

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) 5642, da ACEL, não foram consideradas, já que não registraram movimentações.

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 sigilo E quebra" e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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.

No entanto, em fase de engajamento, a empresa informou ao InternetLab — com a devida supressão dos dados pessoais das partes — processos em que a empresa contestou, às autoridades policiais, pedidos de quebra de sigilo de dados por diferentes razões, como a falta de legitimidade em tal solicitação. Por isso, o parâmetro foi considerado atendido.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a TIM Banda Larga obteve estrela cheia, pois atendeu ao parâmetro I e II.

O parâmetro I, relativo ao posicionamento em geral da empresa, foi considerado atendido. Em fase de engajamento, o InternetLab tomou conhecimento da participação da empresa na consulta pública sobre a "Estratégia Nacional de Inteligência Artificial", elaborada pelo Ministério da Ciência, Tecnologia e Inovações (MCTIC), em que defendeu, dentre outros:

> "Transparência e explicabilidade: As partes envolvidas na criação e execução de aplicações de IA devem estar comprometidas com a transparência e a divulgação responsável de informações sobre os sistemas de IA. Devem ser fornecidas informações suficientes a fim de (i) conscientizar as partes interessadas sobre suas interações com os sistemas de IA, (ii) permitir que as pessoas afetadas por um sistema de IA entendam as razões do resultado obtido e (iii) permitir que aqueles afetados adversamente por um sistema de IA contestem seus resultados com base em informações fáceis de entender sobre os fatores e a lógica que serviu de base para a decisão automatizada.
> (...)
> Privacidade e governança no uso de dados: uma vez que a utilização massiva de dados é da essência da IA, além de garantir o respeito total à privacidade e à proteção destes, deve-se assegurar a criação de ambiente que assegure sua governança, levando em consideração a qualidade e a integridade dos dados e garantindo acesso legítimo a eles."

Além disso, averiguou-se que a empresa se posicionou, na mídia comum e na mídia especializada, a favor de boas práticas em privacidade e proteção de dados (1, 2, 3, 4, 5, 6). Por ter apresentado propostas concretas de inovações técnicas ou normativas, em especial na consulta pública referida acima, o parâmetro foi considerado atendido.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido. Isso porque, no contexto das parcerias para monitoramento da população firmadas entre as operadoras e estados e municípios (vide notícia do TeleTime), houve preocupação da empresa para que somente dados anonimizados/agregados, por exemplo via mapas de calor e tabelas dinâmicas, fossem compartilhados. Durante a Live "As telecomunicações em tempos de incertezas: quatro perspectivas", realizada pelo portal de notícias especializadas Teletime no dia 23/04/2020, a TIM confirmou esse posicionamento, ressaltando o compartilhamento somente de dados anônimos, por meio de seu CTIO, Sr. Leonardo Capdeville. Outros posicionamentos no mesmo sentido foram identificados na fase de engajamento (1, 2, 3).

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 parcialmente ao parâmetro IV.

O parâmetro I, relativo à publicação de relatórios de transparência em português, foi considerado atendido, já que a TIM publicou este ano, em português, um Relatório de Sustentabilidade sobre suas atividades no Brasil. Mesmo que ainda caibam aperfeiçoamentos (vide itens abaixo), o relatório contém informações sobre a quantidade de ofícios recebidos do poder judiciário e o número de ações judiciais em que a empresa está envolvida (vide p. 47 do relatório - trechos copiados na análise do parâmetro IV abaixo), razão pela qual se considerou o parâmetro atendido.

captura de tela de 31.07.2020. Página de sustentabilidade da TIM.

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".

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

O parâmetro IV, relativo às informações sobre pedidos de acesso a dados, foi considerado parcialmente atendido. Em seu relatório de transparência, a empresa informa (p. 47):

> ""Em 2019, a TIM se envolveu em pouco mais de mil ações judiciais relacionadas à privacidade de dados, das quais 801 aguardam julgamento e 239 foram encerradas, sendo 76 casos concluídos com decisões a favor da TIM. Durante o mesmo período, a empresa registrou 3 incidentes de vazamentos de dados de clientes, que foram identificados, monitorados e gerenciados pela companhia para as devidas tratativas e resoluções."
>
> e
>
> "Em 2019, a TIM recebeu mais de 250 mil ofícios por parte do Poder Judiciário com solicitações de quebra de privacidade relativas a:
> • Interceptações telefônicas: 381.113
> • Dados cadastrais: 513.468
> • Extratos telefônicos: 595.728.
> Não é possível auferir com precisão o número de clientes afetados pelos pedidos de informações, uma vez que autoridades diferentes podem solicitar dados do mesmo alvo, seja por meio do número da linha (MSISDN), do IMEI ou do CPF, além da possibilidade de solicitação de relatórios de chamadas com os cadastros de todos os números, não sendo possível, atualmente, precisar a quantidade de registros nesses relatórios. Os números correspondem aos pedidos atendidos manualmente, bem como aos pedidos realizados diretamente pelas autoridades competentes por meio do Webservice disponibilizado para essa finalidade."

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", não obstante isso já ter sido feito por outras empresas. Por isso, 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 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 a todos os parâmetros.

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, no item "Que tipo de Dados e com qual finalidade a TIM trata", a empresa especifica a origem, o tipo de dado coletado, a finalidade e a base legal de tratamento de diversos dados pessoais processados por ela. Dentre outros, informa 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: e-mail, 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 locacionais (país, cidade e estado) de onde ocorreu o acesso ou onde a ligação está ocorrendo; registros de telefonia e de envio de SMS e MMS; desempenho da rede e da infraestrutura de telecomunicações . Dados sobre pagamento: números e dados de cartão de crédito, transações de recargas, informações bancárias necessárias para prestação de serviços; informações de crédito para os sistemas de tarifação e emissão de faturas. 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.

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.

Quanto ao parâmetro II, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, considerou-se que foi atendido, tendo sido o sub-parâmetro (a) considerado parcialmente atendido e os sub-parâmetros (c), (d), (e) e (f) foram considerados integralmente atendidos.

O sub-parâmetro (a), referente a por quanto tempo e onde os dados são armazenados, foi considerado parcialmente cumprido. Em sua Política de Privacidade, no item “Por quanto tempo os Dados serão armazenados”, a empresa estabelece:

> “Nós manteremos seus Dados Pessoais somente pelo tempo que for necessário para cumprir com as finalidades para as quais os coletamos, inclusive para fins de cumprimento de quaisquer obrigações legais, contratuais, de prestação de contas ou requisição de autoridades competentes.
> Para determinar o período de retenção adequado para os Dados Pessoais, além do prazo prescricional, consideramos a quantidade, a natureza e a sensibilidade destes Dados, o risco potencial de danos decorrentes do uso não autorizado ou da divulgação de seus Dados Pessoais, a finalidade de Tratamento destes Dados e se podemos alcançar tais propósitos por outros meios, e os requisitos legais aplicáveis. Por exemplo, por obrigação imposta pelo Marco Civil da

> Internet, os Dados relacionados a IP, data e hora das suas conexões à internet, quando a TIM for responsável por prover este acesso, serão mantidos por, no mínimo, 12 meses e referente aos aplicativos criados pela Tim, por, no mínimo, 6 meses."

Ainda que seja positivo que a empresa estabeleça um prazo mínimo, a ausência de informações sobre o período máximo pelo qual são armazenados alguns dados torna demasiado imprecisa tal disposição. Além disso, mesmo com os detalhamentos acima sobre o processo decisório para determinação do tempo de retenção, poucas informações concretas são oferecidas.

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."

Mesmo que haja alguma informação sobre o fato de os dados pessoais poderem ser tratados fora do Brasil, não são fornecidas informações claras e completas sobre o local de seu armazenamento. Em vista disso e das questões apontadas quanto ao tempo de armazenamento, o sub-parâmetro foi considerado parcialmente atendido.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, não foi considerado foi atendido. Isso porque, no mesmo trecho apontado acima, em "Por quanto tempo os Dados serão armazenados" na Política de Privacidade, a empresa informa apenas o período mínimo de armazenamento, sem apontar expressamente a hipóteses e em quanto tempo os dados são apagados.

O sub-parâmetro (c), referente às práticas de segurança que a empresa observa, foi considerado atendido. Em seu Relatório de Sustentabilidade 2019, p. 46, a empresa esclarece:

> "Na TIM, a gestão da segurança e privacidade dos dados dos clientes é realizada em acordo com a norma ISO 27001, padrão para sistema de gestão da segurança da informação (ISMS – Information Security Management System) e tem como requisitos mandatórios os seguintes pontos:

> • Somente colaboradores autorizados têm permissão para acessar as informações de cadastro e dados de comunicação dos clientes, e em situações específicas;
> • Fornecedores – incluindo os prestadores de Serviço de Valor Agregado (VAS) – assinam contratos com cláusula de confidencialidade e privacidade dos dados dos clientes."

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, vide parágrafo acima, 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. A TIM Banda Larga, em seu Contrato de Prestação de Serviços TIM LIVE, estabelece que:

> "19.3 O CLIENTE autoriza a TIM a reter os seus dados e transmiti-los para empresas do GRUPO TIM, além de instituições financeiras, empresas de cartão de crédito e parceiros comerciais com a finalidade de prestar o serviço, criar e disponibilizar novas ofertas e serviços ao CLIENTE."

Além disso, 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.

Por fim, 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

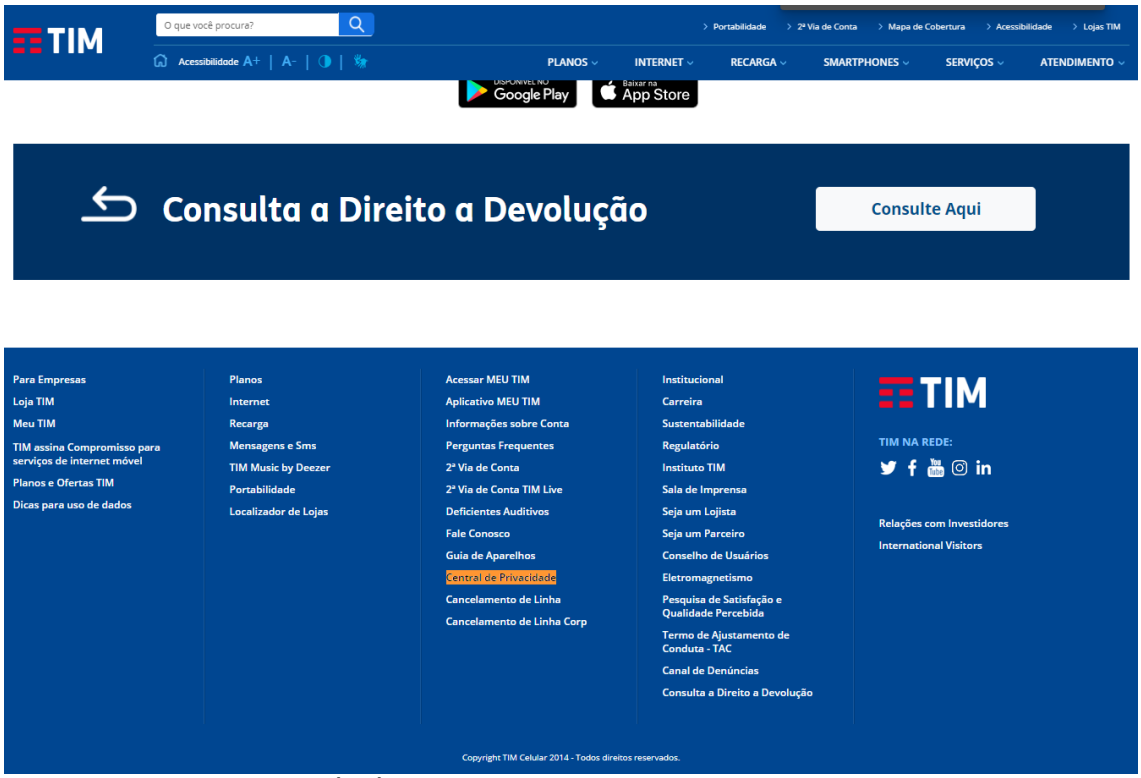
> de pagamento para poder processar os dados de faturamento dos nossos Serviços.
> (...)
> Análise de desempenho: Os dados armazenados pela TIM podem vir a ser coletados por tecnologia de terceiros e utilizados para fins de estatísticas (analytics), com a finalidade de a TIM compreender quem são as pessoas 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."

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. Por meio de e-mail a dpo.consumer@timbrasil.com.br, um integrante do InternetLab conseguiu acesso a seus dados cadastrais básicos, como nome, CPF, data de nascimento etc. O InternetLab ressalta que dados pessoais vão além das informações de natureza principalmente cadastral que foram compartilhadas, e que o efetivo cumprimento ao direito de acesso aos dados pelo seu titular envolveria o compartilhamento de outras e mais detalhadas informações. No entanto, nessa edição do Quem Defende Seus Dados, por termos obtido sucesso no contato e na averiguação de funcionamento do canal de contato com a empresa, tal parâmetro foi considerado atendido.

Independentemente disso, o InternetLab enaltece o procedimento de exercício do direito de acesso aos dados, que contou com verificação da identidade do titular solicitante, de forma a resguardar sua privacidade e a segurança de suas informações.

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: "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 igualmente considerado atendido. Isso porque a Central de Privacidade da TIM é de acesso relativamente fácil: em sua página principal, na barra final, há um link para esse ambiente.



captura de tela de 29/10/2020. Página inicial da TIM.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a TIM Móvel obteve um quarto de estrela, tendo cumprido parcialmente o parâmetro I.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente cumprido. A TIM Móvel, em seu Contrato de prestação do Serviço Móvel Pessoal pré-pago, estabelece:

> 10.4 A TIM dispensará tratamento sigiloso e confidencial aos dados e comunicações do CLIENTE, podendo disponibilizá-los em caso de determinação de autoridade competente." (*Obs.: mesma redação da cláusula 10.12 do contrato de SMP pós-pago e na cláusula 8.4 do Termo de Adesão do SMP pré-pago*)

Além disso, em seu Relatório de Sustentabilidade 2019 (p. 46):

> "Dados cadastrais e de comunicações telefônicas são compartilhados apenas com autoridades, de acordo com a legislação brasileira, e para o cumprimento de obrigações judiciais de quebra de sigilo telefônico e telemático."

A empresa não identifica as autoridades às quais entende ser devida a entrega de dados cadastrais sem ordem judicial. No entanto, por prometer cumprir com a legislação na disponibilização de dados às "autoridades competentes", o parâmetro foi considerado parcialmente cumprido. Recomendamos que a empresa identifique de forma expressa quais são as autoridades competentes a quem ela entrega dados sem ordem judicial.

Além disso, 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 TIM Móvel.

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

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 foi encontrada menção ao tema nos documentos analisados da TIM Móvel.

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 TIM Móvel obteve estrela cheia, pois atendeu a ambos 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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas TIM, Vivo, Claro e Oi, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

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 ADI 5642, da ACEL, não foram consideradas, já que não registraram movimentações.

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 sigilo E quebra" e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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.

No entanto, em fase de engajamento, a empresa informou ao InternetLab — com a devida supressão dos dados pessoais das partes — processos em que a empresa contestou, às autoridades policiais, pedidos de quebra de sigilo de dados por diferentes razões, como a falta de legitimidade em tal solicitação. Por isso, o parâmetro foi considerado atendido.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: ★

Nesta categoria, a TIM Banda Larga obteve estrela cheia, pois atendeu ao parâmetro I e II.

O parâmetro I, relativo ao posicionamento em geral da empresa, foi considerado atendido. Em fase de engajamento, o InternetLab tomou conhecimento da participação da empresa na consulta pública sobre a "Estratégia Nacional de Inteligência Artificial", elaborada pelo MCTIC, em que defendeu, dentre outros:

> “Transparência e explicabilidade: As partes envolvidas na criação e execução de aplicações de IA devem estar comprometidas com a transparência e a divulgação responsável de informações sobre os sistemas de IA. Devem ser fornecidas informações suficientes a fim de (i) conscientizar as partes interessadas sobre suas interações com os sistemas de IA, (ii) permitir que as pessoas afetadas por um sistema de IA entendam as razões do resultado obtido e (iii) permitir que aqueles afetados adversamente por um sistema de IA contestem seus resultados com base em informações fáceis de entender sobre os fatores e a lógica que serviu de base para a decisão automatizada.
> (...)
> Privacidade e governança no uso de dados: uma vez que a utilização massiva de dados é da essência da IA, além de garantir o respeito total à privacidade e à proteção destes, deve-se assegurar a criação de ambiente que assegure sua governança, levando em consideração a qualidade e a integridade dos dados e garantindo acesso legítimo a eles.”

Além disso, averiguou-se que a empresa se posicionou, na mídia comum e na mídia especializada, a favor de boas práticas em privacidade e proteção de dados (1, 2, 3, 4, 5, 6). Por ter apresentado propostas concretas de inovações técnicas ou normativas, em especial na consulta pública referida acima, o parâmetro foi considerado atendido.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido. Isso porque, no contexto das parcerias para monitoramento da população firmadas entre as operadoras e estados e municípios (vide notícia do TeleTime), houve preocupação da empresa para que somente dados anonimizados/agregados, por exemplo via mapas de calor e tabelas dinâmicas, fossem compartilhados. Durante a Live “As telecomunicações em tempos de incertezas: quatro perspectivas”, realizada pelo portal de notícias especializadas Teletime no dia 23/04/2020, a TIM confirmou esse posicionamento, ressaltando o compartilhamento somente de dados anônimos, por meio de seu CTIO, Sr. Leonardo Capdeville. Outros posicionamentos no mesmo sentido foram identificados na fase de engajamento (1, 2, 3).

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

Resultado: 

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

O parâmetro I, relativo à publicação de relatórios de transparência em português, foi considerado atendido, já que a TIM publicou este ano, em português, um Relatório de Sustentabilidade sobre suas atividades no Brasil.

Mesmo que ainda caibam aperfeiçoamentos (vide itens abaixo), o relatório contém informações sobre a quantidade de ofícios recebidos do poder judiciário e o número de ações judiciais em que a empresa está envolvida (vide p. 47 do relatório - trechos copiados na análise do parâmetro IV abaixo), 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 31.07.2020. Página de sustentabilidade da TIM.

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

O parâmetro IV, relativo às informações sobre pedidos de acesso a dados, foi considerado parcialmente atendido. Em seu relatório de transparência, a empresa informa (p. 47):

> ""Em 2019, a TIM se envolveu em pouco mais de mil ações judiciais relacionadas à privacidade de dados, das quais 801 aguardam julgamento e 239 foram encerradas, sendo 76 casos concluídos com decisões a favor da TIM. Durante o mesmo período, a empresa registrou 3 incidentes de vazamentos de dados de clientes, que foram identificados, monitorados e gerenciados pela companhia para as devidas tratativas e resoluções."

e

“Em 2019, a TIM recebeu mais de 250 mil ofícios por parte do Poder Judiciário com solicitações de quebra de privacidade relativas a:
• Interceptações telefônicas: 381.113
• Dados cadastrais: 513.468
• Extratos telefônicos: 595.728.
Não é possível auferir com precisão o número de clientes afetados pelos pedidos de informações, uma vez que autoridades diferentes podem solicitar dados do mesmo alvo, seja por meio do número da linha (MSISDN), do IMEI ou do CPF, além da possibilidade de solicitação de relatórios de chamadas com os cadastros de todos os números, não sendo possível, atualmente, precisar a quantidade de registros nesses relatórios. Os números correspondem aos pedidos atendidos manualmente, bem como aos pedidos realizados diretamente pelas autoridades competentes por meio do Webservice disponibilizado para essa finalidade.”

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”, não obstante isso já ter sido feito por outras empresas. Por isso, 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 TIM Móvel não obteve estrela, pois não há menção à possibilidade de notificação do usuário em qualquer um dos documentos analisados.

2020

VIVO BANDA LARGA

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Vivo Banda Larga obteve ¾ de estrela, 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 algumas informações estão disponíveis no Relatório de Sustentabilidade e no Centro de Privacidade, no website da Vivo. Nessa seção, os usuários contam um com breve vídeo informativo sobre os pontos principais da proteção de dados pela empresa e depois, através do menu, podem encontrar outras informações mais pormenorizadas.

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 “Dados Coletados”, a empresa informa:

> “A Vivo coleta as suas informações de acordo com o serviço que você utiliza. Saiba quais são estas informações: Dados cadastrais: O que você disponibilizou quando contratou os nossos serviços, como nome, endereço, CPF etc.; Volumes de dados trafegados na internet via rede 2G, 3G e/ou 4G; Histórico de uso dos produtos e serviços contratados: Exatamente o que o nome diz, mas é importante saber que esse histórico não envolve registro de apps utilizados no seu celular nem o que você faz nas redes sociais ou sites. Isso vale apenas para os apps da Vivo! Aí sim é feita a coleta de dados para deixar o app cada vez melhor; Eventos de SMS que estão dentro e fora da rede Vivo nacional: Essa coleta inclui eventos Vivo internacionais e de operadoras internacionais em roaming; Histórico de chamadas realizadas e recebidas: Informações contábeis e fiscais, de fatura e pagamento do cliente; Transações de recargas e acompanhamento do uso desses créditos; Dados de atendimento ao cliente em lojas e no call center.”

Ainda, o Contrato de Adesão de Prestação do Serviço de Telefônico Fixo Comutado, a empresa informa quais são os dados coletados no momento da instalação do serviço:

> 5.2.12. Entregar, no momento da instalação ou sempre que solicitado pela VIVO, cópia dos documentos de identificação

> pessoal, tais como RG, CPF, CNPJ, Contrato Social, comprovante de endereço, dentre outros, que comprovem os dados cadastrais informados pelo CLIENTE quando da contratação.

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 'Dados Coletados" (vide trecho acima) e "Para que e como coletamos dados?" (vide trecho abaixo), informa-se que "a Vivo coleta as suas informações de acordo com o serviço que você utiliza", especifica-se a coleta de dados de uso dos produtos e serviços contratados, históricos de chamada, dados de atendimento, transações de recarga, 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 e como coletamos dados?" a empresa descreve algumas das finalidades, mencionando a melhora do serviço da rede, a personalização do atendimento, dentre outros:

> "Queremos que a sua experiência com a Vivo seja cada vez melhor. Por isso, vamos explicar aqui os motivos para coletarmos todas essas informações. Transações de recargas e acompanhamento do uso desses créditos; Melhorar o desempenho da rede e aumentar a qualidade dos nossos serviços; Corrigir as falhas nos serviços de rede móvel, fixa e TV ainda mais rápido; Deixar os processos para a elaboração de planos, serviços e ofertas personalizadas ainda mais próximos do seu perfil; Avaliar a demanda por região geográfica; Ajudar nas decisões estratégicas da Vivo, como redistribuir o sinal ou remanejar a carteira de serviços; Melhorar a experiência de relacionamento entre você e a Vivo, como envio de marketing direto e fornecimento de ofertas mais relevantes."

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 per l 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 a empresa 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 "Direito de Acesso, Retificação, Oposição e Cancelamento", a empresa informa sobre a existência desses quatro direitos do consumidor 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 um número de telefone e de SMS para que se possa exercer tais direitos.

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, item (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 e os sub-parâmetros (a), (e) e (f) considerados parcialmente atendidos.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado parcialmente cumprido. No Centro de Privacidade, em "Por quanto tempo armazenamos os dados?" a empresa informa:

> "Em conformidade ao Marco Civil da Internet, a Vivo armazena por no mínimo 1 ano os seus registros de

> conexão, que são as informações sobre o tempo das suas conexões à internet e o IP para envio e recebimento de dados. Os seus dados cadastrais (como nome completo, endereço e CPF) e os dados de faturamento (documentos fiscais) são armazenados por no mínimo 5 anos, para processos judiciais e administrativos. Não registramos conteúdo de provedores de apps, a não ser aqueles que criamos. Então, neste caso, de acordo com o Marco Civil da Internet, mantemos o registro por até 6 meses, sob sigilo, em ambiente controlado e de segurança."

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, ainda, quais os prazos máximos de armazenamento. Quanto ao local de armazenamento, ainda no Centro de Privacidade, em "Onde processamos os dados?", a empresa informa:

> "A maior parte das informações é tratada dentro da Vivo ou em empresas do Grupo Telefônica, respeitando sempre a legislação vigente no Brasil. Mas, às vezes, quando precisamos tratar dados externamente, fazemos tudo com cláusulas de confidencialidade e assegurando que todo o acesso seja auditado e monitorado, para garantir a sua privacidade."

Considerou-se a redação do trecho acima, por ser excessivamente ampla, insatisfatória. Mesmo que a empresa informe que "a maior parte das informações é tratada dentro da Vivo", dando mais alguns poucos detalhes, 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.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, não foi considerado atendido. Isso porque, no mesmo trecho apontado acima, em "Por quanto tempo armazenamos os dados?" no Centro de Privacidade, a

empresa informa apenas o tempo mínimo pelo qual armazena os dados, sem garantir que serão apagados ou quando serão apagados.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, foi considerado atendido. No Relatório de Sustentabilidade de 2019 da empresa (p. 34), 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 (ISO27001 e ISO22301, NIST, PCI/ DSS etc) de protocolos a serem seguidos, especialmente relacionados a sistemas e servidores seguros." 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 Dados", e na cláusula 13ª do Contrato de Adesão, que dispõe sobre o uso de dados pessoais do cliente, a empresa elenca duas hipóteses de fornecimento de dados a terceiros: (i) mediante ordem judicial e (ii) por requisição de autoridades administrativas competentes. Fora essas duas hipóteses, a empresa se compromete a não fornecer dados pessoais, salvo mediante livre consentimento:

> "A Vivo pode, eventualmente, apoiar um estudo de comportamento em eventos que promovam deslocamento de um público em determinada localização. Mas é importante ressaltar que, nesse caso, não é possível qualquer forma de individualização dessas informações. As informações individualizadas só vão ser compartilhadas com parceiros se você autorizar. Seus dados podem ser compartilhados: Com parceiros sempre que relacionado com a prestação do serviço contratado por você (por exemplo, quando você está em roaming); Em casos previstos em lei e/ou por força de ordem judicial; Com parceiros, de forma individualizada, apenas com sua autorização expressa e sempre com a possibilidade de opt out."

> 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, trazendo somente o exemplo do *roaming* para o caso de prestação de serviços de terceiros por meio da Vivo, 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.

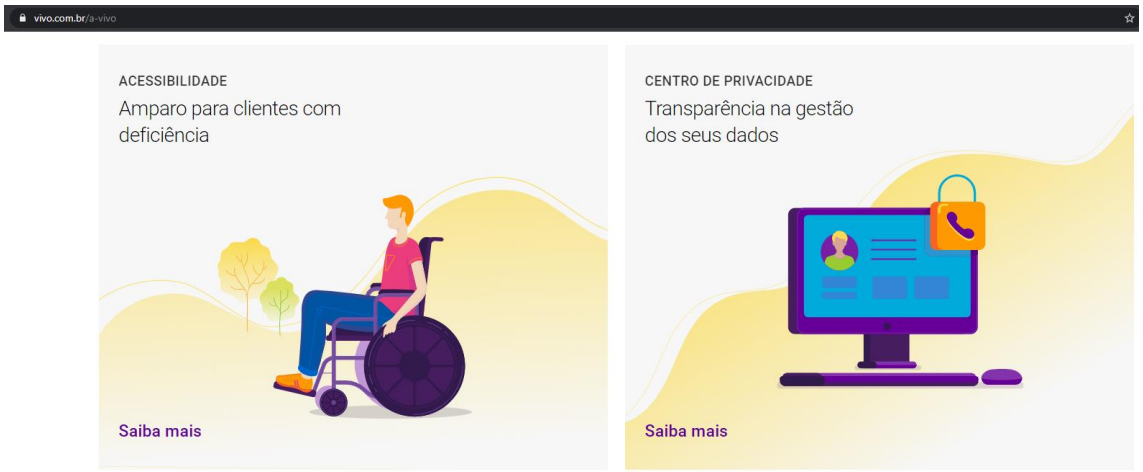
Por fim, quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, considerou-se igualmente que foi parcialmente atendido. Isso porque as informações trazidas sobre o tema, referenciadas na análise do sub-parâmetro (e) acima, são pouco claras e afirmam somente de forma genérica que os dados podem ser compartilhados "sempre que relacionado com a prestação do serviço contratado por você" ou "de forma individualizada, apenas com sua autorização expressa". 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 parâmetro III, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. Por meio de acesso ao portal "Meu Vivo", um integrante do InternetLab conseguiu acesso a dados cadastrais básicos seus, como nome, CPF, data de nascimento etc. O InternetLab ressalta que dados pessoais vão além das informações de natureza principalmente cadastral que foram compartilhadas, e que o efetivo cumprimento ao direito de acesso aos dados pelo seu titular envolveria o compartilhamento de outras e mais detalhadas informações. No entanto, nessa edição do Quem Defende Seus Dados, por termos obtido sucesso no contato e na averiguação de funcionamento do canal de contato com a empresa, tal 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, não foi considerado atendido. Nenhum documento da Vivo mencionava tal possibilidade, sendo afirmado em todas as seções do Centro de Privacidade, ainda, que "A Vivo pode mudar, a qualquer momento, o conteúdo desta política. A alteração mais recente aconteceu em dezembro de 2018."

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.



captura de tela de 07/07/2020. Página inicial da Vivo.

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 meia estrela, tendo cumprido o parâmetro I e parcialmente os parâmetros II e IV.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado cumprido. No *Informe de Transparencia en las Comunicaciones 2019* (p. 20), a empresa afirma que busca cumprir a legislação e marcos regulatórios em âmbito nacional. No seu Centro de privacidade, na seção "quebra de sigilo", esclarece que em algumas situações, “como em caso de ordens judiciais e solicitações de autoridades competentes”, pode haver o compartilhamento registros de conexão, voz e dados sem o conhecimento do usuário, “de acordo com a legislação vigente no Brasil”. Além disso, na mesma página 20 do *Informe de Transparencia en las Comunicaciones*, há a definição de quais seriam as autoridades competentes para interceptações e requisição de metadados de acordo com a legislação brasileira, além de menção da competência dos “juízes de qualquer esfera”:

> *“Interceptación legal: De acuerdo con el artículo 3o de la Ley Federal brasileña n. 9.296/1996 (ley de las interceptaciones), solamente el Juez (de la esfera criminal)*

> *puede determinar las interceptaciones (telefónicas y telemáticas), a petición de la Fiscalía (Ministério Público) o Comisario de Policía (Autoridade Policial).*
> *Metadatos asociados a las comunicaciones: Autoridades competentes » Fiscalía, Comisarios de Policía y Jueces de cualquier esfera, como también Presidentes de las Comisiones Parlamentarias de Investigación: el nombre y dirección del usuario registrado (datos de abonado), así como la identidad de los equipos de comunicación (incluyendo IMSI o IMEI).”*
> *Jueces de cualquier esfera: los datos para identificar el origen y el destino de una comunicación (por ejemplo, números de teléfono, nombres de usuario para los servicios de Internet), la fecha, hora y duración de una comunicación y la localización del dispositivo.”*

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

O parâmetro II, referente à identificação das autoridades competentes e dos crimes no âmbito dos quais a requisição ocorrer, foi considerado parcialmente 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”. No entanto, não há menção à Lei 9.613/98 (Lei de Prevenção à Lavagem de Dinheiro) ou ao artigo 13-A do CPP, nem qualquer outra especificação sobre no âmbito de quais crimes as autoridades competentes poderão requisitar dados.

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, 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, não foi atendido. Em nossas buscas, nenhum documento como esse pôde ser localizado.

O InternetLab enaltece a conduta da Telefónica Global de tornar públicas as suas interpretações sobre quais as autoridades competentes para solicitar dados de usuários e em que circunstâncias. 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 meia estrela, pois atendeu ao parâmetro I.

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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas Vivo, TIM, Claro e Oi, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

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) 5642, da ACEL não foram consideradas, já que não registraram movimentações.

Por fim, para averiguação do parâmetro II, referente à contestação de pedidos abusivos, realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado de São Paulo e no portal “Jusbrasil”, em ambos os casos pelos termos “vivo S/A E sigilo E quebra” e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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 Vivo Banda Larga obteve estrela cheia, pois atendeu o parâmetro II e atendeu parcialmente ao parâmetro I.

O parâmetro I, relativo ao posicionamento em geral da empresa, foi considerado parcialmente atendido. Em fase de engajamento, a empresa informou ao InternetLab sobre sua participação na Consulta Pública nº 13 da Anatel sobre "proposta de requisitos mínimos de segurança cibernética para equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações...", em que forneceu comentários, em nome próprio, defendendo a existência mecanismos de segurança da informação e de controle dos titulares sobre seus dados pessoais em dispositivos conectados à internet.

No entanto, o parâmetro foi considerado somente parcialmente atendido em vista o posicionamento público da empresa não ter sido, na maior parte das vezes, suficientemente propositivo e transparente.

Por exemplo, a Vivo ofereceu contribuição à consulta pública sobre a "Estratégia Nacional de Inteligência Artificial", elaborada pelo MCTIC, defendendo que "as próprias empresas criem sistemas e práticas éticas de forma a ganhar a confiança dos [consumidores]" e afirmando que "os princípios da Telefônica englobam diversos pilares, [como] gestão ética e responsável, governança corporativa e controle interno, respeito aos direitos de expressão e privacidade, compromisso com segurança da informação, comunicação responsável e compromisso com a sociedade em que atuamos." Por mais que seja louvável a participação da empresa nessa consulta, não foram localizadas propostas concretas, normativas ou técnicas, para a proteção de seus clientes.

Em nossas buscas, ainda, foi localizada notícia segundo a qual uma falha de segurança expôs nome completo, endereço, data de nascimento, RG, CPF, e-mail, nome da mãe e número de telefone de 24 milhões de usuários da Vivo. Em sua resposta ao portal que noticiou o vazamento, Olhar Digital, a Vivo confirmou a vulnerabilidade e afirmou haver número "consideravelmente menor" de atingidos. Além disso, afirmou que:

> "A Vivo lamenta o ocorrido e ressalta que revisa constantemente suas políticas e procedimentos de segurança, na busca permanente pelos mais rígidos controles nos acessos aos dados dos seus clientes e no combate a práticas que possam ameaçar a sua privacidade.

> A empresa reitera que respeita a privacidade e a transparência na relação com os seus clientes."

A redação foi considerada excessivamente genérica e insatisfatória para os fins desse relatório, já que não defendeu concretamente a adoção de técnicas que pudessem fazer frente ao ocorrido, nem quais situações específicas levaram a ele.

Além disso, também foi localizada notícia segundo a qual a Vivo, a Net e Oi teriam compartilhado, entre si, "dados pessoais de cidadãos sem cobertura específica para alavancar o número de clientes atendidos". De acordo com a reportagem, do portal Tecmundo, a suspeita advém de relatos de usuários que, após contatarem uma das empresas e receberem negativa quanto à cobertura em sua área, foram contatados pelas outras empresas para oferecendo outros planos de internet, relatos esses confirmados por atendentes de telemarketing da empresa. Em sua resposta ao portal, a Vivo negou que compartilhe "com terceiros quaisquer informações que envolvam dados pessoais de seus clientes ou prospecções." No entanto, não foram dadas explicações para os relatos dos usuários ou das confirmações pelos atendentes, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações.

Por fim, em seu Relatório de Sustentabilidade (p. 35), a empresa afirma ter realizado um workshop de "Segurança da Informação e Proteção de Dados, voltado aos [seus] principais fornecedores." Por mais que a iniciativa seja louvável, a menção ao encontro no relatório da Vivo não traz quaisquer detalhes práticos ou concretos sobre o que foi nele defendido ou exigido.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido. Isso porque, no contexto da parceria para monitoramento da população firmada entre a Vivo e o governo do Estado de São Paulo (vide notícia do Terra), houve preocupação da empresa para que somente dados anonimizados/agregados, por exemplo via mapas de calor e tabelas dinâmicas, fossem compartilhados. Durante a Live "As telecomunicações em tempos de incertezas: quatro perspectivas", realizada pelo portal de notícias especializadas Teletime no dia 23/04/2020, a Vivo confirmou esse posicionamento, ressaltando o compartilhamento somente de dados anônimos, por meio de seu Vice-Presidente de Dados e Inteligência Artificial, Sr. Luiz Médici.

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

Resultado: 

Nesta categoria, a Vivo Banda Larga obteve meia estrela, pois atendeu ao parâmetro III e parcialmente aos parâmetros I e IV.

O parâmetro I, relativo à publicação de relatórios de transparência em português, foi considerado parcialmente atendido. Pelo quarto ano seguido,

encontramos a publicação do *Informe de Transparencia en las Comunicaciones de 2019,* do Grupo Telefônica (documento em espanhol), em que há certo detalhamento sobre o conjunto regulatório em cada país no qual o grupo está presente, o número de requerimentos de dados que receberam em cada país entre 2013 e 2017 e, especialmente no caso do Brasil, quais são as autoridades que consideram competentes. Além disso, o Relatório de Sustentabilidade 2019 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. No entanto, pelo fato de a maior parte das informações relevantes serem apresentadas somente em espanhol, no relatório do Grupo Telefônica mencionado, o parâmetro foi considerado parcialmente atendido.

O parâmetro II, relativo à acessibilidade do relatório de transparência, não foi considerado atendido. Isso porque o Relatório de Sustentabilidade não pode ser encontrado na página da Vivo, marca sob a qual a empresa apresenta seus serviços e produtos no Brasil, e, mesmo no site da Telefônica, é necessário buscar o relatório em "A Telefônica" e, depois, "Sustentabilidade". Quanto ao *Informe de Transparencia en las Comunicaciones,* sequer pode ser encontrado na página da Telefônica Brasil, sendo acessível somente pelo site da Telefónica Espanha, em "Negocio Responsable", e, depois, "Informe de Transparência".

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. 20 e 21), informa-se que, em 2018, foram feitos 445.480 requerimentos de interceptação e 3.131.634 requerimentos de acesso a metadados. No entanto, em ambos os casos, não há informação sobre a quantidade de requerimentos rechaçados ou aceitos, afirmando-se que "el sistema de registro durante el periodo de reporte no disponía de los mecanismos para filtrar por peticiones rechazadas. Se está trabajando para disponer de este dato en los próximos informes." Por isso, 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 ¾ de estrela, tendo atendido aos parâmetros I, II e III e parcialmente ao parâmetro V.

Embora os contratos de telefonia móvel nas modalidades pós e pré-pago não ofereçam informações substanciais sobre as práticas de tratamentos de dados da empresa, constatamos que algumas informações estão disponíveis no Relatório de Sustentabilidade e no Centro de Privacidade, no website da Vivo. Nessa seção, os usuários contam um com breve vídeo informativo sobre os pontos principais da proteção de dados pela empresa e depois, através do menu, podem encontrar outras informações mais pormenorizadas.

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 “Dados Coletados”, a empresa informa:

> “A Vivo coleta as suas informações de acordo com o serviço que você utiliza. Saiba quais são estas informações: Dados cadastrais: O que você disponibilizou quando contratou os nossos serviços, como nome, endereço, CPF etc.; Volumes de dados trafegados na internet via rede 2G, 3G e/ou 4G; Histórico de uso dos produtos e serviços contratados: Exatamente o que o nome diz, mas é importante saber que esse histórico não envolve registro de apps utilizados no seu celular nem o que você faz nas redes sociais ou sites. Isso vale apenas para os apps da Vivo! Aí sim é feita a coleta de dados para deixar o app cada vez melhor; Eventos de SMS que estão dentro e fora da rede Vivo nacional: Essa coleta inclui eventos Vivo internacionais e de operadoras internacionais em roaming; Histórico de chamadas realizadas e recebidas: Informações contábeis e fiscais, de fatura e pagamento do cliente; Transações de recargas e acompanhamento do uso desses créditos; Dados de atendimento ao cliente em lojas e no call center.”

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 ‘Dados Coletados” (vide trecho acima) e “Para que e como coletamos dados?” (vide trecho abaixo), informa-se que “a Vivo coleta as suas informações de acordo com o serviço que você utiliza”, especifica-se a coleta de dados de uso dos

produtos e serviços contratados, históricos de chamada, dados de atendimento, transações de recarga, 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 e como coletamos dados?" a empresa descreve algumas das finalidades, mencionando a melhora do serviço da rede, a personalização do atendimento, dentre outros:

> "Queremos que a sua experiência com a Vivo seja cada vez melhor. Por isso, vamos explicar aqui os motivos para coletarmos todas essas informações. Transações de recargas e acompanhamento do uso desses créditos; Melhorar o desempenho da rede e aumentar a qualidade dos nossos serviços; Corrigir as falhas nos serviços de rede móvel, fixa e TV ainda mais rápido; Deixar os processos para a elaboração de planos, serviços e ofertas personalizadas ainda mais próximos do seu perfil; Avaliar a demanda por região geográfica; Ajudar nas decisões estratégicas da Vivo, como redistribuir o sinal ou remanejar a carteira de serviços; Melhorar a experiência de relacionamento entre você e a Vivo, como envio de marketing direto e fornecimento de ofertas mais relevantes."

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 "Direito de Acesso, Retificação, Oposição e Cancelamento", a empresa informa sobre a existência desses quatro direitos do consumidor 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 um número de telefone e de SMS para que se possa exercer tais direitos.

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 e os sub-parâmetros (a), (e) e (f) considerados parcialmente atendidos.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado parcialmente cumprido. No Centro de Privacidade, em "Por quanto tempo armazenamos os dados?" a empresa informa:

> "Em conformidade ao Marco Civil da Internet, a Vivo armazena por no mínimo 1 ano os seus registros de conexão, que são as informações sobre o tempo das suas conexões à internet e o IP para envio e recebimento de dados. Os seus dados cadastrais (como nome completo, endereço e CPF) e os dados de faturamento (documentos fiscais) são armazenados por no mínimo 5 anos, para processos judiciais e administrativos. Não registramos conteúdo de provedores de apps, a não ser aqueles que criamos. Então, neste caso, de acordo com o Marco Civil da Internet, mantemos o registro por até 6 meses, sob sigilo, em ambiente controlado e de segurança."

As informações sobre tempo de armazenamento foram consideradas satisfatórias, pois são apresentados os prazos de armazenamento detalhados para cada tipo de dado coletado, especificando, ainda, quais os prazos máximos de armazenamento. Quanto ao local de armazenamento, ainda no Centro de Privacidade, em "Onde processamos os dados?", a empresa informa:

> "A maior parte das informações é tratada dentro da Vivo ou em empresas do Grupo Telefônica, respeitando sempre a legislação vigente no Brasil. Mas, às vezes, quando precisamos tratar dados externamente, fazemos tudo com cláusulas de confidencialidade e assegurando que todo o acesso seja auditado e monitorado, para garantir a sua privacidade."

Considerou-se a redação do trecho acima, por ser excessivamente ampla, insatisfatória. Mesmo que a empresa informe que "a maior parte das informações é tratada dentro da Vivo", dando mais alguns poucos detalhes, 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.

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, não foi considerado atendido. Isso porque, no mesmo trecho apontado acima, em "Por quanto tempo armazenamos os dados?" no Centro de Privacidade, a empresa informa apenas o tempo mínimo de armazenamento, não estipulado prazo para que os dados sejam apagados.

O sub-parâmetro (c), relativo às práticas de segurança da empresa, foi considerado atendido. No Relatório de Sustentabilidade de 2019 da empresa (p. 34), 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 (ISO27001 e ISO22301, NIST, PCI/ DSS etc) de protocolos a serem seguidos, especialmente relacionados a sistemas e servidores seguros." 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 Dados", e nas "Cláusulas Gerais do Contrato de Prestação do Serviço Móvel Pessoal Pós-Pago", especifica algumas circunstâncias e compartilhamentos de dados com terceiros, afirmando, respectivamente, que:

> "A Vivo pode, eventualmente, apoiar um estudo de comportamento em eventos que promovam deslocamento de um público em determinada localização. Mas é importante ressaltar que, nesse caso, não é possível qualquer forma de individualização dessas informações. As informações individualizadas só vão ser compartilhadas com parceiros se você autorizar. Seus dados podem ser compartilhados: Com parceiros sempre que relacionado com a prestação do serviço contratado por você (por exemplo, quando você está em roaming); Em casos previstos em lei e/ou por força de ordem judicial; Com parceiros, de forma individualizada, apenas com sua autorização expressa e sempre com a possibilidade de opt out."

> "CLÁUSULAS GERAIS DO CONTRATO DE PRESTAÇÃO DO SERVIÇO MÓVEL PESSOAL PÓS-PAGO:
> 20.3. A VIVO poderá divulgar e comercializar em lista (impressa ou digital) informações constantes em seu cadastro relativas ao CLIENTE, desde que este tenha autorizado a divulgação de seu nome e Código de Acesso, no Termo de Adesão ao Serviço Móvel Pessoal ou, ainda, por autorização verbal via serviço de "Call Center", a qualquer tempo."

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, trazendo somente o exemplo do *roaming* para o caso de prestação de serviços de terceiros por meio da Vivo, não traz exemplos

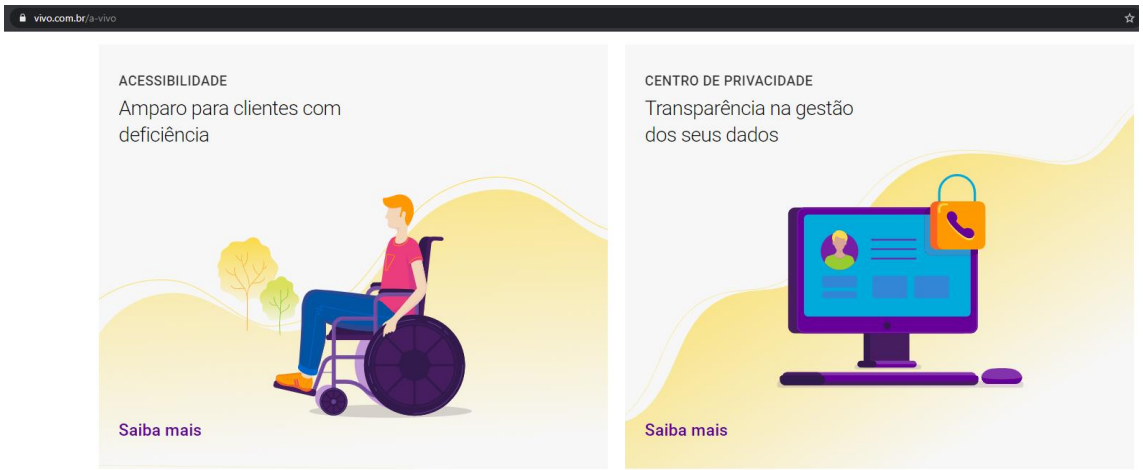
de situações em que possa ter havido autorização expressa do usuário, não tendo sido encontrados casos de tais autorizações nos documentos analisados e não determina quais dados e em quais situações são compartilhados. No entanto, por haver preocupação em apontar informações sobre o tema, com um mínimo de detalhamento, o sub-parâmetro foi considerado parcialmente atendido.

Por fim, 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 somente de forma genérica que os dados podem ser compartilhados "sempre que relacionado com a prestação do serviço contratado por você" ou "de forma individualizada, apenas com sua autorização expressa". 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 parâmetro III, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado atendido. Por meio de acesso ao portal "Meu Vivo", um integrante do InternetLab conseguiu acesso a seus dados cadastrais básicos, como nome, CPF, data de nascimento etc. O InternetLab ressalta que dados pessoais vão além das informações de natureza principalmente cadastral que foram compartilhadas, e que o efetivo cumprimento ao direito de acesso aos dados pelo seu titular envolveria o compartilhamento de outras e mais detalhadas informações. No entanto, nessa edição do Quem Defende Seus Dados, por termos obtido sucesso no contato e na averiguação de funcionamento do canal de contato com a empresa, tal 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, não foi considerado atendido. Nenhum documento da Vivo mencionava tal possibilidade, sendo afirmado em todas as seções do Centro de Privacidade, ainda, que "A Vivo pode mudar, a qualquer momento, o conteúdo desta política. A alteração mais recente aconteceu em dezembro de 2018."

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.



captura de tela de 07/07/2020. Página inicial da Vivo.

No entanto, a maior parte de tais informações não são apresentadas nos contratos de internet móvel 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 móvel obteve meia estrela, tendo cumprido o parâmetro I e parcialmente os parâmetros II e IV.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado cumprido. No *Informe de Transparencia en las Comunicaciones 2019* (p. 20), a empresa afirma que busca cumprir a legislação e marcos regulatórios em âmbito nacional. No seu Centro de privacidade, na seção "quebra de sigilo", esclarece que em algumas situações, "como em caso de ordens judiciais e solicitações de autoridades competentes", pode haver o compartilhamento registros de conexão, voz e dados sem o conhecimento do usuário, "de acordo com a legislação vigente no Brasil". Além disso, na mesma página 20 do *Informe de Transparencia en las Comunicaciones*, há a definição de quais seriam as autoridades competentes para interceptações e requisição de metadados de acordo com a legislação brasileira, além de menção da competência dos "juízes de qualquer esfera":

> *"Interceptación legal: De acuerdo con el artículo 3o de la Ley Federal brasileña n. 9.296/1996 (ley de las interceptaciones), solamente el Juez (de la esfera criminal) puede determinar las interceptaciones (telefónicas y telemáticas), a petición de la Fiscalía (Ministério Público) o Comisario de Policía (Autoridade Policial).*

2020

> *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 parcialmente 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”. No entanto, não há menção à Lei 9.613/98 (Lei de Prevenção à Lavagem de Dinheiro) ou ao artigo 13-A do CPP, nem qualquer outra especificação sobre no âmbito de quais crimes as autoridades competentes poderão requisitar dados.

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, 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, não foi atendido. Em nossas buscas, nenhum documento como esse pôde ser localizado.

O InternetLab enaltece a conduta da Telefónica Global de tornar públicas as suas interpretações sobre quais as autoridades competentes para solicitar dados de usuários e em que circunstâncias. 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 meia estrela, pois atendeu ao parâmetro I.

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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas Vivo, TIM, Claro e Oi, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

Por fim, para averiguação do parâmetro II, referente à contestação de pedidos abusivos, realizamos buscas exploratórias na base de dados do Tribunal de Justiça do Estado de São Paulo e no portal "Jusbrasil", em ambos os casos pelos termos "vivo S/A E sigilo E quebra" e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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, 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 ADI 5642, da ACEL, não foram consideradas, já que não registraram movimentações.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: ★

Nesta categoria, a Vivo móvel obteve estrela cheia, pois atendeu ao parâmetro II e parcialmente ao parâmetro I.

O parâmetro I, relativo ao posicionamento em geral da empresa, foi considerado parcialmente atendido. Em fase de engajamento, a empresa informou ao InternetLab sobre sua participação na Consulta Pública nº 13 da Anatel sobre "proposta de requisitos mínimos de segurança cibernética para equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações...", em que forneceu comentários, em nome próprio, defendendo a existência mecanismos de segurança da informação e de controle dos titulares sobre seus dados pessoais em dispositivos conectados à internet.

No entanto, o parâmetro foi considerado somente parcialmente atendido em vista de o posicionamento público da empresa não ter sido, na maior parte das vezes, suficientemente propositivo e transparente.

Por exemplo, a Vivo ofereceu contribuição à consulta pública sobre a "Estratégia Nacional de Inteligência Artificial", elaborada pelo MCTIC, defendendo que "as próprias empresas criem sistemas e práticas éticas de forma a ganhar a confiança dos [consumidores]" e afirmando que "os princípios da Telefônica englobam diversos pilares, [como] gestão ética e responsável, governança corporativa e controle interno, respeito aos direitos de expressão e privacidade, compromisso com segurança da informação, comunicação responsável e compromisso com a sociedade em que atuamos." Por mais que seja louvável a participação da empresa nessa consulta, não foram localizadas propostas concretas, normativas ou técnicas, para a proteção de seus clientes.

Em nossas buscas, ainda, foi localizada notícia segundo a qual uma falha de segurança expôs nome completo, endereço, data de nascimento, RG, CPF, e-mail, nome da mãe e número de telefone de 24 milhões de usuários da Vivo. Em sua resposta ao portal que noticiou o vazamento, Olhar Digital, a Vivo confirmou a vulnerabilidade e afirmou haver número "consideravelmente menor" de atingidos. Além disso, afirmou que:

> "A Vivo lamenta o ocorrido e ressalta que revisa constantemente suas políticas e procedimentos de segurança, na busca permanente pelos mais rígidos controles nos acessos aos dados dos seus clientes e no combate a práticas que possam ameaçar a sua privacidade. A empresa reitera que respeita a privacidade e a transparência na relação com os seus clientes."

A redação foi considerada excessivamente genérica e insatisfatória para os fins desse relatório, já que não defendeu concretamente a adoção de técnicas que pudessem fazer frente ao ocorrido, nem quais situações específicas levaram a ele.

Além disso, também foi localizada notícia segundo a qual a Vivo, a Net e Oi teriam compartilhado, entre si, "dados pessoais de cidadãos sem cobertura específica para alavancar o número de clientes atendidos". De acordo com a reportagem, do portal Tecmundo, a suspeita advém de relatos de usuários que, após contatarem uma das empresas e receberem negativa quanto à cobertura em sua área, foram contatados pelas outras empresas para oferecendo outros planos de internet, relatos esses confirmados por atendentes de telemarketing da empresa. Em sua resposta ao portal, a Vivo negou que compartilhe "com terceiros quaisquer informações que envolvam dados pessoais de seus clientes ou prospecções." No entanto, não foram dadas explicações para os relatos dos usuários ou das confirmações pelos atendentes, nem foram defendidos concretamente normas ou técnicas que pudessem fazer frente às alegações. Por isso, a resposta da empresa foi considerada excessivamente genérica.

Por fim, em seu Relatório de Sustentabilidade (p. 35), a empresa afirma ter realizado um workshop de "Segurança da Informação e Proteção de Dados, voltado aos [seus] principais fornecedores." Por mais que a iniciativa seja louvável, a menção ao encontro no relatório da Vivo não traz quaisquer detalhes práticos ou concretos sobre o que foi nele defendido ou exigido.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, foi considerado atendido. Isso porque, no contexto da parceria para monitoramento da população firmada entre a Vivo e o governo do Estado de São Paulo (vide notícia do Terra), houve preocupação da empresa para que somente dados anonimizados/agregados, por exemplo via mapas de calor e tabelas dinâmicas, fossem compartilhados. Durante a Live "As telecomunicações em tempos de incertezas: quatro perspectivas", realizada pelo portal de notícias especializadas Teletime no dia 23/04/2020, a Vivo confirmou esse posicionamento, ressaltando o compartilhamento somente de dados anônimos, por meio de seu Vice-Presidente de Dados e Inteligência Artificial, Sr. Luiz Médici.

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

Resultado: 

Nesta categoria, a Vivo móvel obteve meia estrela, pois atendeu ao parâmetro III e parcialmente aos parâmetros I e IV.

O parâmetro I, relativo à publicação de relatórios de transparência em português, foi considerado parcialmente atendido. Pelo quarto ano seguido, encontramos a publicação do *Informe de Transparencia en las Comunicaciones de 2019,* do Grupo Telefônica (documento em espanhol), em que há certo detalhamento sobre o conjunto regulatório em cada país no qual o grupo está presente, o número de requerimentos de dados que receberam em cada país entre 2013 e 2017 e, especialmente no caso do Brasil, quais são as autoridades que consideram competentes. Além disso, o Relatório de Sustentabilidade 2019

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. No entanto, pelo fato de a maior parte das informações relevantes serem apresentadas somente em espanhol, no relatório do Grupo Telefônica mencionado, o parâmetro foi considerado parcialmente atendido.

O parâmetro II, relativo à acessibilidade do relatório de transparência, não foi considerado atendido. Isso porque o Relatório de Sustentabilidade não pode ser encontrado na página da Vivo, marca sob a qual a empresa apresenta seus serviços e produtos no Brasil, e, mesmo no site da Telefônica, é necessário buscar o relatório em "A Telefônica" e, depois, "Sustentabilidade". Quanto ao *Informe de Transparencia en las Comunicaciones,* sequer pode ser encontrado na página da Telefônica Brasil, sendo acessível somente pelo site da Telefónica Espanha, em "Negocio Responsable", e, depois, "Informe de Transparência".
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. 20 e 21), informa-se que, em 2018, foram feitos 445.480 requerimentos de interceptação e 3.131.634 requerimentos de acesso a metadados. No entanto, em ambos os casos, não há informação sobre a quantidade de requerimentos rechaçados ou aceitos, afirmando-se que "el sistema de registro durante el período de reporte no disponía de los mecanismos para filtrar por peticiones rechazadas. Se está trabajando para disponer de este dato en los próximos informes." Por isso, 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.

2020

ALGAR

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: ★

Nesta categoria, a Algar obteve estrela cheia, pois atendeu dispõe aos parâmetros I, III e V e parcialmente ao parâmetro II.

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

O sub-parâmetro (a), referente aos dados coletados, foi considerado cumprido. Na seção "Privacidade de Dados Pessoais,", de sua Política de Dados, a empresa informa em uma tabela o tipo de dados coletados (cadastrais), quais são os dados (nome, data de nascimento, dados bancárias etc.) e a finalidade do uso dos dados.

4.1.4 - Tipo de Dados

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

Captura de tela de 27.10.2020

O sub-parâmetro (b), referente às situações em que a coleta ocorre, também foi considerada 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 e-mail 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 exercícios 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 tratamento de Dados Pessoais, além da exibição ou retificação de seus Dados Pessoais, por meio do nosso Canal de Atendimento.

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

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:

● Chat Ajuda Online:
○ www.algartelecom.com.br

● Central de Atendimento:
○ Para Você: 103 12/(34) 9 9884 0123;
○ Micro e pequenas empresas: 0800 942 1212/(34) 9 9779 0112;
○ Médias e grandes empresas: 0800 941 2822/(34) 9 9889 2822.

● Redes Sociais Oficiais:
○ https://www.facebook.com/algartelecom/
○ https://twitter.com/algartelecom/

● Carta:
○ Algar Telecom - Núcleo de retorno ao cliente, Rua José Alves Garcia, 415 Bairro Brasil, Uberlândia MG;

● Portal de Consentimento;
● Encarregado pelo Tratamento de Dados Pessoais (DPO):
○ Alexandre da Silva Simões e-mail:
dpo@algartelecom.com.br

● Ouvidoria:
○ https://www.algar.com.br/ouvidoria/

Governança de Dados Pessoais
4.11 - Diretrizes de resposta às 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.

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 parcialmente atendido, pois a empresa fornece informações claras e completas sobre os sub-parâmetros (b), (c) e (d); e cumpre parcialmente os sub-parâmetros (a), (e) e (f).

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado parcialmente 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 esse país;
> 4.5.3 - Os meios físicos e digitais de armazenamento dos dados pessoais devem assegurar a sua qualidade, devendo ser mantidos exatos e atualizados, de acordo com a necessidade para o cumprimento da finalidade de tratamento;
> 4.5.4 - Quando o titular dos dados pessoais solicitar a correção ou atualização de seus dados pessoais, o encarregado pelo tratamento de dados pessoais, após análise da requisição, deve acionar as áreas responsáveis para assegurar que os meios físicos e digitais onde esses dados pessoais foram replicados e armazenados sejam também atualizados

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

Quanto ao tempo de armazenamento, no mesmo documento, a empresa informa que mantém dados cadastrais e de identificação por até 5 anos após o término da relação. Quanto aos “outros dados”, a empresa afirma armazenar

"enquanto durar a relação e não houver pedido de apagamento ou revogação de consentimento".

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

Captura de tela de 27.10.2020

Assim, como as informações referentes ao tempo de armazenamento foram consideradas insatisfatórias, considerou-se que o sub-parâmetro foi apenas parcialmente atendido.

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":

> 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 casos 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 informa:

> 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 pseudoanonimização, 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.

Em sua Política de Governança de Dados, a empresa informa:

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, pseudoanonimização e anonimização dos dados pessoais quando for o caso;
g) Treinamento em proteção de dados pessoais e supervisão da adoção das práticas ensinadas.

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:

> 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.

A empresa informa, também sobre a hipótese de transferência internacional de dados pessoais:

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.

Enaltecemos a postura da empresa de oferecer informações sobre a transferência internacional de dados e sobre seus critérios para compartilhamento de dados com terceiros, prática não comum na indústria. No entanto, por não especificar os receptores ou tipos de receptores dos dados, o sub-parâmetro foi considerado somente parcialmente cumprido.

Por fim, 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 realizados 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.

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. Por meio de acesso a seu portal como representante de pessoa jurídica, um integrante do InternetLab conseguiu confirmação de que não "há tratamento de dados para este Titular". O InternetLab ressalta que dados pessoais vão além das informações de natureza principalmente cadastral, e que, no caso em questão, havia conhecimento da detenção de tais dados pessoais. No entanto, nessa edição do Quem Defende Seus Dados, por termos obtido sucesso no contato e na averiguação de funcionamento do canal de contato com a empresa, tal parâmetro foi considerado atendido.

Independentemente disso, o InternetLab enaltece o procedimento de exercício do direito de acesso aos dados, que contou com verificação da identidade do titular solicitante, de forma a resguardar sua privacidade e a segurança de suas informações.

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. No entanto, enaltecemos a iniciativa da empresa de manter registrado o histórico de alterações de suas políticas, sinalizando quais itens foram modificados.

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 da Informação", que pode ser acessado no rodapé de seu site, 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 vazia, pois não atendeu a 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 informa apenas que "compartilhar com terceiros e autoridades dentro das hipóteses de cumprimento de obrigação legal ou regulatória, administração pública", sem especificar quais são as autoridades competentes e em quais hipóteses a empresa compartilha os dados sem mandado judicial. Em nenhum dos documentos analisados, a empresa detalha quais são as autoridades competentes para requisitar dados.

Política de Privacidade
4.1.6 - Compartilhamento

2020

> 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.

Essa redação não esclarece ao usuário o tratamento a que estão submetidos seus dados cadastrais, dados de localização e registros de conexão. 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, nas hipóteses previstas em lei. Atualmente, entretanto, em face de controvérsia sobre quais são tais "autoridades administrativas competentes", é imprescindível que a empresa seja transparente acerca de suas práticas e interpretações, no que diz respeito a pedidos de quebra de sigilo, assim como qual o seu entendimento do que considera registros de conexão.

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 Algar, além das cláusulas mencionadas no parâmetro I.

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

O parâmetro IV, referente à promessa de fornecer registros de conexão apenas mediante ordem judicial estritamente nos termos do Marco Civil, também não foi considerado não foi considerado atendido. Não foi encontrada menção ao tema nos documentos analisados da Algar, além das cláusulas mencionadas no parâmetro I.

Por fim, o parâmetro V, relativo à existência de protocolos específicos sobre entrega de dados ao Estado, também não foi considerado não foi considerado atendido. Não foi encontrada menção ao tema nos documentos analisados da Algar, além das cláusulas mencionadas no parâmetro I.

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado:

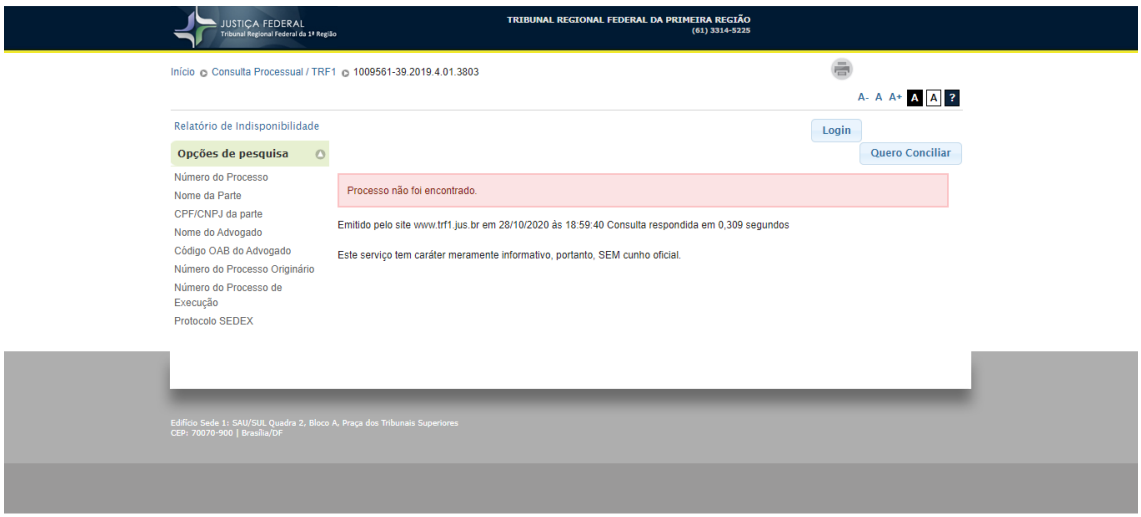
Nesta categoria, a Algar obteve estrela vazia, pois não atendeu a nenhum dos parâmetros.

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. As empresas têm a possibilidade de, durante a fase de discussão dos parâmetros e troca de documentos, comprovar sua atuação nesse sentido.

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

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 01/08/2019 e 31/07/2020. 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.

Na fase de engajamento, a empresa nos informou sobre duas ações em que a empresa foi parte por contestação de pedidos abusivos (Processo n° 1009561-39.2019.4.01.3803, TRF-1 e processo n° 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 1° Região, a ação não foi encontrada.



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 estrela vazia, pois não atendeu a nenhum parâmetro.

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, independentemente das iniciativas diretamente relacionadas à pandemia de COVID-19. O adiamento da entrada em vigor da LGPD é um exemplo nesse sentido.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido. Durante as discussões no Congresso Nacional relativas ao adiamento da LGPD, além disso, não foi encontrada qualquer participação da Algar por meio de comunicados de imprensa, participação das discussões no congresso etc.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, também não foi considerado atendido. Isso porque nenhum posicionamento da empresa pôde ser encontrado, tanto em buscas no Google quanto na mídia especializada, em relação à privacidade dos seus usuários nesse contexto.

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 e atendidos.

As únicas informações sobre dados pessoais que constam no Relatório de Sustentabilidade 2019 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.

> “Em 2019, não foram registrados vazamentos de dados, roubo e/ou perda de informações confidenciais.

> Também mantemos esforços para acompanhar alterações normativas, garantindo que nossa atuação respeite as normas e a legislação brasileira. Estamos nos adequando às exigências da Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, que dispõe sobre o tratamento de informações pessoais, de modo a garantir a privacidade e o sigilo dos dados.
>
> Com o apoio de uma consultoria jurídica externa, avançamos em 2019 para nos adequarmos à nova lei. Contratamos um profissional que passou a se dedicar exclusivamente ao assunto e adquirimos ferramentas tecnológicas, visando mitigar os riscos cibernéticos, assim como realizar a gestão da privacidade no dia a dia da Companhia. A Algar Telecom está comprometida, em todas as suas esferas hierárquicas, com a adequação dos controles tecnológicos, físicos e organizacionais e incorporação de práticas de conformidade com a nova lei de privacidade de dados até 2020, ano em que a lei passará a vigorar". (p. 41)

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.

2020

NEXTEL

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Nextel obteve ¼ de estrela, tendo atendido ao parâmetro III.

A Nextel não atende ao parâmetro I, referente às informações sobre coleta e finalidade, não fornecendo quaisquer informações sobre quaisquer dos sub-parâmetros em seu contrato de Prestação do Serviço Móvel Pessoal.

Mais especificamente, a empresa não fornece quaisquer informações 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, (e) quais são e quais os meios (e.g. e-mails ou links) para exercício dos direitos dos titulares sobre seus dados.

Quanto ao parâmetro II, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, considerou-se, na média, que não foi atendido, já que somente informações o sub-parâmetro (e) foi considerado parcialmente atendido.

Mais especificamente, a empresa não fornece quaisquer informações sobre (a) por quanto tempo e onde os dados pessoais são armazenados; (b) quando/se são apagados; (c) quais práticas de segurança observa; (d) quem tem acesso aos dados; (f) para quais finalidades os dados são compartilhados.

No tocante ao sub-parâmetro (e), em seu Contrato de Prestação do Serviço Móvel Pessoal, a Nextel dispõe:

> "VII – DIREITOS E DEVERES DO ASSINANTE
> 7.1. Além dos direitos previstos nas demais cláusulas deste instrumento e na normatização de regência, o Assinante poderá: a. Ter as informações relativas ao próprio Assinante e constantes do cadastro da NEXTEL, inclusive o Código de Acesso, mantidos em sigilo, as quais somente poderão ser fornecidas nas seguintes hipóteses: (i) ao próprio Assinante ou procurador munido de procuração com poderes específicos para acessar tais informações; (ii) para agência especializada ou banco de dados em face do inadimplemento de obrigações contratuais; e, (iii) em decorrência de determinação administrativa ou judicial."

A cláusula transcrita acima foi considerada excessivamente genérica por não trazer hipóteses claras em que os dados podem ser compartilhados, atividade sabidamente necessária para o bom funcionamento dos serviços de telefonia móvel (e.g. para *roaming,* parceiros comerciais etc.) No entanto, por haver

preocupação com a menção ao tema, o sub-parâmetro foi considerado parcialmente atendido.

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. Por meio de acesso ao portal "Nextel Responde", um integrante do InternetLab conseguiu confirmação, em poucos dias, de que não estava cadastrado como cliente da Nextel. O InternetLab ressalta que dados pessoais vão além das informações de natureza cadastral, e que o efetivo cumprimento ao direito de acesso aos dados pelo seu titular envolveria o compartilhamento de outras e mais detalhadas informações, tais como dados pessoais recebidos de outras operadoras ou de terceiros, dados para e-mail marketing, dados financeiros etc. No entanto, nessa edição do Quem Defende Seus Dados, por termos obtido sucesso no contato e na averiguação de funcionamento do canal de contato com a empresa, tal 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, não foi considerado atendido. Nenhum documento da Nextel mencionava tal possibilidade.

Por fim, o parâmetro V, referente à acessibilidade das informações sobre privacidade e proteção de dados, também não foi considerado atendido. Isso porque nenhuma informação sobre privacidade e proteção de dados pôde ser encontrada de forma acessível no site ou outro ambiente da Nextel.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: ☆

Nesta categoria, a Nextel obteve estrela vazia, pois somente atendeu parcialmente ao parâmetro I.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados, foi considerado parcialmente cumprido. Na mesma cláusula 7.1. do seu Contrato de Prestação do Serviço Móvel Pessoal transcrita acima, item (iii), a Nextel afirma que as informações pessoais do assinante somente poderão ser compartilhadas "em decorrência de determinação administrativa ou judicial." No entanto, por não identificar as autoridades a quem poderia entregar os dados por requisição, o parâmetro foi considerado parcialmente cumprido.

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 Nextel.

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

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 foi encontrada menção ao tema nos documentos analisados da Nextel.

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

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: 

Nesta categoria, a Nextel obteve meia estrela, pois atendeu ao parâmetro I.

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.

No entanto, em fase de engajamento, o InternetLab tomou conhecimento da ação rescisória nº 0802518-50.2020.4.05.0000, perante o TRF5. Nela, as empresas Claro, Vivo, TIM e Oi, mediante atuação pelo Sinditelebrasil questionaram a tentativa de alteração do RGC pela Anatel, que permitia o fornecimento, a qualquer destinatário de ligações telefônicas, de informações pessoais do titular da linha originadora da chamada. Por defenderem a não alteração do referido regulamento com base, entre outros, em argumentos de privacidade e proteção de dados, o parâmetro foi considerado atendido. Por mais que o InternetLab, excepcionalmente, tenha reconhecido a referida ação em vista de sua importância normativa, ressaltamos que, em linha com a averiguação do comprometimento público das empresas sob sua marca, ações iniciadas em nome próprio pelas empresa de telefonia, e não mediante associações ou equivalentes, são preferíveis para a averiguação do cumprimento deste parâmetro.

Ressaltamos que, mesmo a Nextel se tratando de empresa com apresentação de marca distinta da Claro, razão pela qual é avaliada separadamente nesse

relatório, por fazer parte do mesmo grupo econômico, a atuação judicial da Claro também foi considerada, excepcionalmente, para essa categoria da Nextel, e porque eventual vitória teria caráter coletivo, não atingindo somente clientes sob a marca da Claro.

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 "Nextel E sigilo E quebra" e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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 Nextel obteve estrela vazia, pois não atendeu a nenhum dos 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, independentemente das iniciativas diretamente relacionadas à pandemia de COVID-19. O adiamento da entrada em vigor da LGPD é um exemplo nesse sentido.

Após buscas em sites oficiais do governo, imprensa especializada e tradicional e salas de imprensa das empresas, não encontramos nenhum material nesse sentido. Durante as discussões no Congresso Nacional relativas ao adiamento da LGPD, além disso, não foi encontrada qualquer participação da Nextel por meio de comunicados de imprensa, participação das discussões no congresso etc.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, também não foi considerado atendido. Isso porque nenhum posicionamento da empresa pôde ser encontrado, tanto em buscas no Google quanto na mídia especializada, em relação à privacidade dos seus usuários nesse contexto.

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

Resultado:

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

Não foram localizados quaisquer relatórios de transparência da Nextel. Assim, os parâmetros I a IV dessa categoria não puderam ser atendidos.

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

2020

SKY

CATEGORIA 1: Informações sobre a política de proteção de dados

Resultado: 

Nesta categoria, a Sky obteve ¾ de estrela, pois atendeu ao parâmetro I e III, e parcialmente ao parâmetro II.

A Sky, atende ao parâmetro I, pois fornece informações claras e completas sobre os todos os sub-parâmetros.

O sub-parâmetro (a), referente aos dados coletados, foi considerado cumprido. Na cláusula 19 do Contrato de Adesão e na cláusula 7 — que dispõe sobre as obrigações e direitos do cliente — do Contrato de Banda Larga, a empresa informa de maneira clara quais são os dados coletados:

> "19. Privacidade e Coleta de Dados
> 19.1. Serão coletados os dados de identificação fornecidos pelo CLIENTE (tais como: nome, endereço, RG e CPF, números de telefone e endereços de e-mail) e dados relativos à prestação dos Serviços SKY tais como histórico de produtos utilizados ou adquiridos, valores despendidos pelos CLIENTE, número de televisores e seus hábitos de compra/consumo."

> "7. XII - enviar cópia de documentos de identificação pessoal, tais como RG, CPF, comprovante de endereço, de titularidade de conta bancária e de cartão de crédito, dentre outros, tanto no momento da contratação, quanto em momento posterior, desde que solicitado pela OPERADORA"

Em sua Política de Privacidade (vide trecho abaixo), a empresa informa quais dados são coletados e em quais situações a coleta ocorre.

O sub-parâmetro (b), referente às situações em que a coleta ocorre, também foi considerado cumprido. Isso porque a Política de Privacidade da empresa, na seção "2. Informações Coletadas", é informado que os dados podem ser coletados: durante (i) solicitação na primeira interação nas plataformas digitais da Sky; (ii) ao preencher os cadastros relacionados aos serviços da empresa; (iii) durante os usos dos serviços e plataformas; (iv) ao entrar em contato com a Sky; e (v) "dados pessoais disponibilizados por terceiros, desde que legitimamente obtidos". Considerou-se que tais informações são capazes de detalhar as situações em que a coleta ocorre.

> Geralmente, os dados pessoais tratados pela SKY são solicitados em sua primeira interação em nossas plataformas digitais, como, por exemplo, quando você

deseja se cadastrar em nossas plataformas digitais. Ao preencher os cadastros relacionados aos serviços ou plataformas da SKY e ao usar as plataformas e/ou serviços da SKY, você declara ter lido, de forma atenta, todas as condições desta Política, manifestando de forma livre, informada e inequívoca seu desejo de continuar a navegação e o uso dos referidos serviços, e estando ciente de que, para tanto, a SKY tratará seus dados pessoais, para fins de cumprimento das obrigações previstas nos contratos de prestação de serviços em que você é parte ou na legislação em vigor, para garantir a sua segurança nos processos de identificação e autenticação nas plataformas SKY, e/ou para possibilitar o exercício de legítimos interesses da SKY, ou, ainda, para outros fins, quanto aos quais será solicitado seu consentimento, na forma da Lei.
(...)
Quando você utiliza os serviços e plataformas oferecidos pelo grupo SKY para fazer compras, por exemplo, algumas informações sobre a transação e/ou dados associados a ela podem ser coletadas, tais como o valor pago e o meio de pagamento utilizado. Essas informações são tratadas pela SKY principalmente para viabilizar o processamento e envio de avisos de transações, o gerenciamento de riscos e/ou o fornecimento de proteção ao crédito e implementação de medidas antifraude.

Certas informações também podem ser coletadas quando você entra em contato com a SKY, seja através do Serviço de Atendimento ao Consumidor (SAC) ou qualquer outro canal de atendimento, sempre no contexto da prestação dos serviços por você contratados, do cumprimento de obrigações legais ou em situações em que a SKY possui o legítimo interesse de melhorar as suas plataformas e/ou serviços fornecidos, de acordo com as previsões legais aplicáveis.

Com o objetivo de realizar auditorias internas, de garantir proteção ao crédito, implementar medidas antifraude ou assegurar o cumprimento da legislação em vigor, a SKY também pode eventualmente tratar dados pessoais disponibilizados por terceiros, desde que legitimamente obtidos, a exemplo de provedores de dados e agências de crédito, e/ou disponibilizados de forma pública.

Resumindo, a SKY apenas tratará seus dados pessoais nas hipóteses previstas nesta Política; para cumprimento de obrigações contratuais em que você é parte; por força de ordem judicial; mediante seu consentimento manifestado de forma livre, informada e inequívoca, quando necessário; ou nas demais hipóteses autorizadas por Lei.

O sub-parâmetro (c), referente à finalidade do tratamento de dados, foi considerado cumprido. No Contrato de Adesão, a empresa informa apenas que a coleta e uso de dados tem por objetivo proporcionar "a melhor experiência" dos serviços oferecidos pela Sky". No entanto, em sua Política de Privacidade, na seção "Informações Coletadas" (vide trecho acima), a empresa afirma que os dados cadastrais são tratados para "cumprimento das obrigações previstas nos contratos de prestação de serviços em que você é parte ou na legislação em vigor, para garantir a sua segurança nos processos de identificação e autenticação nas plataformas SKY, e/ou para possibilitar o exercício de legítimos interesses da SKY, ou, ainda, para outros fins, quanto aos quais será solicitado seu consentimento, na forma da Lei". Já os dados coletados após compras dos serviços da empresa são tratados para "viabilizar o processamento e envio de avisos de transações, o gerenciamento de riscos e/ou o fornecimento de proteção ao crédito e implementação de medidas antifraude"; já os dados disponibilizados por terceiros são tratados para auditorias internas, garantir proteção de crédito e implementar medidas antifraude. Considerou-se que tais informações são capazes de detalhar as hipóteses de tratamento de dados.

> Contrato de Adesão
> "19. Privacidade e Coleta de Dados
> 19.2. Fica desde já certo e ajustado entre as Partes que a coleta e uso de dados mencionada acima ocorrerá única e exclusivamente para proporcionar ao CLIENTE a melhor experiência de Serviços SKY.

O sub-parâmetro (d), referente à forma como se dá a utilização, foi considerado cumprido. Isso porque a empresa, nos excertos dos contratos mencionados no sub-parâmetro (b), informa algumas finalidades do tratamento de dados, bem como, algumas hipóteses específicas de utilização dos dados.

Por fim, o sub-parâmetro (e), relativo à informação quanto aos direitos dos titulares e meios para exercícios desses direitos, foi considerado atendido. Em sua Política de Privacidade, na seção "Direito dos Usuários", a Sky informa quais são os direitos dos titulares dos dados, como acesso, retificação, anonimização, bloqueio e revogação de consentimento. Ainda, a empresa também oferece um e-mail para o exercício desses direitos e um "portal LGPD", que afirma estar disponível em seu site. No entanto, não encontramos tal portal no site da Sky. Apesar da falha quanto ao portal LGPD, como a empresa oferece um outro meio (o e-mail) para o exercício dos direitos dos titulares dos dados, consideramos o sub-parâmetro cumprido.

> Política de Privacidade
> "8. Direito dos Usuários
> A SKY se preocupa com sua a privacidade e, por conta disso, está comprometida com a proteção de todos os seus direitos dispostos nas legislações sobre privacidade e proteção de dados em vigor. Você possui a faculdade de exercer, por exemplo, os direitos de acesso, de retificação, de anonimização, de bloqueio ou de eliminação de seus

> dados pessoais, bem como de solicitar informação sobre as entidades públicas e privadas com as quais a SKY compartilhou seus dados e/ou a revogação de eventual consentimento fornecido anteriormente e suas consequências, quando assim aplicável.
> Para exercer estes e outros direitos previstos na legislação vigente sobre privacidade e proteção de dados pessoais, pedimos que encaminhe sua solicitação através do e-mail indicado ao final desta Política ou que acesse o link de acesso ao portal LGPD disponível no site www.sky.com.br
> 11. Questões
> Se você tiver questionamentos ou dúvidas em relação a esta Política, ao tratamento de dados realizado pela SKY ou ao exercício de seus direitos relacionados a dados pessoais, por favor, entre em contato conosco através do atendimento@sky.com.br."

Quanto ao parâmetro II, referente ao fornecimento de informações claras e completas sobre a proteção de dados pessoais, considerou-se que foi parcialmente atendido, visto que apenas o sub-parâmetro (b) foi considerado atendido; enquanto os sub-parâmetros (a), (c), (e) e (f) foram considerados parcialmente atendidos.

O sub-parâmetro (a), referente ao tempo e local de armazenamento dos dados, foi considerado parcialmente cumprido. Em sua Política de Privacidade, a empresa informa que "pode" armazenar os dados pessoais dos clientes em nuvem ou infraestruturas similares em servidores de "diversos países". Em virtude da redação ampla e pouco precisa, tal ponto foi considerado insatisfatório.

> Política de Privacidade:
> "3. Compartilhamento de informações
> (...) como de praxe no mercado, a SKY pode armazenar seus dados pessoais em sistema de "nuvem" ou infraestruturas e tecnologias similares, cujos servidores geralmente ficam localizados em diversos países, tais como os Estados Unidos da América (...)."

As informações sobre tempo de armazenamento também não foram consideradas satisfatórias. Nas Condições Gerais de Comunicação consta o prazo mínimo para a manutenção dos dados cadastrais e dos registros de conexão. No entanto, ainda que seja positivo que a empresa estabeleça um prazo mínimo, a ausência de informações sobre o período máximo pelo qual a empresa armazena os dados de seus clientes acaba por tornar demasiado impreciso período de tempo pelo qual os dados são armazenados.

> Condições gerais de comunicação
> "8. Obrigações e Direitos da OPERADORA
> XV - manter os dados cadastrais e os registros de conexão de seus CLIENTES pelo prazo mínimo de três anos."

Quanto ao sub-parâmetro (b), referente a quando/se os dados são apagados, considerou-se que foi atendido. A Sky informa que com o término do tratamento, os dados são eliminados:

> Contrato de Adesão - Serviços de Valor Adicionado
> "9. Privacidade e Proteção de Dados Pessoais
> 9.8. Os dados pessoais tratados pela SKY serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as finalidades definidas em Lei."

O sub-parâmetro (c), relativo às práticas de segurança da empresa, foi considerado parcialmente atendido. Em sua Política de Privacidade, a Sky elenca algumas das medidas de segurança que adota para a preservação da confidencialidade dos dados dos clientes, tais como controle e rastreamento de acesso de usuários e proteção de softwares, como antivírus e firewalls. No entanto, tanto na própria Política de Privacidade, quanto no Contrato de Adesão - Serviços de Valor Adicionado, a empresa que não garante a segurança absoluta dos bancos de dados. Na hipótese de violação ou utilização indevida dos dados, a empresa assume responsabilidade sobre os prejuízos causados ao cliente.

> Política de Privacidade:
> "7. Segurança da Informação
> Para preservar a confidencialidade dos seus dados pessoais, a SKY mantém medidas atualizadas de segurança técnicas, físicas e administrativas projetadas especialmente para o fornecimento de proteção necessária contra perda, divulgação, alteração e quaisquer outras violações aos seus dados pessoais. Dentre essas medidas, incluem-se o controle e rastreamento de acessos de usuários, proteções de softwares (como antivírus e firewalls) e o backup dos dados. Infelizmente, por mais que o nosso sistema seja seguro, é de notório conhecimento no meio tecnológico que nenhum sistema de segurança é completamente impenetrável. Sendo assim, não temos como garantir segurança absoluta de nosso banco de dados e nem podemos garantir que as informações pessoais de identificação que você forneceu não possam ser interceptadas quando a transmissão é feita pela Internet."

> Contrato de Adesão - Serviços de Valor Adicionado
> "9. Privacidade e Proteção de Dados Pessoais
> 9.5. Nos limites fixados na legislação aplicável, a SKY é responsável por qualquer violação e/ou utilização indevida dos dados comprovadamente armazenados em seus bancos de dados e pelos prejuízos que possa vir a causar ao CLIENTE.
> 9.7. Os sistemas e os procedimentos utilizados pela SKY no tratamento de dados pessoais são auditáveis e estruturados de forma a atender os melhores requisitos de segurança e

> aos padrões de boas práticas e de governança, bem como aos princípios gerais previstos nas legislações e regulamentos vigentes, garantindo-se a inviolabilidade da intimidade, da honra e da imagem, bem como adequada proteção contra a perda, mau uso, acesso não autorizado, divulgação e alteração dos dados pessoais do CLIENTE."

As informações em questão foram consideradas demasiadamente genéricas para o cumprimento do sub-parâmetro. A empresa não informa, por exemplo, quais padrões de segurança adota, quais protocolos segue, se utiliza criptografia na transferência dos dados pessoais dos dispositivos dos usuários ou quais são os princípios de segurança da informação que segue.

O sub-parâmetro (d), referente a quem tem acesso aos dados, foi não foi considerado atendido. Em nenhum dos documentos disponíveis no site da empresa encontramos previsões sobre quem tem acesso aos dados. A SKY oferece apenas informações sobre o compartilhamento de dados.

O sub-parâmetro (e), referente aos terceiros com quem os dados são compartilhados, foi considerado parcialmente atendido. Em diversos documentos (Política de Privacidade, Condições Gerais para Empresas, Contrato de Adesão Banda Larga e Contrato de Adesão dos Serviços de Valor Adicionado), a empresa afirma que o compartilhamento de dados ocorre apenas com terceiros integrantes do grupo Sky, ou seja, as empresas controladoras, coligadas ou subsidiárias. Além das empresas integrantes, de acordo com o que consta na cláusula 3 da Política de Privacidade, os dados pessoais podem ser também compartilhados com outros terceiros, apontando a imposição de limites por meio dos termos de confidencialidade e das finalidades expressas contratualmente e nos termos da LGPD:

> Política de Privacidade:
> 3. Compartilhamento de Informações
> A SKY está sempre buscando proporcionar privacidade aos nossos clientes e usuários, portanto, temos como política institucional o não compartilhamento de dados pessoais com terceiros não integrantes do grupo SKY. Fazem parte do grupo SKY suas empresas controladoras, coligadas e subsidiárias. Todavia, para que possamos oferecer nossos serviços e plataformas, determinados dados pessoais poderão ser compartilhados com terceiros não relacionados, sempre respeitando a legislação brasileira em matéria de proteção de dados pessoais. Esse compartilhamento, quando necessário, ocorrerá para finalidades específicas e determinadas, sempre objetivando o correto funcionamento das plataformas e serviços que a SKY disponibiliza a você. Ao utilizar nossas plataformas ou serviços, você manifesta seu desejo de continuar com a navegação ou o uso de referidos serviços, estando ciente de que seus dados pessoais poderão ser compartilhados com terceiros não relacionados, sendo certo que a SKY realizará

tal compartilhamento para fins da execução de obrigações contratuais ou legais; para possibilitar o exercício de um legítimo interesse; e/ou mediante o seu consentimento, quando aplicável, na forma da Lei.

Condições Gerais para Empresas:
17. Disposições Finais
17.5. A SKY respeita a privacidade dos dados pessoais fornecidos pelos CLIENTES, utilizando-se destes apenas para os fins objeto deste Contrato, nos termos da legislação vigente. O CLIENTE autoriza, desde já, o compartilhamento destes dados a empresas fornecedoras de serviços da SKY, que trabalham com a SKY ou em nome da SKY vinculados a acordos de confidencialidade.
17.5.1. As empresas parceiras da SKY poderão, desde que previamente autorizadas pelo CLIENTE, usar os dados pessoais previstos na cláusula retro, com o objetivo de auxiliar a SKY na comunicação estabelecida com o CLIENTE sobre ofertas da própria SKY e/ou de parceiros mercadológicos

Contrato de assinatura banda larga pré-paga:
19. Privacidade e Coleta de Dados
19.3. Os dados mencionados na cláusula 19.1 acima serão transferidos apenas para empresas parceiras e/ou fornecedores da SKY, sendo que tais empresas firmam com a SKY termos de confidencialidade nos quais se comprometem a não repassar a terceiros os dados colhidos dos clientes SKY.

Contrato de Adesão - Serviços de Valor Adicionado
9.3. Os dados pessoais a que se refere a cláusula 9.2 poderão ser transferidos para empresas parceiras, assim entendidas como empresas fornecedoras de bens e serviços à SKY e/ou pertencentes ao mesmo grupo econômico da SKY, bem como para outros terceiros, na forma especificada na "Política de Privacidade SKY" a que se refere a cláusula 9.9, sendo certo que, na transferência de dados pessoais para terceiros, há compromisso por parte do receptor quanto ao integral cumprimento do regime de proteção de dados previsto no ordenamento jurídico brasileiro, bem como de confidencialidade das informações, assegurando-se que não haverá repasse dos dados pessoais do CLIENTE a terceiros não autorizados pela SKY.
9.3.1. Fica desde já estabelecido que, para fins do presente Contrato, os dados pessoais a que se refere a cláusula 9.2. serão transferidos para as EMPRESAS PARCEIRAS, assim entendidas como as empresas fornecedoras dos SERVIÇOS DE VALOR ADICIONADO, sendo certo que, na transferência de dados pessoais para as EMPRESAS PARCEIRAS, há

> compromisso por parte do receptor quanto ao integral cumprimento do regime de proteção de dados previsto no ordenamento jurídico brasileiro, bem como de confidencialidade das informações, assegurando-se que não haverá repasse dos dados pessoais do CLIENTE a terceiros não autorizados pela SKY.

No entanto, as informações acima, mesmo que ofereçam algum guia para quais terceiros têm acesso aos dados, são excessivamente abrangentes. Não determinam especificamente quais terceiros podem recebê-los e não determina quais dados e em quais situações estes são compartilhados. Ainda, a previsão de que "todavia, (...) determinados dados pessoais poderão ser compartilhados com terceiros não relacionados" torna a informação sobre quais são os terceiros demasiadamente imprecisa, já que a empresa não fornece nenhum exemplo ou hipótese de quem seriam esses "terceiros não relacionados" ou quais seriam esses "determinados dados pessoais". 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, quanto ao sub-parâmetro (f), relativo às finalidades do compartilhamento de dados com terceiros, também foi considerada parcialmente atendida. Isso porque as informações trazidas sobre o tema, referenciadas na análise do sub-parâmetro (e) acima, são pouco claras e afirmam somente de forma genérica que os dados podem ser compartilhados para "oferecer nossos serviços e plataformas" ou para "com o objetivo de auxiliar a SKY na comunicação estabelecida com o CLIENTE sobre ofertas da própria SKY e/ou de parceiros mercadológicos". 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 o sub-parâmetro foi considerado parcialmente atendido.

O parâmetro III, que avalia se a empresa respondeu tempestivamente à solicitação de pedidos de acesso aos dados por integrantes do InternetLab, foi considerado cumprido. Por meio de e-mail a atendimento@sky.com.br, um integrante do InternetLab conseguiu confirmação, em poucos dias, de que não estava cadastrado como cliente da Sky. O InternetLab ressalta que dados pessoais vão além das informações de natureza cadastral, e que o efetivo cumprimento ao direito de acesso aos dados pelo seu titular envolveria o compartilhamento de outras e mais detalhadas informações, tais como dados pessoais recebidos de outras operadoras ou de terceiros, dados para e-mail marketing, dados financeiros etc. No entanto, nessa edição do Quem Defende Seus Dados, por termos obtido sucesso no contato e na averiguação de funcionamento do canal de contato com a empresa, tal 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, não foi considerado atendido. A Sky não traz em seus contratos a previsão de notificação o cliente em caso de atualização nas políticas de privacidade, mas compromete-se a divulgar novas versões dos contratos por meio do site da empresa ou meios de

comunicação. No entanto, a empresa garante ao cliente a possibilidade de formalizar a uma oposição fundamentada à nova versão, em um prazo de 30 dias, e garantindo a possibilidade de rescindir o contrato sem penalidade, caso esteja em desacordo com as alterações. Enaltecemos a postura da empresa de garantir aos clientes a possibilidade de se opor às atualizações dos contratos, mas recomendamos que a empresa notifique seus clientes, para que eles possam exercer este direito.

> Condições gerais para empresas:
> 16. Contrato por adesão
> 16.2. A Sky compromete-se a divulgar no site www.sky.com.br e/ou em outros meios de comunicação as novas versões do presente Contrato, ficando facultado ao CLIENTE o direito de formalizar sua oposição, de forma fundamentada, em até 30 (trinta) dias contados da divulgação. Após esse prazo, passam a vigorar as novas condições contratuais.
>
> Contrato pré-pago:
> 3. Programação:
> 3.6. O CLIENTE está ciente de que qualquer alteração da composição do Plano de Serviço por parte da SKY faz parte da natureza dos serviços prestados, bem como está ciente de que poderão ocorrer referidas alterações em razão de modificações na legislação, facultando-se ao CLIENTE o direito de rescindir o Contrato sem qualquer penalidade, obrigando-se a efetuar o pagamento dos valores remanescentes, mediante comunicação à SKY no prazo de 30 (trinta) dias contados da referida alteração, pelo site www.sky.com.br ou atendimento telefônico através do SAC.

Por fim, o parâmetro V, referente à acessibilidade das informações sobre privacidade e proteção de dados, não foi considerado atendido. A empresa não possui nenhum formato alternativo aos contratos em que disponibilize de forma acessível informações sobre privacidade e proteção de dados.

De qualquer forma, enaltecemos o fato de que há facilidade para encontrar os contratos no site da empresa. Estão disponíveis no rodapé da página inicial ("contratos gerais" e “contratos pré-pago”), assim como a política de privacidade. Dessa forma, os clientes não deverão ter muitas dificuldades para encontrar esse tipo de informação. O fácil acesso a essas informações, no entanto, não foi suficiente nesta edição do relatório para que o parâmetro V fosse considerado atendido.

CATEGORIA 2: Protocolos de entrega de dados para investigações

Resultado: 

Nesta categoria, a Sky obteve ¼ de estrela, tendo cumprido parcialmente o parâmetro I.

O parâmetro I, referente à identificação das autoridades competentes para requisitar dados cadastrais, foi considerado parcialmente atendido. Em sua Política de Privacidade, a empresa identifica as autoridades competentes com as quais podem ser compartilhados dados pessoais. No entanto, o rol de autoridades mencionadas não é restritivo; além das autoridades identificadas, o compartilhamento de informações pode ocorrer com diversas outras agências, departamentos, instituições ou entidades públicas que não foram expressamente mencionadas:

> Política de Privacidade:
> 3. Compartilhamento de Informações
> Para cumprimento de obrigações legais e/ou regulatórias aplicáveis à SKY, determinados dados pessoais também podem ser compartilhados com e/ou transferidos às autoridades competentes, tais como, mas não se limitando, ao Banco Central do Brasil – BCB, ao Conselho de Controle de Atividades Financeiras – COAF, à Receita Federal do Brasil, a Birôs de Crédito e às Secretarias Estaduais e Municipais da Fazenda ou quaisquer outras agências, departamentos, instituições ou entidades públicas para quais o envio de referidos dados pessoais seja um obrigação.

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 pode ocorrer, não foi considerado atendido. A empresa se compromete a respeitar as hipóteses e condições constitucionais e legais de quebra de sigilo, sem, no entanto, especificar quais são as hipóteses de quebra de sigilo ou quais são as autoridades competentes. Em virtude dessa redação ampla e da ausência de informações detalhadas sobre o tema, o parâmetro não foi considerado cumprido.

> CONDIÇÕES GERAIS DA PRESTAÇÃO DO SERVIÇO DE COMUNICAÇÃO

> 7.2. Além de outros direitos previstos no presente Contrato e na legislação e regulamentação aplicável, o CLIENTE tem direito:
> V - À inviolabilidade e ao segredo de sua comunicação, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;

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

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 foi encontrada menção ao tema nos documentos analisados da Sky.

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

CATEGORIA 3: Defesa dos usuários no Judiciário

Resultado: ☆

Nesta categoria, a Sky 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. 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 “Sky E sigilo E quebra” e por acórdãos publicados entre 01/08/2019 e 31/07/2020. 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.

Na fase de engajamento, a empresa não contribuiu com o InternetLab, não oferecendo ações judiciais e administrativas em que tenham participado e que pudessem ser consideradas para essa categoria.

CATEGORIA 4: Postura pública pró-privacidade

Resultado: 

Nesta categoria, a Sky obteve ½ de estrela, pois atendeu parcialmente ao parâmetro I.

O parâmetro I, relativo ao posicionamento em geral da empresa, foi considerado parcialmente 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, independentemente das iniciativas diretamente relacionadas à pandemia de COVID-19. O adiamento da entrada em vigor da LGPD é um exemplo nesse sentido.

A empresa participou do painel "Proteção de dados: como combater e mitigar riscos, perdas e danos", no Seminário de Transformação Digital e Cibersegurança. Conforme reportado pela mídia especializada, o *head* de Segurança da Informação da Sky se pronunciou sobre as ações adotadas pela empresa para a adequação à LGPD:

> "A Sky tem uma política de proteção de dados há tempos. Seguimos protocolos da AT&T, que possui foco bem grande na proteção de dados e não apenas na LGPD".
>
> "O principal desafio é a cobertura do programa sobre LGPD. A nossa malha é o Brasil, logo temos clientes do Amazonas até o Rio Grande do Sul. Além disso, como podemos fazer para conscientizar não apenas os consumidores, mas também os nossos parceiros? O que nos preocupa são os parceiros"

Por mais que a iniciativa de participar em debates sobre LGPD e proteção de dados seja louvável, não encontramos detalhes práticos ou concretos sobre o que foi defendido pela empresa no que tange o aumento da proteção conferida aos usuários dos seus serviços.

O parâmetro II, relativo ao posicionamento da empresa no contexto da COVID-19, não foi considerado atendido. Isso porque nenhum posicionamento da empresa pôde ser encontrado, tanto em buscas no Google quanto na mídia especializada, em relação à privacidade dos seus usuários nesse contexto.

Na fase de engajamento, a empresa não contribuiu com o InternetLab, não compartilhando conosco eventos públicos ou participações relevantes que pudessem ser consideradas para essa categoria.

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

Resultado: 

Nesta categoria, Sky obteve meia estrela, pois atendeu aos parâmetros I, II e III.

O parâmetro I, relativo à publicação de relatórios de transparência em português, foi considerado atendido. O grupo AT&T, do qual a Sky faz parte, publica relatórios de transparência em português que traz informação histórica/dados cadastrais dos assinantes e negócios que operam e pedidos de bloqueio de URL/IP pelas entidades governamentais. No Brasil foram feitos os seguintes pedidos:

> "Janeiro - junho/2019
> Informações históricas: dados cadastrais do assinante 1.015
> Bloqueio de IP/URL 1
>
> Julho - dezembro/2019
> Informações históricas: dados cadastrais do assinante 389
> Bloqueio de IP/URL 4".

O parâmetro II, relativo à acessibilidade do relatório de transparência, foi considerado atendido. O Relatório de Transparência pode ser encontrado com facilidade no rodapé da página inicial da Sky. No entanto, vale ressaltar que através da página inicial é possível acessar apenas o último relatório publicado, sendo necessário acessar o site da AT&T para obter os relatórios dos semestres anteriores.

O parâmetro III, relativo à periodicidade do relatório, foi considerado atendido, visto que os relatórios de transparência da empresa são publicados semestralmente.

O parâmetro IV, relativo às informações sobre pedidos de acesso a dados, não foi considerado atendido. O relatório não contém informações mais detalhadas sobre a quantidade de pedidos recebidos, atendidos e rechaçados ou quais as autoridades que considera competentes para tal.

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