CÓDIGO DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA O SETOR DE TELECOMUNICAÇÕES

conexis
brasil.digital

Iniciativa

conexis brasil.digital

Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal

Algar Telecom

Claro

oi

SERCOMTEL TODO MUNDO CONECTADO

TIM

vivo

EQUIPE

Conexis Basil Digital

Marcos Ferrari
(Presidente Executivo)

Natasha Nunes
(Diretora Jurídica)

Maria Eliza Mac-Culloch
(Coordenadora Jurídica)

Daphne Nunes
(Coordenadora Regulatória)

Coordenação científica:

Laura Schertel Mendes
Mônica Tiemy Fujimoto
Isabela Rosal Santos

Membros do Grupo de Trabalho:

Aline Calmon de Oliveira
Alexandre da Silva Simões
Ana Clara Maia
Andrea Mattos
Caiky Avellar
Carlos Pelegrini
Christian Lopes Kratochwil
Cristiane Casagrande
Débora Batista Araújo
Duilio Novaes Alves
Ederson Santos
Jessica Cristina Ferracioli
Isabella Dalla Bernardina De Mingo
Márcia R. Cavalcante
Maria Tereza Ali Pelicano David
Matheus Pereira
Piero Formica
Renata Bertele
Wesley de Oliveira Cabral
Zuleica Pereira Ivo Rodrigues

INTRODUÇÃO

A Conexis Brasil Digital representa as principais prestadoras do setor de telecomunicações do Brasil. Um setor que detém a base de dados de grande parte da população brasileira e soma um total de 340 milhões de acessos, entre telefonia celular, banda larga, telefonia fixa e TV por assinatura. O acesso a informações de milhões de brasileiros requer um cuidado especial com a proteção dos dados desses cidadãos, transmitindo segurança e confiança a todos.

Com a publicação da Lei Geral de Proteção de Dados (LGPD), as empresas do setor tomaram suas iniciativas para atender este direito do brasileiro da melhor forma, enquanto garantiam também a continuidade da prestação de serviços de conectividade e interação nesta era digital. Com o avanço destas práticas e o conhecimento acumulado com os desafios da implantação da lei dentro de cada associada da Conexis, o setor se uniu para trocar informações, construir aprendizados e compartilhar questionamentos através de um grupo de trabalho que estimula o debate da melhor forma de tratar estes dados pessoais.

A evolução das discussões levou à proposta de se elaborar um código de boas práticas do setor de telecomunicações, como previsto no caput do artigo 50 da LGPD, para registrar avanços e incentivar a boa governança e replicação de bons exemplos. Após mais de um ano de muito trabalho e discussões, com apoio de consultoria científica especializada que colaborasse no rigor técnico dos registros, concluímos a elaboração deste manual para a adoção de boas práticas para proteção de dados pessoais e da privacidade.

Este código é mais uma iniciativa das empresas de telecomunicações associadas da Conexis na ampliação das boas práticas com os consumidores e se soma ao Sistema de Autorregulação do Setor de Telecomunicações (SART), lançado em 2020, como um marco para uma regulação efetiva e eficiente estimulando boas práticas como a criação de normativos de atendimento, cobrança e ofertas, além do código de conduta de telemarketing.

Com a conclusão deste código, compartilhamos e damos mais um passo na atuação responsável das empresas para a segurança e a transparência em relação aos titulares de dados pessoais.

Brasília, 30 de agosto de 2022.

Marcos Ferrari
Presidente Executivo

SUMÁRIO

PARTE GERAL 9

1. CONSIDERAÇÕES INICIAIS 11

2. DEFINIÇÕES 13

3. A LEI GERAL DE PROTEÇÃO DE DADOS APLICADA AO SETOR DE TELECOMUNICAÇÕES: CONCEITOS FUNDAMENTAIS 17

4. MARCO NORMATIVO APLICÁVEL AO SETOR 33

5. REGULAÇÃO DO SETOR DE TELECOMUNICAÇÕES NO BRASIL 37

6. AUTORREGULAÇÃO DO SETOR DE TELECOMUNICAÇÕES 45

7. NORMAS QUE DIALOGAM COM A PROTEÇÃO DE DADOS 49

8. ÂMBITO DE APLICAÇÃO 52

9. CICLO DE VIDA DOS DADOS NO SETOR DE TELECOMUNICAÇÕES 54

PROTOCOLOS 57

I - PROTOCOLO PARA ARMAZENAMENTO DE DADOS PESSOAIS 59

II - PROTOCOLO PARA COMPARTILHAMENTO DE DADOS PESSOAIS 67

III - PROTOCOLO PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS 85

IV - PROTOCOLO PARA GARANTIA DO DIREITO DOS TITULARES 97

V - PROTOCOLO PARA REGISTRO DE OPERAÇÕES DE TRATAMENTO 107

VI - PROTOCOLO PARA AVALIAÇÃO DE LEGÍTIMO INTERESSE 109

VII - PROTOCOLO PARA ELABORAÇÃO DE RELATÓRIO DE IMPACTO 113

VIII - PROTOCOLO PARA SEGURANÇA DA INFORMAÇÃO 117

CONCLUSÃO 131

REFERÊNCIAS 133

CÓDIGO DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA O SETOR DE TELECOMUNICAÇÕES

PARTE GERAL

conexis brasil.digital

1. CONSIDERAÇÕES INICIAIS

O presente Código de Boas Práticas tem como objetivo orientar as empresas do setor de telecomunicações na aplicação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD)[1], e representa o compromisso do setor em prol da garantia da privacidade e da proteção dos dados pessoais do indivíduo.

A Conexis Brasil Digital (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal) é uma entidade sindical que reúne as empresas de telecomunicações e de conectividade, que são a plataforma da economia digital, da sustentabilidade e da conexão de todos os brasileiros. Em 2020, a Conexis substituiu a marca do SindiTelebrasil, a fim de acompanhar o movimento de transformação digital pelo qual o mundo está passando, reforçando o propósito do setor de telecomunicações de digitalizar o país e de conectar todos os brasileiros.

O setor de telecomunicações é caracterizado pelo intenso tratamento de dados pessoais, que está no cerne da prestação dos serviços oferecidos pelas empresas deste segmento. Tal fato se deve à conhecida complexidade do setor, que em diversas ocasiões requer o compartilhamento de estruturas físicas, bem como tecnológicas, além do constante acompanhamento de padrões de qualidade, para que os serviços sejam efetivamente prestados e alcancem toda a população.

Nesse sentido, este Código de Boas Práticas tem como objetivo auxiliar os prestadores de serviço de telecomunicações a adotar boas práticas de governança, nos termos do art. 50, da LGPD. Este trabalho explorará o diálogo normativo entre a legislação de proteção de dados, bem como

1 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

as normas regulatórias e outros dispositivos aplicáveis aos processos de tratamento de dados do setor.

A primeira parte se destinará a explorar o marco normativo que permeia o encontro entre a proteção de dados e a regulação setorial, bem como analisará a atuação regulatória e os mecanismos de autorregulação, que marcam o setor. Ademais, serão tratados os principais conceitos da LGPD, o âmbito de aplicação do Código e os principais conceitos da lei aplicados ao setor.

A segunda parte estabelecerá protocolos operacionais, que visam orientar de forma concreta a aplicação da LGPD no setor de telecomunicações. Os protocolos são os seguintes: i) protocolo para armazenamento de dados pessoais; ii) protocolo de compartilhamento de dados; iii) protocolo de transferência internacional de dados; iv) protocolo de garantia do direito dos titulares; v) protocolo para registro de operações de tratamento; vi) protocolo para avaliação de legítimo interesse; vii) protocolo para elaboração de relatório de impacto e; viii) protocolo para segurança da informação.

Sabe-se que o tratamento de dados pessoais pode acarretar inúmeros benefícios, como o aumento do valor das empresas ocasionado pela utilização e desenvolvimento de novas tecnologias, a prestação de serviços públicos mais eficientes e o aumento da qualidade do serviço prestado ao consumidor. Por outro lado, caso o tratamento dos dados seja feito de forma inadequada, efeitos adversos podem ocorrer, tais como incidentes de segurança, prejuízos econômicos, vigilância excessiva e a perpetuação de práticas discriminatórias.

O papel central do tratamento de dados pessoais no âmbito dos serviços de telecomunicações evidencia a importância da aplicação da LGPD, de modo a proteger os dados dos usuários adequadamente e consolidar a confiança da sociedade na infraestrutura de comunicação e nos serviços executados pelas prestadoras. Nesse sentido, o provimento de serviços seguros, confiáveis e que atendam às expectativas dos usuários é, para além de uma obrigação legal, uma atuação estratégica, rumo a um serviço competitivo, inovador e fundado no respeito aos direitos do cidadão.

2. DEFINIÇÕES[1]

Associação Brasileira de Recursos em Telecomunicações (ABR Telecom): entidade com atuação na gestão centralizada de soluções tecnológicas em ambientes compartilhados que atua como Entidade Administradora da Portabilidade Numérica, Entidade Supervisora de Ofertas de Atacado e Entidade Aferidora de Qualidade;

Agência Nacional de Telecomunicações (Anatel): entidade integrante da Administração Pública Federal indireta, submetida a regime autárquico especial e vinculada ao Ministério das Comunicações, com a função de órgão regulador das telecomunicações, com sede no Distrito Federal e unidades regionais;

Agentes de tratamento: o controlador e o operador;

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709/18 (LGPD) em todo o território nacional;

1 Definições extraídas da LGPD, do Marco Civil da Internet, Lei nº 9.472/97, Resolução nº 623/13 da Anatel, Resolução nº 632/14 da Anatel e Resolução nº 654/15 da Anatel.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Conexão à internet: a habilitação de um terminal para envio e recebimento de pacote de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Dado pseudonimizado: dado relativo ao titular que não possa ser identificado, senão pelo uso de informação adicional;

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Plano de Serviço: documento que descreve as condições de prestação do serviço quanto às suas características, ao seu acesso, utilização e facilidades, as tarifas ou preços associados, seus valores e as regras e critérios de sua aplicação;

Prestadora (de serviço de telecomunicação): pessoa jurídica que, mediante concessão, permissão ou autorização, presta serviço de telecomunicações de interesse coletivo;

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação mantida separadamente pelo controlador em ambiente controlado e seguro;

Registro de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP;

Registro de conexão: 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 pacote de dados;

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos;

Serviço de nuvem (cloud): modelo de armazenamento de dados na internet que utiliza um provedor de computação na nuvem para gerenciar as informações;

Terminal: o computador ou qualquer dispositivo que se conecte à internet;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

3. A LEI GERAL DE PROTEÇÃO DE DADOS APLICADA AO SETOR DE TELECOMUNICAÇÕES: CONCEITOS FUNDAMENTAIS

3.1. Conceito de dado pessoal

Os dados pessoais são conceituados na LGPD em duas categorias, os dados pessoais e os dados pessoais sensíveis. Nos termos do art. 5º, I, são dados pessoais toda informação relacionada a pessoa natural identificada ou identificável. Já os dados pessoais sensíveis são aqueles que versam "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II).

A distinção entre as duas categorias de dados pessoais justifica-se pelo maior potencial discriminatório que o tratamento de dados sensíveis acarreta. Por esse motivo, também foram definidas bases legais para tratamento diferenciadas para cada categoria de dado, conforme se verá no próximo tópico.

No quadro abaixo, apresentamos os principais tipos de dados do setor[1]:

1 Lista meramente exemplificativa.

3.2. Princípios de proteção de dados pessoais

Os princípios da proteção de dados, presentes no art. 6º, LGPD, são parâmetros fundamentais para nortear o tratamento de dados e devem ser observados ao longo de todo tratamento de dados pessoais realizados por organizações. São eles:

BOA-FÉ OBJETIVA (*art. 6º, caput*)	O tratamento de dados deve ser pautado nos ditames éticos e morais.
FINALIDADE (*art. 6º, I*)	O tratamento deve ter como finalidade propósitos legítimos, específicos, explícitos e informados ao titular em toda a sua duração. Caso a finalidade se altere ao longo do processo, este deve ser compatível com essas finalidades.
ADEQUAÇÃO (*art. 6º, II*)	O tratamento deve ser compatível com as finalidades informadas ao titular.
NECESSIDADE (*art. 6º, III*)	O tratamento deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
LIVRE ACESSO (*art. 6º, IV*)	Os titulares dos dados devem poder consultar a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Tal direito não se estende aos dados inferidos.
QUALIDADE DOS DADOS (*art. 6º, V*)	Os dados dos titulares devem ser exatos, claros, relevantes e atualizados.
TRANSPARÊNCIA (*art. 6º, VI*)	Devem ser disponibilizadas aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
SEGURANÇA (*art. 6º, VII*)	Os dados pessoais devem ser protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, por meio de medidas técnicas e administrativas.
PREVENÇÃO (*art. 6º, VIII*)	É necessário prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
NÃO DISCRIMINAÇÃO (*art. 6º, IX*)	O tratamento de dados não deve ser realizado para fins discriminatórios ilícitos ou abusivos.
RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS (*art. 6º, X*)	O agente deve adotar medidas eficazes e deve ser capaz de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

3.3. Bases legais para o tratamento de dados pessoais

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) estabelece um sistema que considera todos os dados pessoais como bens jurídicos tutelados e, dessa forma, protegidos do tratamento ilegítimo que possa comprometer direitos como autodeterminação informativa e não discriminação dos titulares. De acordo com a LGPD, portanto, todo tratamento de dados pessoais deve estar amparado por uma das bases legais presentes em seus artigos 7º e 11.

No primeiro dispositivo mencionado (art. 7º) são definidas as bases legais que justificam o tratamento de dados pessoais não sensíveis, assim definidas:

- Consentimento
- Cumprimento de obrigação legal e regulatória
- Execução de políticas públicas pela administração pública
- Realização de estudos por órgão de pesquisa
- Exercício regular de direitos
- Proteção da vida ou da incolumidade física
- Tutela da saúde
- Execução contratual
- Legítimo interesse
- Proteção de crédito

Importa ressaltar que a utilização do consentimento deve ser realizada por meio de manifestação livre, informada e inequívoca do titular, que deve concordar com o tratamento de dados para determinada finalidade. Caso essa finalidade se altere ao longo do processo de tratamento de dados, o titular deve ser informado sobre a alteração.

Ademais, importa destacar que o consentimento previsto na LGPD não é idêntico ao consentimento previsto no Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações - RGC. Isso porque o consentimento do RGC é mais específico e está relacionado somente ao recebimento de mensagens de cunho publicitário pela prestadora e não ao tratamento de dados em geral. O RGC traz também os requisitos de validade do consentimento, devendo o consentimento ser prévio, livre e expresso. Em relação à categoria dos dados, a LGPD estabelece um nível de proteção mais forte para os dados pessoais sensíveis, em razão do seu potencial discriminatório e de consequências negativas do mau uso de tais informações. Por isso, no art. 11 da LGPD são elencadas as bases legais que podem ser utilizadas para tratamentos envolvendo dados pessoais sensíveis, que

apresentam algumas diferenças das bases previstas no art. 7º, como por exemplo a impossibilidade da utilização do legítimo interesse como base legal ou os requisitos adicionais do consentimento, que deve ser específico e destacado. As bases legais que justificam o tratamento de dados pessoais sensíveis são as seguintes:

- Consentimento específico e destacado
- Cumprimento de obrigação legal e regulatória
- Execução de políticas públicas pela administração pública
- Realização de estudos por órgão de pesquisa
- Exercícios regular de direitos
- Proteção da vida ou da incolumidade física
- Tutela da saúde
- Garantia da prevenção à fraude e à segurança do titular

Ademais, também existem hipóteses de cumprimento de obrigação regulatória para outras atividades de tratamento, como armazenamento de dados e compartilhamento, conforme será descrito em detalhes nos protocolos que constam na Parte II deste Código. A base legal do cumprimento de obrigação legal e regulatória é extremamente importante para o setor, podendo embasar diversas atividades de tratamento que são realizadas, por exemplo, para realização de fiscalização regulatória.

3.4. Direitos dos titulares

A efetiva proteção dos dados pessoais do titular depende da observância dos princípios (tópico 3.2.) e dos direitos do titular (arts. 9º ,18 a 22 LGPD). O principal objetivo da previsão de direitos do titular é permitir o controle do fluxo de seus dados, bem como ampliar a transparência do tratamento. Os direitos básicos atribuídos ao titular pelas diversas

legislações nacionais e tratados internacionais são conhecidos pela sigla "ARCO", abreviação de: acesso, retificação, cancelamento e oposição.[2]

A LGPD prevê um rol extenso de direitos do titular para além dos direitos básicos, que estão estabelecidos em seus arts. 9º, 18 e 20, conforme abaixo:

- Acesso facilitado às informações
- Confirmação da existência de tratamento
- Acesso aos dados
- Correção de dados incompletos, inexatos ou desatualizados
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com regulamentação da ANPD, observados os segredos comercial e industrial
- Eliminação dos dados pessoais tratados com o consentimento do titular salvo exceções legais
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
- Revogação do consentimento
- Oposição ao tratamento irregular
- Revisão de decisões automatizadas
- Petição perante a ANPD ou perante os organismos de defesa do consumidor (Art 18 1 º LGPD)

2 SCHERTEL, Laura. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. In: **Panorama setorial da Internet**, nº 2, junho/2019, ano 11.

A arquitetura de proteção de dados pessoais desenhada pelo ordenamento jurídico e consubstanciada na jurisprudência assegura a observância da autodeterminação informativa, fundamento da disciplina de proteção de dados (art. 2º, II, da LGPD). Busca-se o equilíbrio entre o controle dos dados pelo titular e o fluxo de dados inerente à sociedade da informação, tendo o titular controle sobre seus dados pessoais e o tratamento a eles realizado.

Os direitos previstos na LGPD não são absolutos e devem ser interpretados considerando outros direitos fundamentais, bem como o contexto em que se inserem. Diferentes jurisdições entendem que nem todos os direitos previstos nas normas de proteção de dados pessoais podem ser exercidos em todas as situações de tratamento de dados pessoais. A autoridade nacional de proteção de dados do Reino Unido (*Information Commissioner's Office* - ICO), por exemplo, compreende que o direito de acesso a informações pode ser limitado se o indivíduo já tiver tais dados ou se o fornecimento de tais informações exigir esforço desproporcional[3].

Outros diplomas normativos brasileiros contêm direitos para o cidadão sobre seus dados, estando especialmente presente na regulamentação do setor de telecomunicações, como por exemplo, no Código de Defesa do Consumidor ("CDC" ou Lei nº 8.078/1990)[4]. O Marco Civil da Internet (Lei nº 12.965/2014), por sua vez, estabelece uma série de prerrogativas e direitos aos usuários da Internet. Uma tutela de escopo mais amplo, porém igualmente voltada para a proteção de dados pessoais, pode ser observada no próprio Código Civil, incidindo a partir da proteção dos direitos de personalidade e da tutela dos direitos subjetivos.[5]

É possível perceber uma grande convergência entre esses diplomas, cujo objetivo central é a proteção da pessoa, devendo cada uma das legislações ser aplicada no seu contexto específico. A Lei Geral de Proteção de Dados, porém, deve ser entendida como a regulação geral no fluxo de dados no país, inclusive os dados que tenham sido coletados em território nacional, função essa que não se confunde com a de outras legislações nacionais.

3 Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf.

4 Art. 43, Lei 8.078/1990 (CDC): "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".

5 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

3.4. Agentes do tratamento

Nos termos da LGPD, o agente de tratamento - o controlador ou o operador - pode ser pessoa natural ou jurídica, tanto de direito público, como de direito privado. O controlador é o responsável pelas decisões referentes ao tratamento de dados pessoais; já ao operador compete a realização de tratamentos de dados pessoais em nome do controlador.

As situações nas quais uma pessoa física assume o papel de agente de tratamento são específicas e terão um tratamento diferenciado definido pela ANPD, sendo necessário distinguir o operador dos funcionários que estão agindo sob a direção do controlador[6]. Já nos cenários mais corriqueiros, uma pessoa jurídica irá ocupar as funções dos agentes de tratamento; nesses casos, a organização assumirá o papel, não sendo necessária a representação por qualquer funcionário ou sócio da empresa.[7]

Além disso, a definição do papel ocupado por cada agente envolvido naquele determinado processo é feita a partir da avaliação de cada atividade. Ou seja, uma organização pode desenvolver o papel de operador em determinado tratamento que envolve outra organização e, em outro processo, esses papéis podem ser invertidos. Esse é mais um dos motivos que justificam a necessidade de manutenção de registro das operações de tratamento de dados realizadas (art. 37, LGPD), obrigação compartilhada por ambos os agentes de tratamento.

A classificação enquanto controlador ou operador muitas vezes é prevista nos instrumentos contratuais, mas também é possível que o arranjo seja estipulado por meio de outras formas de interação empresarial. Contudo, independentemente de acordos estabelecidos entre os agentes de tratamento, o que é essencial para determinar se uma organização está atuando como controladora dos dados é justamente o **poder de decisão** sobre os tratamentos realizados. Para a caracterização do mencionado poder decisório, é necessário o controle sobre os elementos essenciais

6 LAPIN. Cartilha 'controlador ou operador: quem sou eu? Disponível em: https://lapin.org.br/2021/04/09/cartilha-controlador-ou-operador-quem-sou-eu/.

7 ANPD. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em 06/08/2021.

do tratamento, como a definição da finalidade do tratamento, da natureza dos dados pessoais tratados e a duração do processo.[8]

A depender da situação também pode ocorrer controle conjunto dos dados (co-controle), situação na qual ambos os controladores respondem de forma solidária na reparação de danos ao titular (art. 42, §1º, II). Ainda que o critério para definição do controle conjunto não esteja expresso na LGPD, entende-se que o reconhecimento de sua existência pode ser inferido do nosso sistema de proteção de dados e sua definição pode ser inspirada na definição do Regulamento Geral sobre Proteção de Dados europeu (GDPR).[9]

De acordo com tal definição, a controladoria conjunta pode ser identificada "quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento" (art. 26, GDPR). Cumpre destacar que não é necessário que todos os elementos do tratamento de dados sejam determinados de forma coletiva, e sim que se observe a existência de finalidades comuns, complementares ou ao menos convergentes do tratamento.

Ademais, em caso de atuação do operador fora do escopo das determinações do controlador em relação aos elementos essenciais do tratamento, o operador atua como verdadeiro controlador, fazendo com que o operador se equipare ao controlador e possa, inclusive, responder pelos danos causados.[10]

3.5. Obrigações dos agentes de tratamento

Como mencionado no tópico anterior, a definição do papel desempenhado por cada agente em determinado tratamento de dados é essencial para fins de distribuição de responsabilidade e para compreender quais são as obrigações de cada entidade envolvida naquela cadeia de tratamento.

8 Ibidem.

9 Ibidem.

10 Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - **o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador,** hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

Algumas dessas atribuições são comuns a todos os agentes, mas outras são específicas para cada papel, devido às peculiaridades de sua atuação[11].

São considerados deveres comuns dos operadores e dos controladores:

- Conformidade com os **princípios** da LGPD
  - Atenção especial ao princípio da transparência, uma vez que ao longo da lei são estabelecidas diversas obrigações ao controlador referentes a esse princípio, tais como: disponibilização da identificação do controlador e de informações de contato desse agente (art. 9º), adoção de medidas de transparência do tratamento de dados baseados em legítimo interesse (art. 10, §2º)
- Implementação de **medidas de segurança técnicas e organizacionais** (art. 46 e 47, LGPD)
  - Os agentes de tratamento respondem pelos danos decorrentes da violação da segurança dos dados quando derem causa ao dano e deixarem de adotarem as medidas de segurança previstas no art. 46 (art. 44, par. único, LGPD)
- **Registro** de operações de tratamento de dados pessoais (art. 37)
- Observância das regras de **transferências internacionais**

Nesse sentido, são considerados obrigações dos operadores:

- Cumprir com as instruções do controlador sobre o tratamento de dados (art. 39, LGPD)
- Notificação de incidentes de segurança ou possível violação de proteção de dados ao controlador
- Reparar os danos causados em razão do exercício de atividade de tratamento de dados pessoais, quando este descumprir com suas obrigações ou não seguir as orientações do controlador (art. 42, caput e §1º, I, LGPD)

11 LAPIN. Cartilha 'controlador ou operador: quem sou eu? Disponível em: https://lapin.org.br/2021/04/09/cartilha-controlador-ou-operador-quem-sou-eu/

Por outro lado, compreende-se como obrigações do **controlador**:

- Manutenção do **ônus da prova** de que o consentimento do titular foi obtido em conformidade com a LGPD (art. 8º, §2º, LGPD)
  - Em caso de mudança de finalidade, o controlador deverá informar previamente o titular, momento em que o indivíduo poderá revogar o consentimento (art. 9º, §2º, LGPD)
- Observância dos **direitos dos titulares** (art. 18)
  - A requisição do titular para o exercício de direitos pode ser direcionada a qualquer um dos agentes de tratamento envolvidos naquele processo, mas é dever do controlador executá-lo.
- **Comunicação de incidentes de segurança que possam acarretar risco ou dano relevante** à ANPD e aos titulares afetados (art. 48, LGPD)
- Elaboração de **Relatório de Impacto de Proteção de Dados** (art. 38, LGPD)
- Nomeação de **encarregado** de dados (art. 41, LGPD)
- Implementação de **programa de governança** em privacidade com os requisitos previstos no art. 50, §2º, LGPD

3.6. Função e atribuições do encarregado

O encarregado (ou, em algumas empresas denominado *data protection officer – DPO*) faz parte do ecossistema de proteção de dados e é essencial para demonstração de adequação de uma organização às regras impostas pela LGPD. Este ator tem como principal função atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Por isso, compreende-se que o encarregado assume papel duplo nas organizações, na medida em que protege tanto os interesses da empresa quanto dos titulares.

Ainda que a LGPD traga como dever para os controladores a indicação de um encarregado, a ANPD ainda irá determinar critérios para a obrigação de

indicação de encarregado (Art. 41, §3º, LGPD). É possível que em determinadas situações o operador também indique um encarregado pelo tratamento de dados pessoais, a depender da natureza, volume e sensibilidade.

Contudo, não restam dúvidas de que todas as prestadoras sujeitas ao âmbito de aplicação deste código deverão indicar um encarregado, seja pelo seu porte, pela centralidade que o tratamento de dados tem nos seus serviços e mesmo pelo fato de que atuam em grande parte de suas atividades de tratamento como controladores[12].

O encarregado pode ser parte da equipe interna da organização ou contratado externamente, mas é importante garantir-lhe algum grau de independência funcional. Isso porque é fundamental que esse agente seja ouvido e possa influenciar a administração da empresa, principalmente no desenvolvimento de novos produtos e na tomada de decisões relacionadas à privacidade.

Nesse mesmo sentido, é necessário garantir que a atuação do encarregado dentro da empresa não gere conflito de interesse com as suas atribuições legais. Diante disso, é considerada uma boa prática a adoção de medidas internas, a fim de mitigar eventual conflito de interesses, tais como: delimitação das funções do encarregado; definição do posicionamento do encarregado dentro da organização; esclarecimento sobre os limites da confidencialidade entre o encarregado e a empresa; não indicação de funcionários com atribuições comerciais para essa função.

Tendo em vista que o encarregado não tem poder direto de decisão quanto às atividades de tratamento de dados, ele não assume qualquer responsabilidade pelas ações da empresa, salvo, apenas, se agir comprovadamente de má-fé.

O encarregado pode ser representado por uma única pessoa ou por uma equipe. Além disso, é possível a indicação de um único encarregado para o mesmo grupo econômico, desde que cumpra com as funções

12 Destaca-se que a ANPD editou Resolução CD/ANPD nº 2/2022 estabelecendo regras específicas para micro e pequenas empresas, na qual isenta as empresas de pequeno porte de indicar encarregado, desde que seja disponibilizado um canal de comunicação que aceite reclamações e comunicações dos titulares, preste esclarecimentos e adote providências (art. 41, § 2º, I da LGPD).

determinadas pela LGPD. Tampouco é obrigatória a dedicação exclusiva do encarregado para essa função, podendo assumir outros encargos relacionados, como na área jurídica ou de segurança da informação de determinada organização.

Contudo, considerando a elevada quantidade de atividades de tratamentos de dados realizadas pelo setor de telecomunicações, é recomendável que pelo menos uma pessoa atue exclusivamente nessa função, ainda que na liderança de uma equipe, a fim de cumprir com as diferentes atribuições desse papel, como:

- Atuar como **ponto de contato entre a ANPD e a entidade que representa** (art. 41, §2º, II, LGPD)
- Atuar como **ponto de contato entre os titulares de dados e a entidade que representa** (art. 41, §2º, I, LGPD)
- **Aconselhar a empresa** em assuntos relacionados à proteção de dados pessoais
- Engajar a empresa no ***compliance* de privacidade** (art. 41, §2º, III, LGPD)

Ademais, é imprescindível que o encarregado tenha conhecimentos técnicos e atualizados sobre os temas relacionados à proteção de dados. Isso traz implicações para a entidade que o indicou, porque essa empresa deverá incentivar e proporcionar meios para a capacitação e atualização do profissional. Outra atuação essencial por parte da empresa é o oferecimento de recursos adequados para o cumprimento de todas as funções indicadas para esse agente.

Além dessa incumbência de patrocínio e incentivo ao encarregado, a LGPD ainda traz a obrigatoriedade de a empresa oferecer uma forma de contato com o encarregado publicamente, de preferência no sítio eletrônico do controlador (art. 41, §1º, LGPD). Sobre esse ponto é relevante a compreensão de que esse contato não precisa ser uma ponte direta com o encarregado, sendo suprida tal obrigação a partir da publicação sobre os contatos com a equipe do encarregado. Tampouco é necessário disponibilizar

informações ao público sobre a sua identificação. Entende-se, assim, que esse encargo foi atendido se há a disponibilização de e-mail impessoal do canal do encarregado (p.ex. dpo@empresarelacionada.com.br) ou com o oferecimento de plataforma de envio de mensagens para essa equipe.

Ressalta-se que, muitas vezes, os canais de comunicação do encarregado recebem alguma solicitação não relacionada à proteção de dados. Por essa experiência, é legítimo que as empresas adotem formas de filtragem das comunicações para garantir o correto encaminhamento de cada solicitação.

3.7. Autoridade Nacional de Proteção de Dados - ANPD

A Autoridade Nacional de Proteção de Dados, recém-constituída no Brasil, teve a sua estrutura regimental definida pelo Decreto nº 10.474/2020. Nesse sentido, sua agenda regulatória ainda está em processo de implementação, estando pendentes aspectos como a definição de diretrizes para transferência internacional, portabilidade, avaliação de risco de incidentes de segurança, dentre outros.

Há inúmeros temas na LGPD que precisarão ser regulamentados pela autoridade, tais como prazos para resposta aos pedidos dos titulares; prazos para a notificação de incidentes de segurança; nível de proteção de dados de país estrangeiro e definição de cláusulas padrão.

Faz-se necessário reconhecer os esforços que a autoridade vem envidando nos primeiros anos de implementação da LGPD para consolidar sua estrutura e iniciar suas ações em um modelo responsivo, especialmente com a entrada em vigor dos artigos da LGPD que tratam das sanções administrativas. Tais penalidades estão previstas no art. 52 da mesma lei e são bastante diversas, existindo, por exemplo, a possibilidade de advertência, aplicação de multa ou mesmo a suspensão parcial ou total das atividades que envolvem o tratamento de dados. As sanções previstas no art. 52 da LGPD são as que seguem:

- **advertência**, com indicação de prazo para adoção de medidas corretivas
- **multa simples e multa diária**, observando o limite de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração
- **publicização** da infração após devidamente apurada e confirmada a sua ocorrência
- **bloqueio** dos dados pessoais a que se refere a infração até a sua regularização
- **eliminação** dos dados pessoais a que se refere a infração
- **suspensão** do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período
- **proibição parcial ou total** do exercício de atividades relacionadas a tratamento de dados

Assim, acredita-se que a ANPD caminha para consolidar um marco regulatório brasileiro de proteção de dados robusto e técnico, buscando a coordenação com órgãos e entidades específicas de setores regulados. As recentes resoluções editadas - Resoluções CD/ANPD nº 1/2021 e 2/2021 – evidenciam o esforço de concretizar a interpretação da LGPD, trazendo mais segurança jurídica para os regulados. Além disso, a ANPD criou um fluxo para petições dos titulares, de modo a incentivar que o titular entre em contato com o controlador antes de enviar à ANPD sua petição[13]. Outra iniciativa que merece destaque foi a edição da Medida Provisória nº 1.124/2022 que representou importante passo no fortalecimento da ANDP, ao transformá-la em autarquia de natureza especial, conferindo maior autonomia à sua atuação.

13 ANPD. *Petição de Titular*. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados.

4. MARCO NORMATIVO APLICÁVEL AO SETOR

Por se tratar de setor altamente regulado, faz-se necessário listar os principais decretos, leis e resoluções da Anatel, relevantes para análise de matérias relacionadas à proteção de dados pessoais. Assim, apresentamos um rol não exaustivo do marco normativo aplicável ao setor, que poderá ser atualizado posteriormente.

- Lei nº 9.472, de 16 de julho de 1997 (Lei Geral das Telecomunicações, LGT) – Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995.

- Lei nº 8.078, de 11 de setembro de 1990 - Dispõe sobre a proteção do consumidor e dá outras providências.

- Lei nº 10.703, de 18 de julho de 2003 - Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências.

- Decreto nº 6.523, de 31 de julho de 2008 - Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para fixar normas gerais sobre o Serviço de Atendimento ao Consumidor (SAC).

- Lei nº 12.414, de 9 de junho de 2011 (Lei do Cadastro Positivo) - Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para a formação de histórico de crédito.

Resoluções ANPD

- Resolução CD/ANPD nº 2, de 27 de janeiro de 2022 - Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

- Resolução CD/ANPD nº 1, de 28 de outubro de 2021 - Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.

Resoluções e Portarias ANATEL

- Resolução nº 73, de 25 de novembro de 1998 – Aprova o Regulamento dos Serviços de Telecomunicações.

- Resolução nº 426, de 9 de dezembro de 2005 - Aprova o Regulamento do Serviço Telefônico Fixo Comutado (STFC).

- Resolução nº 460, 19 de março de 2007 - Aprova o Regulamento Geral de Portabilidade (RGP).

- Resolução nº 477, de 7 de agosto de 2007 - Aprova o Regulamento do Serviço Móvel Pessoal (SMP).

- Resolução nº 581, de 26 de março de 2012 - Aprova o Regulamento do Serviço de Acesso Condicionado (SeAC) bem como a prestação do Serviço de TV a Cabo (TVC), do Serviço de Distribuição de Sinais Multiponto Multicanal (MMDS), do Serviço de Distribuição de Sinais de Televisão e de Áudio por Assinatura via Satélite (DTH) e do Serviço Especial de Televisão por Assinatura (TVA).

- Resolução nº 600, de 08 de novembro de 2012 - Aprova o Plano Geral de Metas de Competição (PGMC).

- Resolução nº 614, de 28 de maio de 2013 - Aprova o Regulamento do Serviço de Comunicação Multimídia e altera os Anexos I e III do Regulamento de Cobrança de Preço Público pelo Direito de Exploração de Serviços de Telecomunicações e pelo Direito de Exploração de Satélite.

- Resolução nº 632, de 7 de março de 2014 – Aprova o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações (RGC).[1]

- Resolução nº 654, de 13 de julho de 2015 - Aprova o Regulamento das Condições de Aferição do Grau de Satisfação e da Qualidade Percebida Junto aos Usuários de Serviços de Telecomunicações.

- Resolução nº 717, de 23 de dezembro de 2019 - Aprova o Regulamento de Qualidade dos Serviços de Telecomunicações (RQUAL).

- Resolução nº 740, de 21 de dezembro de 2020 - Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações.

- Resolução nº 746, de 22 de junho de 2021 - Aprova o Regulamento de Fiscalização Regulatória.

1 Conforme mencionado, o RGC se encontra em processo de revisão, podendo ser alterado após a publicação deste guia.

5. REGULAÇÃO DO SETOR DE TELECOMUNICAÇÕES NO BRASIL

5.1. Introdução

A estruturação de programas de *compliance* de dados em setores regulados apresenta um desafio adicional, uma vez que, além de adequar as suas atividades de tratamento ao disposto na legislação sobre proteção de dados pessoais, é necessário cumprir com disposições regulatórias que também tratam da temática. Por isso, é importante compreender as peculiaridades de cada setor em áreas altamente reguladas, como é o caso do setor de telecomunicações.

No caso da regulação dos serviços de telecomunicações no Brasil, tendo em vista a competência da União para exploração dos serviços, os agentes econômicos que pretendem atuar no setor devem realizá-lo mediante autorização, concessão ou permissão de exploração de tais serviços[1]. Com o objetivo de organizar a exploração dos serviços de telecomunicações e possibilitar o desenvolvimento do setor, bem como garantir o acesso aos serviços de telecomunicações de qualidade por toda a população, foi criada a Agência Nacional de Telecomunicações (Anatel), por meio da Lei nº 9.472/1997.

Compete à Agência adotar medidas para o desenvolvimento das telecomunicações no Brasil, inclusive por meio da expedição de normas sobre prestação de serviços de telecomunicações no regime privado e da deliberação na esfera administrativa quanto à interpretação da legislação de telecomunicações e sobre os casos omissos[2]. Conforme

1 Art. 21, XI, CF. - explorar, diretamente ou mediante autorização, concessão ou permissão, os serviços de telecomunicações, nos termos da lei, que disporá sobre a organização dos serviços, a criação de um órgão regulador e outros aspectos institucionais;

2 Art. 19, incisos X e XVI, da Lei 9.472/97.

será observado em detalhes ao longo deste Código, diversos aspectos da prestação de serviços de telecomunicações normatizados pela Anatel, bem como do processo de fiscalização da Agência envolvem o tratamento de dados. Isso inclui o compartilhamento de dados, sobretudo para atender as solicitações de informações e documentos feitas pela Agência.

Além disso, nos processos administrativos instaurados pela Reguladora, nos quais a prestadora, em exercício de seu direito de defesa ou atendendo a requisição de apresentação de determinadas informações, também é realizado tratamento de dados pessoais. Ademais, as exigências regulatórias também requerem atividades de armazenamento e tratamento específico que são necessários para possibilitar o aumento da competitividade e da qualidade dos serviços prestados, inclusive no escopo de políticas públicas estudadas pela Agência.

Dessa forma, a adequação do setor à LGPD também requer a compreensão dessas atribuições legais e vai além dos tratamentos de dados pessoais por parte ou de iniciativa das prestadoras, sendo em grande medida decorrente da obrigação de atendimento de solicitações da ANATEL ou outros órgãos, como o Ministério das Comunicações, CADE; não deixando de mencionar as demandas judiciais e extrajudiciais, envolvendo PROCONs e afins.

5.2. Atuação da Anatel como órgão regulador e seu papel no tratamento de dados pessoais

A Anatel é entidade integrante da Administração Pública Federal indireta, submetida a regime autárquico especial, vinculada ao Governo Federal, mais especificamente ao Ministério das Comunicações. O processo normativo do Órgão Regulador é observado nas Resoluções, Portarias, Decretos e demais normativos expedidos e disponíveis para consulta em seu portal na Internet, estando a entidade caminhando para responsividade.

Nesse processo de regulação, a utilização de dados pessoais dos usuários dos serviços prestados encontra-se presente em diversas resoluções da Agência, como, por exemplo o Regulamento do Serviço Telefônico Fixo Comutado (Resolução nº 426/2005), Regulamento do Serviço Móvel Pessoal (Resolução nº 477/2007) e o Regulamento do Serviço de Comunicação Multimídia (Resolução nº 614/2013) e o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações – RGC (Resolução nº 632/2014). Ademais, mesmo antes da entrada em vigor da LGPD, já existia a Política de Governança de Dados da Agência Nacional de Telecomunicações (Portaria nº 1.502/2014), que tem como objetivo o aumento da eficiência na gestão de dados e a minimização dos riscos operacionais (art. 1 º).

Com a entrada em vigor da LGPD e dada a importância do tratamento de dados para as atividades regulatórias desempenhadas pela Anatel, foram adotadas algumas medidas importantes para adequar os processos da Agência à legislação, destacando-se o Programa de Governança de Privacidade ANATEL (Resolução Interna Anatel nº 25/2021), a edição da Política de Proteção de Dados Pessoais da Anatel (Resolução Interna Anatel nº 24/2021) e a definição em regulamento próprio das diversas etapas para a execução do programa, além da criação de seção para divulgação de informações sobre o tratamento de dados pessoais realizado pela Anatel (https://www.gov.br/anatel/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais).

De acordo com o disposto em sua Política de Privacidade, a coleta de dados pela Anatel ocorre por meio da utilização de sites ou aplicativos da Agência, ou em decorrência da utilização de serviços de telecomunicações, tratando-se de: i) informações fornecidas de forma voluntária ou a requerimento do Órgão Regulador; ii) dados fornecidos por meio da utilização de serviços; e iii) informações recebidas ou coletadas de terceiros, de fontes disponíveis publicamente e de empresas que prestam serviços de telecomunicações.

Em geral, a Anatel ocupa o papel de controladora dos dados, tendo o tratamento a finalidade institucional de regular serviços de telecomunicações e proteger os direitos dos usuários dos serviços de telecomunicações. Dessa forma, na relação com as prestadoras, as organizações e a Agência atuam como co-controladores de dados. Ademais, também são finalidades do tratamento realizado pela Anatel:

Cumprimento da função regulatória e fiscalizatória da Anatel, como acesso, obtenção e averiguação de dados e informações, apuração do cumprimento de obrigações, bem como avaliação da execução dos serviços de telecomunicações, elaboração de Análises de Impacto Regulatório e desenvolvimento da atividade normativa
Endereçamento de reclamações e/ou de denúncias e atualização dos usuários sobre o seu andamento
Acompanhamento do andamento de dúvidas e sugestões realizadas pelos usuários
Processamento de pagamentos dos tributos e outras receitas recolhidos pela Agência, bem como outras atividades afetas à arrecadação; ou para identificar o sujeito passivo da obrigação tributária e processar os pagamentos dos tributos recolhidos pela Agência;
Processar solicitações de homologações de produtos de telecomunicações
Processar requerimentos de obtenção e renovação de outorga de serviços de telecomunicações e de uso de radiofrequência
Contratação de empresas fornecedoras de bens e serviços
Processos de participação social da agência

Nesse sentido, a Agência compreende[3] que, nos processos de negócio em que a Anatel trata dados pessoais, o consentimento do titular não é necessário, especialmente tendo em vista que, em geral, as bases legais aplicáveis tratam do cumprimento de obrigação legal ou regulatória pelo controlador.

3 Resolução Interna Anatel nº 24/2021: "Art. 34. O tratamento de dados pessoais pela Anatel independe do consentimento do titular quando for indispensável para o cumprimento de obrigação legal ou para a execução de políticas públicas legalmente previstas".

Em relação aos tipos de dados coletados, a agência classifica os dados da seguinte forma[4]:

Atributos biográficos	Dados da pessoa natural tais como nome civil ou social, data do nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, endereço, vínculo empregatício, endereços de correio eletrônico, números de telefone
Dados cadastrais	Informações identificadoras perante o cadastro de órgãos públicos tais como número de inscrição no Cadastro de Pessoas Físicas – CPF, número de Identificação Social – NIS, número de inscrição no Programa de Integração Social – PIS, número de inscrição no Programa de Formação do Patrimônio do Servidor Público – Pasep, número do Título de Eleitor
Reclamações junto às Prestadoras	Protocolos com a reclamação de forma que a Anatel possa atuar junto à prestadora a fim de solucionar o pleito do usuário
Dados coletados automaticamente	Características do dispositivo de acesso, do navegador, IP (com data e hora), localização, origem do IP, informações sobre cliques, páginas acessadas, a página seguinte acessada após a saída das Páginas, ou qualquer termo de procura digitado nos sites ou em referência a estes, dentre outros. Para tal coleta, a Anatel fará uso de algumas tecnologias padrões, como cookies, pixel tags, entre outros, que são utilizadas com o propósito de melhorar a experiência de navegação do usuário, de acordo com seus hábitos e suas preferências. É importante esclarecer que, com o advento do desenvolvimento tecnológico, no intuito de viabilizar a prestação do serviço público com o mínimo de segurança, poderá ser coletado, com o consentimento do usuário, atributos biométricos, isto é, características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado.

4 Disponível em: https://www.gov.br/anatel/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais/aviso-de-privacidade. Acesso em: 24/09/2021.

Conforme será observado no Protocolo de Compartilhamento previsto no item II, a Agência ainda possui previsões amplas que amparam a possibilidade de compartilhamento de dados dos regulados com o órgão Regulador, sendo necessária uma reflexão sobre o cumprimento dos princípios da minimização e a constante revisão dos seus requisitos de segurança.

5.3. Portabilidade numérica

O setor de telecomunicações regulamentou o seu processo de portabilidade numérica por meio do Regulamento Geral da Portabilidade - RGP (Resolução nº 460/2007). Essa é uma importante iniciativa regulatória que se encontra alinhada com as discussões deste Código e com a LGPD.

O procedimento existente permite a portabilidade dos dados entre prestadores de serviço, a pedido do titular, para que o titular não fique vinculado a um determinado serviço por conta da ausência dessa previsão. No caso das prestadoras de serviços de telefonia, a migração do número de telefone do titular, e a consequente migração do contrato de prestação de serviços, possibilita a completa interoperabilidade dos serviços de telefonia há anos, se tratando de iniciativa verdadeiramente inovadora.

Nesse sentido, a portabilidade numérica executada pelas prestadoras pode ser considerada um importante precursor do art. 18, V, da LGPD, cumprindo com a função pretendida pelo referido dispositivo legal.

Para que a portabilidade numérica ocorra, é necessário que o titular de dados solicite o serviço, passando por processos de provisão, notificação, validação, nos termos descritos no art. 32 do RGP, o que implica em troca de informações entre a prestadora doadora e a prestadora receptora, além da Entidade Administradora (ABR Telecom) e a própria Anatel.

Tal operação demanda a gestão de grandes bases de dados, que são mantidas tanto pelas prestadoras, quanto pela entidade gestora, além de ser necessária a coleta de outros dados pessoais para que o processo de autenticação do pedido ocorra. Nos termos do art. 47 do RGP, na solicitação da portabilidade o usuário deve informar: i) nome completo; ii) RG ou CPF, em caso de pessoa natural ou CNPJ, em caso de pessoa jurídica; iii) endereço; iv) número de telefone; e v) nome da prestadora da qual o usuário é cliente. A portabilidade é conduzida pela ABR, que é a Entidade Administradora do processo e que atua como operadora do tratamento dos dados.

Sujeitos que podem solicitar a portabilidade	O pedido de portabilidade de dados é restrito à iniciativa dos titulares dos dados e clientes das prestadoras.
Tipos de dados que podem ser portados	O dado migrado é o "Código de Acesso" dos usuários (número de telefone do titular), com a consequente migração do contrato de prestação de serviços de uma prestadora para outra
Destinatários dos dados	Os destinatários dos dados são as prestadoras de serviços de telecomunicações, tendo em vista a necessidade de garantir a interoperabilidade de sistemas e a finalidade da portabilidade

Para os demais serviços, como banda larga e IPTV, ainda que inexista procedimento pré-estabelecido para a portabilidade, tal procedimento pode ser oferecido no futuro.

6. AUTORREGULAÇÃO DO SETOR DE TELECOMUNICAÇÕES

Visando a construção de um ambiente regulatório efetivo e eficiente, a Conexis Brasil Digital (ex-Sinditelebrasil) criou o Sistema de Autorregulação das Telecomunicações (SART), responsável pela elaboração e aprovação de normas pelas entidades do setor e instituição de conselheiros independentes, conforme regras de governança.

O SART é responsável pela elaboração de normativos, aprovados pelo Conselho de Autorregulação, sobre a organização e o funcionamento dos serviços de telecomunicações e demais serviços oferecidos ou disponibilizados aos usuários pelas prestadoras Signatárias. Também é a partir dessa tendência de participação dos regulados no processo regulatório que se insere o presente Código de Boas Práticas.

Conforme prevê o Código de Autorregulação das Telecomunicações, o SART representa um conjunto de princípios, regras, instrumentos, procedimentos de autodisciplina que, organizados por meio de estrutura participativa, busca permitir a regulação eficiente do setor. O sistema foi lançado em março de 2020, por uma iniciativa das empresas de telecomunicações Algar Telecom, Claro, Oi, Sercomtel, Sky, TIM e Vivo, sendo composto por: i) Conselho de Signatárias; ii) Conselho de Autorregulação; iii) Diretoria de Regulação e Autorregulação; iv) comitês temáticos setoriais; e v) grupos de trabalho.

Desde a sua criação, o SART já conta com quatro normativos, que trazem regras para orientar as prestadoras no relacionamento com consumidores: i) telemarketing (Normativo SART 01/2019); ii) atendimento ao cliente (Normativo SART 02/2020), iii) oferta (Normativo SART 03/2020) e; iv) cobrança (Normativo SART 04/2021). Dentre os normativos, destacamos

o Código de Conduta para oferta de Serviços de Telecomunicações por meio do Telemarketing.

Especialmente quanto ao Telemarketing, destaca-se a iniciativa "www.naomeperturbe.com.br" que surgiu em julho/2019 após o envio à Anatel de carta-compromisso sobre telemarketing pelas associadas à CONEXIS, em março/2019, constituindo importante iniciativa para o fortalecimento das relações entre consumidores, prestadoras e Regulador.

A iniciativa foi implementada pelas prestadoras com o acompanhamento da Anatel e buscou conciliar os interesses dos consumidores, que frequentemente reclamam das abordagens do telemarketing das prestadoras, e o regular funcionamento de estratégias de captação, que consiste em importante mecanismo de expansão das bases de clientes das empresas.

O projeto tem atraído outros setores econômicos e conta, atualmente, com a participação das empresas de telecomunicação e das Instituições Financeiras, pelo qual o Consumidor pode, mediante cadastro, formalizar o desejo de não receber ligações de telemarketing, "realizadas diretamente pelas prestadoras de Serviços de Telecomunicações participantes, pelas Instituições financeiras participantes ou por terceiros autorizados, destinadas à divulgação de serviços e produtos com a intenção de venda ao usuário".

Destaca-se que o Código de Autorregulação das Telecomunicações prevê a instauração de Procedimento Disciplinar quando houver indícios de violação do próprio Código de Autorregulação ou dos demais normativos do SART por parte de qualquer das prestadoras signatárias. O Código privilegia, no bojo de procedimento, a apresentação de "Plano de Ação" para correção e superação das possíveis irregularidades, mas prevê, igualmente, a sujeição da prestadora infratora à imposição das sanções previstas no art. 40:

> Art. 40. O descumprimento dos instrumentos normativos do SART sujeita, alternativamente ou cumulativamente, a Prestadora Signatária às seguintes sanções:

I Notificação à presidência da Prestadora Signatária para o ajuste de sua conduta, encaminhada por meio de carta reservada, com o conhecimento de todas as Prestadoras Signatárias;

II Notificação à presidência da Prestadora Signatária para o ajuste de sua conduta por meio de carta pública, na página do SART na internet;

III Suspensão temporária da participação da Prestadora Signatária no SART, com a consequente suspensão do mandato de seu representante no Conselho de Autorregulação, por prazo não superior a 2 (dois) anos; e

IV Expulsão da Prestadora Signatária do SART, com a consequente interrupção do direito de uso do Selo da Autorregulação

7. NORMAS QUE DIALOGAM COM A PROTEÇÃO DE DADOS

A LGPD, como o marco para a disciplina da proteção de dados no Brasil, dialoga com outros diplomas normativos brasileiros que abordam de forma lateral a temática do fluxo de dados. É importante a interpretação dessas normas para compreensão do amplo espectro de direitos e obrigações que protegem os titulares de dados no setor de telecomunicações.

Antes da entrada em vigor da LGPD, leis como o Marco Civil da Internet (MCI) e o Código de Defesa do Consumidor (CDC) previam de forma pontual a tutela da proteção de dados no Brasil[1]. O Código de Defesa do Consumidor, por exemplo, trata de cadastros e bancos de dados de consumo, tendo sido o precursor nessa regulamentação no Brasil.

No âmbito da regulamentação do uso da internet, o MCI disciplina o uso da internet no Brasil, protegendo o ambiente de navegação e garantindo o exercício de diversos direitos fundamentais, como as liberdades de expressão e informação. Em relação ao setor de telecomunicações, o disposto no MCI também estabelece outras obrigações, tais como a garantia da neutralidade de rede e a proteção dos registros de conexão e acesso, que apenas podem ser disponibilizados mediante ordem judicial.

O diploma também inovou, ao trazer as primeiras normas sobre proteção de dados na internet, por meio de dispositivos sobre reparação de danos em caso de violação da intimidade (art. 7º, I), não fornecimento a terceiros de dados pessoais (art. 7º, VII,) e princípios da transparência e finalidade no uso de dados (art. 7º, VIII).

1 Nesse sentido, ver: MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor.* vol. 106. ano 25. p. 37-69. São Paulo: Ed. RT, jul.-ago. 2016.

Com a edição da LGPD, contudo, a vigência de alguns dispositivos passou a ser questionada, tendo em vista um suposto conflito com a norma posterior. Esse é o caso da aplicação do consentimento. Enquanto a LGPD estabelece 10 bases legais para o tratamento de dados pessoais em seu art. 7 º, sem determinar qualquer hierarquia entre elas, o MCI prevê, em seu art. 7º, IX, o direito do usuário ao "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais".

Difere o MCI da LGPD não apenas em razão da quantidade de bases legais aptas a fundamentar um tratamento de dados, previstas nesta última, mas também os atributos do consentimento, que não precisa ser expresso, mas deve consistir em uma manifestação livre, informada e inequívoca (art. 5 º, XII, LGPD).

Para a resolução dessa controvérsia, pode-se aplicar o art. 2º, § 1º,[2] da Lei de Introdução às Normas do Direito Brasileiro – LINDB (Decreto-Lei nº 4.657, de 4 de setembro de 1942)[3]. Não seria o caso, contudo, de derrogação tácita de todo o marco legal, mas apenas das normas conflitantes com idêntico âmbito de aplicação (serviços do meio digital).

Isso ocorre apenas com o art. 7º, IX, do MCI, que assegura ao usuário o "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais". Afinal, o dispositivo não traz os relevantes atributos previstos para o consentimento da LGPD (manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada), nem enseja a possibilidade de que os dados pessoais sejam tratados a partir de outras bases legais, que nos termos do art. 7º, LGPD, totalizam 10 bases legais. Dessa forma, ao contrariar explicitamente os art. 5º, XII, e 7º, da LGPD, entende-se que o art. 7º, IX, do MCI foi tacitamente derrogado por ela.

2 Art. 2º Não se destinando à vigência temporária, a lei terá vigor até que outra a modifique ou revogue. §1º A lei posterior revoga a anterior quando expressamente o declare, quando seja com ela incompatível ou quando regule inteiramente a matéria de que tratava a lei anterior.

3 LEONARDI, Marcel. Aspectos controvertidos entre a Lei Geral de Proteção de Dados e o Marco Civil da Internet. In: Temas Atuais de Proteção de Dados. São Paulo: *Revista dos Tribunais*, 2020.

Quanto aos demais artigos do MCI que tratam de dados pessoais (art. 7º, VII, VIII e X), não há divergência com a LGPD apta a ensejar a sua derrogação. Para esses casos, basta uma leitura concomitante e complementar com as normas da LGPD, marco central para o fluxo de dados pessoais tanto nos meios digitais,[4] como nos meios físicos. [5]

Assim, na interpretação do Marco Civil da Internet, do Código de Defesa do Consumidor, bem como de legislações como a Lei do Cadastro Positivo e regulamentos específicos do setor de telecomunicações, não se está a falar, a princípio, de dispositivos conflitantes ou de antinomia. Deve-se aplicá-los de forma simultânea, respeitando-se suas convergências, bem como a sua adequação aos fenômenos jurídicos sob análise[6].

4 O Art. 1º da LGPD refere-se expressamente aos meios digitais para definir o seu âmbito de aplicação: "Esta Lei dispõe sobre o tratamento de dados pessoais, **inclusive nos meios digitais**, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

5 Essa interpretação complementar dá-se por meio do diálogo das fontes, nos termos formulados por Cláudia Lima Marques e Bruno Bioni baseia-se nessa teoria, compreendendo que o diálogo deve ser realizado de 3 formas: i) as leis podem servir como base conceitual, servindo de influência recíproca; ii) os novos dispositivos da LGPD devem complementar outras leis já existentes, como o MCI, a Lei do Cadastro Positivo e o Código de Defesa do Consumidor; iii) os conceitos da LGPD devem redefinir o escopo de aplicação e parâmetros de outras leis, e vice-versa, tendo em vista a influência de sistema geral no especial. MARQUES, Claudia Lima. Diálogo das Fontes. Do conflito à coordenação de normas do direito brasileiro (coord.). São Paulo: *Revista dos Tribunais,* 2012; BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2ª Ed. Rio de Janeiro: Editora Forense, 2020, p. 259 – 261.

6 MENDES, Laura Schertel. Op. Cit.

8. ÂMBITO DE APLICAÇÃO

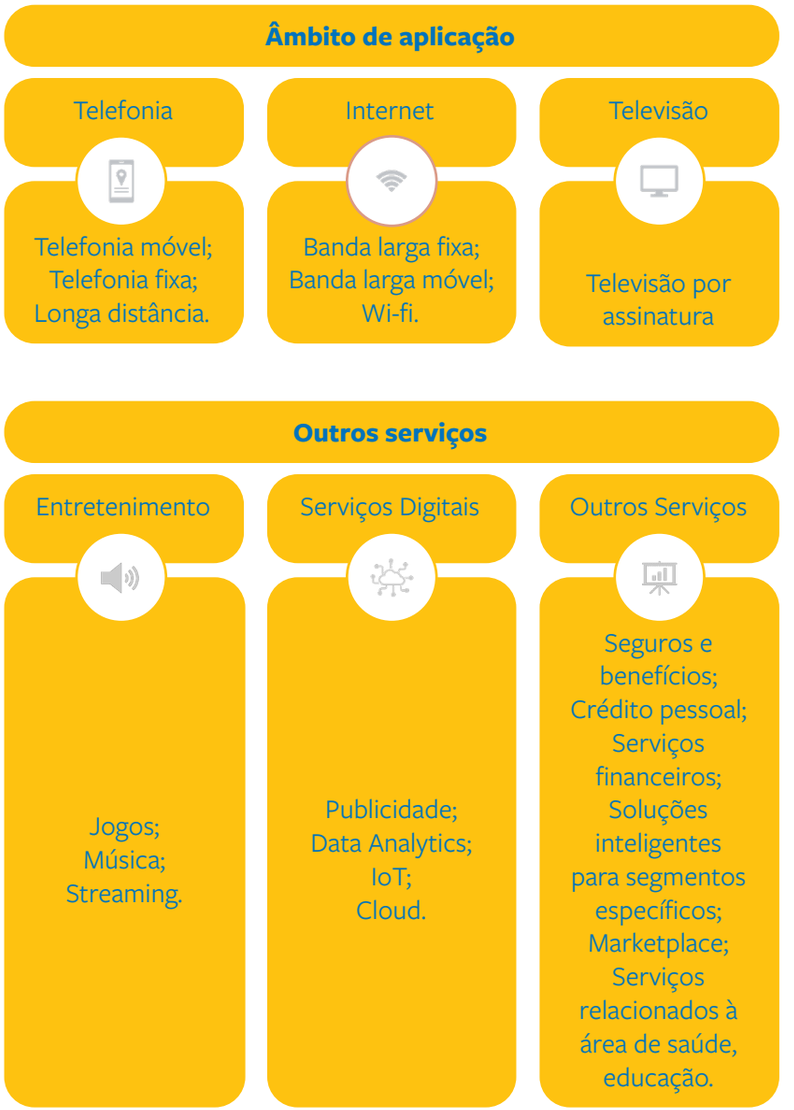
Este Código aplica-se ao tratamento de dados pessoais realizado pelas prestadoras de serviços de telecomunicação associadas à Conexis, abrangendo as atividades de tratamento de dados pessoais realizadas no âmbito da sua prestação de serviços.

Destaca-se que, ainda que o âmbito de aplicação do Código seja direcionado às prestadoras de telecomunicações, outras empresas do setor podem aderir ao seu conteúdo posteriormente, caso os seus termos se adequem ao serviço prestado.

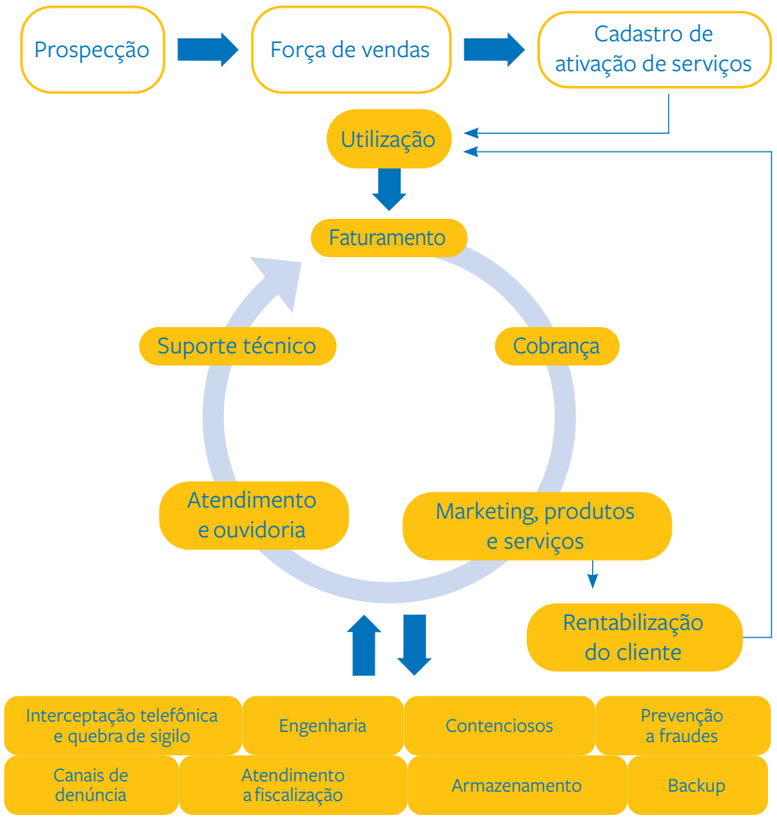
Ressalta-se que além dos serviços tradicionais oferecidos pelas prestadoras, como telefonia, internet e televisão, outra importante frente de serviços é a oferta de aplicações (por exemplo, *Over-the-top* (OTT), Serviços Financeiros Digitais, Internet das Coisas), que não se encontram no âmbito dos serviços regulados pela Anatel.

O Código é aplicável ao tratamento de dados pessoais realizado no âmbito da prestação de todos os serviços prestados pelas prestadoras, uma vez que a LGPD não distingue o tratamento de dados no âmbito da infraestrutura ou de aplicações na internet.

Para melhor compreensão acerca dos serviços prestados pelas prestadoras, representamos o âmbito de aplicação da seguinte forma:



9. CICLO DE VIDA DOS DADOS NO SETOR DE TELECOMUNICAÇÕES



Fonte: material apresentado pelas prestadoras e adaptado pelas autoras.

CÓDIGO DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA O SETOR DE TELECOMUNICAÇÕES

PROTOCOLOS

conexis brasil.digital

I - PROTOCOLO PARA ARMAZENAMENTO DE DADOS PESSOAIS

I.1. Introdução

Conforme explicitado pelo princípio da necessidade (art. 6º, III, LGPD), o tratamento de dados deve ser limitado ao mínimo necessário para realização de suas atividades, de modo que o armazenamento desses dados não deve ser realizado de modo excessivo. Nos termos do art. 15 da LGPD, o término do tratamento de dados deve ocorrer quando: i) a finalidade for alcançada ou os dados não forem mais necessários; ii) o período do tratamento tiver terminado; iii) o titular tiver revogado seu consentimento; e iv) a autoridade nacional determinar o término do tratamento por conta de violação à lei.

Nesse mesmo sentido, de acordo com as melhores práticas internacionais[1], é essencial que os dados sejam armazenados pelo menor tempo possível, devendo ser estabelecidos prazos para que os dados sejam excluídos ou que o protocolo seja revisto. A revisão periódica dos períodos de armazenamento ou o estabelecimento de um prazo para retenção deve ser realizado de forma cuidadosa para o cumprimento do princípio da necessidade.

1 ICO. Principle: Storage limitation. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ Acesso em 06/08/2021. EUROPEAN COMMISSION. For how long can data be kept and is it necessary to update ir? Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en. Acesso em 06/08/2021.

O protocolo para armazenamento de dados pessoais é importante para as prestadoras, não só por conta do princípio da minimização que exige que o tratamento de dados seja realizado apenas quando for adequado, pertinente e limitado aos dados necessários, como também para compreensão de outras obrigações legais que podem exigir que o armazenamento seja realizado por tempo superior ao necessário para a finalidade estrita do tratamento. Ainda assim, as prestadoras devem garantir que, caso o dado não seja mais necessário, os dados sejam excluídos mesmo que o titular não faça a solicitação de forma ativa.

Ademais, importante ressaltar que, nos termos do art. 7º, inciso X, do MCI, ao usuário é assegurado o direito de "exclusão definitiva dos dados pessoais os que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais". Ressalta-se que a exclusão deve ser analisada considerando não apenas a finalidade do tratamento, como também as outras obrigações legais aplicáveis.

Considerando que o setor das telecomunicações é altamente regulado e que os dados de titulares são muitas vezes utilizados em todos os tipos de ações judiciais e procedimentos investigativos, é importante que a definição de prazos para armazenamento não contrarie outras exigências legais ou mesmo impeça o exercício de defesa em processos judiciais.

Nesse sentido, além de ser necessário considerar o princípio da minimização em todo o tratamento realizado, outros prazos, como prescricionais (e.g. arts. 205 e 206 do Código Civil etc.), também devem ser considerados. Os prazos prescricionais são particularmente importantes para dados que constam em documentos com informações de segurança e acesso, documentos relacionados a relações trabalhistas, obrigações fiscais ou outros documentos relevantes para eventuais defesas em processos judiciais e administrativos.

Exemplo disso são as relações trabalhistas, ou mesmo o momento que antecede a contratação de colaboradores. As prestadoras - e outros empregadores – solicitam diversos dados pessoais e até mesmo dados sensíveis. Tais dados podem envolver testes psicológicos, pesquisa de antecedentes criminais, currículo, dados de saúde etc.

Na medida em que a CLT e o Código Civil possibilitam que os titulares dos dados recorram ao judiciário mesmo após o término das relações, em algumas situações as prestadoras não podem excluir de forma definitiva os dados pessoais dos titulares, sob o risco de prejudicarem o seu exercício de defesa em uma lide potencial. Dessa forma, ainda que os titulares (ex-funcionários ou ex-candidatos) solicitem a exclusão dos dados logo após o término da relação, tais dados podem ser mantidos para garantir o exercício de direitos em processos judiciais.

Em relação aos dados coletados dos usuários dos serviços de internet, telefone e TV por assinatura no bojo da prestação do serviço, existem prazos mínimos de armazenamento previstos nos regulamentos da Anatel, bem como no MCI. Portanto, passa-se à análise pormenorizada de alguns tipos de dados, quais sejam: i) registros de aplicações; ii) registro de conexão; iii) histórico de demandas do consumidor; iv) dados cadastrais dos assinantes; v) dados de bilhetagem e do histórico das ligações (incluindo a localização e estações de Rádio Base - ERB utilizadas); vi) dados cadastrais dos usuários; e vii) dados pessoais que constam em documentos de natureza fiscal.

Para tanto, são utilizados os seguintes dispositivos da Lei nº 12.965/2014 (Marco Civil da Internet – MCI); Resolução nº 73/1998 (Regulamento dos Serviços de Telecomunicações) e Resolução nº 632/2014 (Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações – RGC).

Norma	Dados pessoais	Período de retenção
Marco Civil da Internet (Lei nº 12.965/2014)	– registros de conexão (art. 13) – registros de acesso a aplicações de internet (art. 15)	– registros de conexão – 1 ano – registros de acesso a aplicações de internet – 6 meses
Regulamento dos Serviços de Telecomunicações (Resolução nº 73/1998)	– dados relativos à prestação do serviço (art. 65 – J): i) documentos de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada pelo prazo, ii) registros de conexão à Internet.	i) mínimo de 5 (cinco) anos, nos serviços que permitam a realização de tráfego telefônico; ii) prazo mínimo de 1 (um) ano
Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações (Resolução nº 632/2014)	– histórico de demandas (art. 10): número de protocolo do atendimento; a data e hora de registro e de conclusão do atendimento; e, a classificação, a síntese da demanda e o encaminhamento dado pela prestadora – informações sobre atendimento por internet (art. 21) – cópia do contrato e plano de serviço; documentos de cobrança; relatório de serviços prestados, cópia de gravação, histórico de demandas (art. 22) – gravação das interações entre prestadora e consumidor	– mínimo de 3 (três) anos após encaminhamento final da demanda – mínimo 6 (seis) meses após a rescisão contratual. – 6 (seis) meses – mínimo 6 (seis) meses da data de sua realização

Ressalta-se que alguns dispositivos dos artigos de RGC revogaram os prazos anteriormente previstos na Resolução nº 426/2005 (Regulamento do Serviço Telefônico Fixo Comutado – STFC); Resolução nº 477/2007 (Regulamento do Serviço Móvel Pessoal – SMP) e Resolução nº 614/2013 (Regulamento do Serviço de Comunicação Multimídia), com o objetivo de padronizar os protocolos. Ademais, também serão utilizados o disposto no Código de Defesa do Consumidor, Código Nacional Tributário; Decreto nº 6.523/2008 (Decreto SAC), dentre outros.

I.2. Registro de Conexão

O registro de conexão é o "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, assim como as portas lógicas utilizadas quando do compartilhamento de IP público, para o envio e recebimento de pacotes de dados" (art. 65 – J, Resolução nº 73/1998).

Não obstante sua importância para o auxílio em investigações de crimes, tal dado também pode acarretar riscos relevantes para o titular. Dessa forma, o MCI (art. 13) e o Regulamento de Serviços de Telecomunicações estabelecem a obrigatoriedade de seu armazenamento pelo prazo de 1 (um) ano.

I.3. Registros de aplicações

Os Registros de Aplicações se referem ao "conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (art. 5º, VI, do MCI).

Em relação a esses dados, o Marco Civil da Internet estabelece em seu artigo 15 o prazo de retenção de **6 (seis) meses**, além de hipóteses excepcionais de ampliação desse prazo em seu parágrafo 2º, do art. 15. Portanto, dada a sua sensibilidade e o potencial risco decorrente do uso indevido dessas informações, tais dados deverão ser armazenados pelo período aplicável para o cumprimento das obrigações legais e regulatórias.

I.4. Histórico das demandas do Consumidor

De acordo com o art. 10 do RGC (Resolução nº 632/2014) os históricos das demandas dos consumidores, por sua vez, devem ser mantidos por **pelo menos 3 (três) anos** para que o consumidor possa acessar dados como número de protocolo do atendimento; a data e hora de registro e de conclusão do atendimento.

Além disso, também de acordo com o RGC, importa ressaltar que devem ser disponibilizados no espaço reservado do consumidor documentos de cobrança, serviços prestados, histórico da demanda e perfil de consumo referentes à, pelo menos, os últimos **6 (seis) meses**. Já a gravação dos diálogos entre prestadora e Consumidor realizadas por telefone devem ser guardados por, pelo menos, 6 (seis) meses da data de sua realização pelas prestadoras de grande porte e 90 (noventa) dias para as de pequeno porte.

O Decreto nº 6.523/2008 (Decreto SAC), por sua vez, determina que o registro eletrônico do atendimento será mantido à disposição do consumidor e do órgão ou entidade fiscalizadora por um período mínimo de **2 (dois)** anos após a solução da demanda (art. 15, §4º).

Por fim, importa ressaltar que, nos termos do art. 27 do CDC, a pretensão à reparação pelos danos causados por fato do produto ou do serviço prescreve em 5 (cinco) anos, iniciando-se a contagem do prazo a partir do conhecimento do dano e de sua autoria. Nesse mesmo sentido, a Resolução nº 73/1998 determina que dados cadastrais dos assinantes devem ser mantidos por igual período.

Assim, caso o histórico das demandas do consumidor possa ser aspecto essencial para o exercício do direito de defesa, bem como cumprimento de obrigações legais e regulatórias da prestadora, estes podem ser armazenados pelo prazo mínimo de 5 (cinco) anos.

I.5. Dados de bilhetagem e do histórico das ligações

Os dados de bilhetagem referem-se ao histórico de chamadas efetuadas e recebidas, consistindo em importante informação para procedimentos de investigação em diversas searas. Dessa forma, com o intuito de preservar tais dados e possibilitar a persecução de infrações que possam ser comprovadas com tais dados, o art. 65–J da Resolução nº 73/1998, atualizado pela Resolução nº 738/2020, dispõe que os dados de bilhetagem e do histórico de ligações devem ser mantidos pelo prazo mínimo 5 (cinco) anos.

Também a Lei nº 12.850/2013 – que trata da investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal - dispõe que, as concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição do delegado de polícia e do Ministério Público[2], registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais.

I.6. Dados cadastrais dos usuários

De acordo com o art. 65–J da Resolução nº 73/1998, os dados cadastrais devem ser mantidos pelo prazo mínimo de 5 (cinco) anos. Contudo, considerando que dados cadastrais podem ser necessários no cumprimento de obrigações regulatórias ou exercício de direitos, esse prazo pode ser superior a 5 (cinco anos) em determinadas circunstâncias a serem avaliadas por cada prestadora.

I.7. Documentos de natureza contábil e fiscal

Os documentos de natureza contábil e fiscal possuem prazos de armazenamento estabelecidos em diferentes legislações. A Resolução nº 73/1988 traz previsão específica para as prestadoras, assim como diversos outros diplomas legais que dispõe sobre o assunto – e.g. obrigações

2 Lei nº 12.850/2013 - Art. 17. As concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das **autoridades mencionadas no art. 15**, registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais.
(...) Art. 15. O delegado de polícia e o Ministério Público terão acesso, **independentemente de autorização judicial**, apenas **aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito**.

previdenciárias (Decreto-Lei nº 2.052/1983), trabalhistas (Consolidação das Leis do Trabalho e Decreto-Lei nº 2.052/1983) ou mesmo societárias (Lei nº 6.404/96).

De acordo com o art. 65–J da Resolução nº 73/1998, atualizada pela Resolução 738/2020, os documentos de natureza fiscal devem ser mantidos pelo prazo de, pelo menos, 5 (cinco) anos. Nesse mesmo sentido, o Código Tributário Nacional prevê em seu art. 173 que a Fazenda Pública tem o direito de constituir crédito tributário em até 5 (cinco) anos; e o art. 174 prevê que a ação para a cobrança do crédito tributário prescreve em cinco anos.

Contudo, é necessário observar que, além do marco inicial dos prazos de cinco anos poder ser diferente quando os documentos fiscais forem de natureza variadas, os dados que devem ser armazenados são apenas aqueles estritamente necessários para o cumprimento dessas obrigações legais ou regulamentares.

II - PROTOCOLO PARA COMPARTILHAMENTO DE DADOS PESSOAIS

II.1. Introdução

O compartilhamento de dados compõe a dinâmica do setor de telecomunicações, tendo em vista que os serviços são prestados em rede: são compartilhadas infraestruturas de rede de telecomunicações (Resolução nº 638/2017), infraestrutura física (Resolução nº 683/2017), e até mesmo infraestrutura com empresas de distribuição de energia (Resolução Conjunta Aneel e Anatel nº 4/2014).

Além do compartilhamento de dados para fins de captação de clientes e publicidade, também é um importante aspecto do setor a necessidade de compartilhamento de dados exigido pelo próprio órgão regulador e aquele necessário para a prestação de serviços de qualidade. No que diz respeito ao tratamento de dados pessoais, a necessidade de atuação conjunta de diferentes agentes para o oferecimento de serviços pelas prestadoras não seria diferente.

Ocorre, contudo, que os limites para o compartilhamento de dados por empresas de Telecomunicações é assunto que suscitou recentemente importantes controvérsias judiciais,[1] sendo aspecto sensível tanto para os titulares, quanto para as prestadoras, que muitas vezes dependem do compartilhamento para garantir a qualidade da prestação do serviço e ofertar soluções inovadoras. Ademais, o protocolo de compartilhamento também é importante para reforçar a relevância de se adotar medidas de segurança por todos os agentes envolvidos no tratamento.

1 Vide as discussões sobre a possibilidade de compartilhamento de dados pelas empresas de telecomunicações e o IBGE suscitadas a partir da MP 954/2020 que, foi suspensa por força de decisão do STF no bojo das ADIs nº 6387, 6388, 6389, 6390 e 6393 (Rel. Rosa Weber. Julgado em 07/05/2020; DJE nº 137, publicado em 02/06/2020).

Nesse sentido, o protocolo de compartilhamento tem como objetivo identificar as principais finalidades e cuidados que devem ser tomados no compartilhamento de dados no setor, especialmente considerando a sua faceta regulada e a complexidade da estrutura do setor. Para tanto, abordaremos o compartilhamento com os seguintes agentes: **i) órgão regulador; ii) ABR Telecom; iii) bureaus de crédito; e iv) parceiros comerciais.**

II.2. Compartilhamento de dados com órgão regulador

Uma das bases legais que possibilita o compartilhamento de dados pessoais e sensíveis é o cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II, e art. 11, II, a, da LGPD). Dada a importância da regulação do setor de telecomunicações, ressaltamos algumas obrigações regulatórias impostas pela Anatel que versam sobre o fornecimento de dados e informações pelas prestadoras.

Tal possibilidade encontra fundamento no art. 19 da Lei nº 9.472/1997, que atribui à Anatel a competência para adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras. Nesse sentido, ainda que todo o processo de compartilhamento de dados deva ser amparado pelos princípios da LGPD, a depender da requisição de informações realizada pela autoridade, as prestadoras podem ter que compartilhar dados de usuários.

Necessário ressaltar que o compartilhamento de dados com órgão regulador deve ser realizado apenas no limite do que foi solicitado pela autoridade, sempre em atendimento ao princípio da minimização. Ademais, devem ser adotados procedimentos de segurança que garantam a preservação dos dados compartilhados, seja o compartilhamento realizado de forma remota, por meio da concessão de acesso à autoridade aos sistemas, ou de forma física.

Também do lado da administração pública, mesmo quando o tratamento de dados é realizado para execução de políticas públicas (art. 7, III, LGPD), é necessário avaliar se tal ato atende aos requisitos mínimos de um tratamento adequado, proporcional, seguro e não excessivo[2]. Esse cuidado é particularmente importante, uma vez que o tratamento inadequado pelo Estado tem o potencial de produzir impactos enormes na sociedade[3].

Assim, apresentaremos algumas hipóteses legais que constam nas Resoluções da Anatel que possibilitam pedidos de informações que podem incluir dados pessoais:

Regulamento do Serviço Telefônico Fixo Comutado (Resolução nº 426/2005)

Art. 17. A prestadora deve prestar informações à Agência sobre reclamações dos usuários, quando esta solicitar, no prazo máximo de 5 (cinco) dias úteis.
(...)
§ 5º A prestadora deve providenciar os meios eletrônicos e sistemas necessários para o acesso da Agência, sem ônus, em tempo real, a todos os registros de informações relacionadas às reclamações e solicitações dos usuários registradas na central de informação e de atendimento ao usuário, nas lojas de atendimento e nos PST, na forma adequada à fiscalização da prestação do serviço.
Art. 18. Anualmente, as prestadoras com PMS devem proceder à certificação de seus processos de coleta, registro, tarifação e faturamento, através de empresa de auditoria independente, registrada em organismo de certificação credenciado junto ao Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro).
Art. 19. A prestadora deve estabelecer mecanismos que verifiquem a veracidade dos dados fornecidos pelo assinante, inclusive por meio de documentação que permita a sua correta identificação, quando da instalação do acesso e de qualquer alteração contratual.

2 SCHERTEL, Laura, GASIOLA, Gustavo; MACHADO, Diego. A Administração Pública entre transparência e proteção de dados. In: RANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antônio (coord.). *A Lei Geral de Proteção de Dados Pessoais: Aspectos práticos e teóricos relevantes no setor público e privado*. São Paulo: Revista dos Tribunais, 2021.

3 WIMMER, Miriam. O regime do tratamento de dados pessoais pelo poder público. In: Bioni et al (Coords.) *Tratado de Proteção de Dados Pessoais. Rio de Janeiro*: Forense, 2021, p. 274 – 275.

Regulamento do Serviço Móvel Pessoal (Resolução nº 477/2007)

Art. 11. A Prestadora deve informar a identificação do Plano de Serviço, inclusive por seu número, quando aplicável, sempre que solicitado pelo Usuário ou pela Anatel. (Redação dada pela Resolução nº 632, de 7 de março de 2014)
Parágrafo único. A Anatel poderá solicitar a informação descrita no caput por Usuário ou em termos de quantidade de Usuários em cada Plano de Serviço.
Art. 12. A Prestadora do SMP deve fornecer a outras prestadoras de serviços de telecomunicações, as informações sobre os Usuários, constantes de sua base cadastral e necessárias à prestação de serviços.
§ 1º O direito previsto no caput deve ser exercido exclusivamente com a finalidade estabelecida na regulamentação aplicável.
§ 2º A regulamentação pode estender o direito previsto no caput a terceiros legitimamente interessados, que necessitem das informações para a realização de atividade vinculada, direta ou indiretamente, ao serviço.
§ 3º Os contratos para fornecimento das informações têm caráter público, são firmados em bases justas e razoáveis, devendo prever forma e periodicidade de atualização das informações e devem ser reproduzidos, em condições isonômicas, a outros interessados.
(...)
§ 5º A prestadora deve assegurar que todos aqueles que tiverem acesso às informações previstas neste artigo observem as obrigações de sigilo. (Redação dada pela Resolução nº 632, de 7 de março de 2014)
Art. 15. A prestadora deve prestar informações à Anatel, no prazo por ela estipulado, não superior a 5 (cinco) dias úteis, sobre reclamações, solicitações de serviços e pedidos de informação dos Usuários
(...)
§ 15. A prestadora deve providenciar os meios eletrônicos e sistemas necessários para o acesso da Agência, sem ônus, em tempo real, a todos os registros relacionados às reclamações, solicitações de serviços, pedidos de rescisão e pedidos de informação, na forma adequada à fiscalização da prestação do serviço.

Regulamento de Fiscalização (Resolução nº 596/2012)

Art. 26. Cabe ao Agente de Fiscalização determinar a extensão, profundidade, conveniência e oportunidade na obtenção dos dados e das informações necessários para a realização da ação de fiscalização.
Art. 36. Os dados e as informações acessados e obtidos pela Agência nos termos deste Regulamento são aqueles diretamente relacionados às obrigações da fiscalizada e indispensáveis ao exercício efetivo da função fiscalizadora da Anatel, mantendo-se inviolável o fluxo das comunicações entre os usuários.
§ 1º No procedimento de fiscalização será garantido o tratamento confidencial dos dados e informações de natureza técnica, operacional, econômico-financeira e contábil acessados e obtidos pela Agência.
§ 2º Estende-se à Anatel o dever de sigilo das informações pessoais dos usuários a que se submetem as prestadoras de serviços fiscalizadas.
§ 3º A fiscalizada pode solicitar o sigilo de informações relativas a sua atividade empresarial, cuja divulgação possa representar vantagem competitiva a seus concorrentes.

Regulamento do Serviço de Comunicação Multimídia (Resolução nº 614/2013)

Art. 47. Sem prejuízo do disposto na legislação aplicável, as Prestadoras de SCM têm a obrigação de:
(...)
II - apresentar à Anatel, na forma e periodicidade estabelecidas na regulamentação e sempre que regularmente intimada, por meio de sistema interativo disponibilizado pela Agência, todos os dados e informações que lhe sejam solicitados referentes ao

serviço, inclusive informações técnico-operacionais e econômico-financeiras, em particular as relativas ao número de Assinantes, à área de cobertura e aos valores aferidos pela Prestadora em relação aos parâmetros e indicadores de qualidade;
(...)
XV - manter à disposição da Anatel e do Assinante os registros das reclamações, solicitações de serviços e pedidos de rescisão por um período mínimo de dois anos após solução desses e, sempre que solicitada pela Anatel ou pelo Assinante, tornar disponível o acesso de seu registro, sem ônus para o interessado.
Art. 48. A Prestadora deve providenciar os meios eletrônicos e sistemas necessários para o acesso da Agência, sem ônus, em tempo real, a todos os registros relacionados às reclamações, solicitações de serviços e pedidos de rescisão e de informação, na forma adequada à fiscalização da prestação do serviço.

Regulamento de Fiscalização Regulatória (Resolução Anatel nº 746, de 22 de junho de 2021)

Art. 7º Os Administrados submetem-se à Fiscalização Regulatória da Anatel mediante as seguintes obrigações, dentre outras constantes da legislação e da regulamentação:
I - fornecer dados e informações de natureza técnica, operacional, econômico-financeira, contábil ou outras pertinentes, no prazo, local, formato e demais condições estabelecidas pela Anatel, que estejam disponíveis ou que sejam passíveis de obtenção por meio de consulta aos aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos do Administrado ou por ele utilizados, seja em arquivo eletrônico, meio físico ou qualquer outro meio existente, em seu poder ou em poder de terceiros, observado o disposto no art. 19 deste Regulamento
(...)
IV - disponibilizar, sem ônus para a Anatel, o acesso remoto a sistemas de informação utilizados para coleta, tratamento e apresentação de dados, informações e outros aspectos, responsabilizando-se por sua integridade, disponibilidade, consistência, fidelidade e privacidade
(...)
VI - disponibilizar, sempre que solicitado, representante apto a dar suporte à atuação da Anatel, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto.
Art. 18. São modos pelos quais a Anatel pode solicitar, receber, obter e acessar dados e informações dos Administrados, dentre outros:
I - acesso remoto;
II - modo presencial; e,
III - modo não presencial.
Parágrafo único. Os modos previstos neste artigo podem ser utilizados em tempo real ou diferido e de forma concomitante ou não.
Art. 19. Os dados e as **informações solicitados, recebidos, obtidos e acessados pela Anatel** nos termos deste Regulamento **são aqueles necessários ao exercício efetivo das atribuições da Agência**, mantendo-se invioláveis as comunicações entre os usuários.
§ 1º **Os dados e as informações solicitados, recebidos, obtidos e acessados pela Anatel estão sujeitos às regras de acesso e classificação de sigilo previstas na regulamentação específica.**
Art. 30. Cabe ao Agente de Fiscalização determinar a extensão, profundidade, conveniência e oportunidade para a solicitação, recepção, obtenção e acesso dos dados e das informações necessários para o atendimento do escopo da Inspeção.
Parágrafo único. **No exercício dessa atividade, o Agente deverá observar a Política de Gestão de Dados da Anatel.**

II.3. Compartilhamento de dados com ABR Telecom

O compartilhamento de dados entre as prestadoras e a ABR Telecom decorre da necessidade de gestão de soluções tecnológicas em ambientes compartilhados do setor de telecomunicações. Por meio das soluções oferecidas em conjunto pela ABR Telecom e prestadoras associadas, busca-se empregar recursos de alta tecnologia, realizando uma gestão baseada em processos[4].

4 As informações apresentadas nesse protocolo se encontram em: https://www.abrtelecom.com.br/a-abr-telecom

A importância da centralização de algumas soluções é, inclusive, reconhecida pela Anatel, que em processos como da Portabilidade Numérica, regulamentou a participação da ABR como entidade administradora, por meio da Resolução Anatel nº 460/2007.

Para realização da Portabilidade Numérica, a ABR Telecom realiza a gestão de todo o processo de portabilidade tanto para usuários de serviços de telefonia fixa (STFC), quanto de móvel pessoal (SMP), sendo responsável por[5]: i) garantir a disponibilidade e a evolução da solução tecnológica da portabilidade numérica e a operação e atualização da Base de Dados Nacional de Referência (BDR), base que contêm a informação sobre todos os números portados; ii) realizar a concessão e gestão do acesso das prestadoras à BDR; e iii) atuar no relacionamento com a Anatel, prestadoras e fornecedores, garantindo a transparência do processo e o correto acesso aos dados relacionados à portabilidade.

Outro importante processo possibilitado com o auxílio da ABR trata-se da implementação e desenvolvimento do site "não me perturbe". Nesse endereço eletrônico, consumidores que não desejam receber chamadas de telemarketing com ofertas de serviços de telecomunicações e serviços bancários cadastram seus números, conforme descrito no item 6.3. A implementação da medida decorre de atuação conjunta da Anatel e das empresas do setor financeiro e de telecomunicações[6]. Já os dados coletados por meio do site naomeperturbe.com.br são mantidos pelas prestadoras de Serviços de Telecomunicações participantes, pelas Instituições financeiras participantes e controlado pela ABR de forma centralizada.[7]

Nesse sentido, a atuação da ABR Telecom ocorre em diversas frentes, sendo necessário o compartilhamento de dados pessoais da base de clientes das prestadoras para que as soluções sejam implementadas. A base legal utilizada para a prestação desses serviços pela ABR Telecom varia a depender da finalidade da solução, sendo a maior parte dos serviços fruto de cumprimento de obrigação regulatória (art. 7º, II, e art. 11, II, a, da LGPD).

5 Disponível em: https://www.abrtelecom.com.br/entidades/portabilidade-numerica

6 Disponível em: https://www.gov.br/anatel/pt-br/consumidor/destaques/cadastro-nacional-de-nao-me-perturbe-para-servicos-de-telecomunicacoes-esta-disponivel-a-partir-de-16-7

7 Disponível em: https://www.naomeperturbe.com.br/politica.html

Também vale destacar que a atuação da ABR junto às prestadoras, em geral, ocorre na condição de operadora de dados pessoais. Ainda assim, a entidade atua na implementação de sua Política de Privacidade e Proteção de dados Pessoais,[8] bem como de sua Política de Segurança da Informação.[9] Para tanto, são adotadas medidas de segurança lógica, observando, pelo menos[10]:

Uso de senhas e controle de acesso a sistemas e recurso das redes	Disciplina o uso de autorizações de identificação de usuários (ID), senhas de acesso (*Password*) e controles sobre o uso de dados, informações, sistemas e recursos de redes, considerando, proteger a informação de qualquer acesso, modificação, divulgação, uso e destruição não autorizados.
Segurança em estações de trabalho e periféricos	Disciplina o uso e garante a Segurança das Informações guardadas em cada estação de trabalho, Servidor secundário local (departamental) ou notebook / laptop / PDAs / Tablet, além de garantir a integridade funcional de cada estação de trabalho, computador ou notebooks / laptops / PDAs / Tablet, fornecendo manutenção e atualização adequada ao *hardware* e *software* inclusive atualizações automatizadas de segurança e correções (*patches*).
Uso de Equipamentos Portáteis e *Wireless*	Define diretrizes e nomeia responsáveis para assegurar que equipamentos portáteis, principalmente com acesso via sistemas de rede sem fio (*wireless*) recebam um nível adequado de proteção nos ambientes controlados pela ABR Telecom e inclusive fora destes, além de disciplinar o uso e os níveis de proteção exigidos, visando atender à PSI da ABR Telecom.

8 Disponível em: https://front.abrtelecom.com.br/public/arquivos/16110789345l8.pdf

9 Disponível em: https://front.abrtelecom.com.br/public/arquivos/16110790555547.pdf

10 Tabela elaborada com base nas informações disponíveis na Política de Segurança da Informação da ABR Telecom, disponível em: https://front.abrtelecom.com.br/public/arquivos/1611079055547.pdf.

Acesso à Internet	Disciplina o uso dos recursos da Internet em navegação WEB Segura através de redes, considerando proteger Servidores, infraestrutura de rede e Estações de trabalho contra contaminações por vírus, invasões planejadas e a própria Privacidade dos usuários quando em navegação WEB, garantir a integridade dos sistemas e dos arquivos, determinar as regras de acesso para cada aplicação, não autorizar nenhum acesso, salvo os que são expressamente definidos e promover através de recomendações o uso seguro dos recursos da WEB.
Segurança em infraestrutura de Redes	Objetiva estabelecer e disciplinar os requisitos e procedimentos mínimos necessários para garantir a segurança da infraestrutura de redes de voz, dados e imagens da ABR Telecom, considerando estabelecer recomendações para a instalação e manutenção de ferramentas, hardware e software, inclusive atualizações automatizadas de segurança e correções (*patches*) visando a segurança dos sistemas computacionais e de comunicação da ABR Telecom interligados à rede (NAN/WAN/WLAN da ABR Telecom). Também busca orientar, por meio de diretrizes, todas as ações de segurança para minimizar os riscos e garantir autenticidade, confidencialidade, integridade e disponibilidade das informações e estabelecer procedimentos estratégicos visando prevenir e responder a incidentes de segurança na infraestrutura de redes.
Segurança em Desenvolvimento e Manutenção de *Softwares*	Estabelece regras para a aquisição e desenvolvimento pontual de *softwares* tanto por colaboradores, bem como por terceiros para a prestação de serviços, visando controlar e melhorar continuamente os processos de desenvolvimento de *software*, utilizando de melhores práticas e *frameworks* de mercado para garantir a validade permanente dos sistemas e dos arquivos, determinar as regras para fazer, controlar e melhorar o desenvolvimento e uso de *softwares*, estabelecer critérios de aceitação de novos sistemas, atualizações e novas versões e disciplinar o desenvolvimento, instalação, manutenção e atualizações de sistemas existentes e novos da ABR Telecom.

Padrões e práticas Criptográficas	Visa estabelecer regras para aplicação de processos criptográficos sobre informações classificadas como "Restritas" no âmbito da responsabilidade da ABR Telecom, a fim de assegurar que as informações recebam um nível adequado de proteção e também disciplinar a manipulação da informação classificada como Restrita, não importando o meio para proteger a informação de qualquer acesso, modificação, divulgação, uso e destruição não autorizados estabelecendo o emprego de algoritmos apropriados para cada caso, a duração (validade) das Chaves e níveis de proteção.
Segurança em Servidores de Rede	Estabelece diretrizes que possam assegurar um devido nível de proteção aos servidores da ABR Telecom, a fim de definir a contínua melhoria nos processos e controles de segurança e periodicidade de revisão das estruturas de proteção.
Segurança na compra de licenças e manutenção	Definição de regras e nomeação de responsáveis pela gestão dos produtos de softwares de mercado (Pacotes de Sistemas e Aplicativos) visando assegurar que as Licenças de Uso estejam legalmente em quantidade suficiente para a organização, bem como suas atualizações, atentando também para criar critérios para a padronização de ambientes.
Práticas de *Backup*, *Restore*, Manipulação, Guarda e Descarte de Mídias	Diretrizes, regras e nomeia responsáveis pelas ações de *Backup*, *Restore*, *Recovery*, manipulação, guarda e descartes de mídias que contenham dados corporativos (estratégicos e/ou pessoais), bem como estabelecer os processos de Backup de dados, os processos de testes, rotulação, guarda e retenção de mídias, os processos de *Restore* de dados e os processos de *Recovery* de dados.
Arquitetura de Proteção Contra Vírus	Visando estabelecer diretrizes para a arquitetura de proteção contra *vírus*, *trojans*, *spywares*, *ransomwares*, *web-bugs*, entre outros que possam minimizar a possibilidade de ocorrências desses processos nos ambientes delimitados pelo Serviço.

Gestão de vulnerabilidades e respostas à Cybercrime	Estabelece diretrizes para o processo de combate e resposta a Cybercrimes e direciona os processos organizacionais contínuos de segurança da informação visando proteger a informação de qualquer acesso, modificação, divulgação, uso e destruição não autorizados e assegura através de avaliação periódica de possíveis vulnerabilidades dos ativos de informação e serviços.

Por fim, importante pontuar que, apesar de tratar grande volume de dados necessários para viabilizar certas ações pelas prestadoras de telefonia, a ABR não tem autonomia para desenvolver negócios utilizando-se dessas bases, devendo ater-se à finalidade da solução proposta.

II.4. Compartilhamento de dados com bureau de crédito

O compartilhamento de dados de clientes e a consulta de informações relativas a potenciais clientes (ou de clientes do portfólio que buscam melhorar seus planos) são um importante aspecto da relação das prestadoras e bureaus de crédito. Essa relação ocorre por meio da análise de dados possibilitada pelo banco de dados detidos pelos bureaus de crédito e a necessidade de alimentar tais bancos de dados para possibilitar a assiduidade da análise, que se fundam no compartilhamento de informações entre os agentes.

Ademais, no compartilhamento de dados com bureaus de crédito as prestadoras podem atuar tanto como "consulentes/clientes" desse tipo de serviço, quanto como "fonte" de dados para construção das bases de dados, que podem ter finalidades voltadas a crédito e a prevenção à fraude.

O compartilhamento de dados com bureaus é mais um exemplo de aplicação do diálogo das fontes, visto que se faz necessária a interpretação concomitante das regras da LGPD - seus princípios, direitos (art. 20) e obrigações - com a Lei do Cadastro Positivo e do CDC.

Os bureaus de crédito são os agentes responsáveis por intermediar a relação entre credor e consumidor, coletando informações de consumidores junto a credores (como as prestadoras) e fontes públicas, e apresentando tais informações às instituições interessadas, que podem incluir as prestadoras. Essa atuação é realizada por meio de duas principais frentes, o *scoring* de crédito e a Lei do Cadastro Positivo, estando sua regulamentação prevista no CDC, na Lei do Cadastro Positivo e na própria LGPD.

O *scoring* de crédito que é acessado pelas prestadoras para análise do perfil de clientes e potenciais clientes é prática legítima, reconhecida pelo Superior Tribunal de Justiça (STJ),[11] desde que tratado com transparência e boa-fé, nos termos da legislação. Para assegurar a transparência do processo, é necessário que os referidos sistemas de *scoring* garantam ao consumidor a possibilidade de solicitar acesso a seus dados a qualquer momento, sendo vedada a utilização de informações excessivas, sensíveis, inexatas e não verdadeiras.[12]

Nesse sentido, destaca-se que quando a prestadora atua como fonte de dados para a formação do cadastro positivo, a sua responsabilidade está associada ao cumprimento das obrigações estabelecidas no art. 8º. da Lei do Cadastro Positivo. Por outro lado, os bureaus de crédito são considerados os gestores dos bancos de dados e possuem obrigações relacionadas ao exercício dos direitos dos cadastrados, respondendo por eventuais prejuízos a que der causa e ao dever de receber e processar impugnações ou cancelamentos e realizar retificações (Art. 9º, § 1).

A adesão das prestadoras de telecomunicações ao Cadastro Positivo foi formalizada em julho de 2020[13]. Conforme informação da Conexis, "com a entrada do setor, informações de pagamento das contas dos serviços de telecomunicações integrarão o banco de dados do Cadastro Positivo e serão consideradas pelos bureaus de crédito (Boa Vista, Quod, Serasa e SPC) na formação da nota de pessoas físicas e jurídicas" etc. [14]

11 REsp nºs 1.457.199 e 1.419.697.

12 Ademais, é necessário que se respeite as limitações temporais de 5 (cinco) anos para o cadastro negativo e 15 (quinze) anos para o histórico de crédito, nos termos do art. 43 do CDC e 14 da Lei do Cadastro Positivo. CDC – "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. (...) § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores". Lei do Cadastro Positivo – "Art. 14. As informações de adimplemento não poderão constar de bancos de dados por período superior a 15 (quinze) anos".

13 Disponível em: https://conexis.org.br/operadoras-de-telecom-aderem-ao-cadastro-positivo/

14 Disponível em: https://conexis.org.br/operadoras-de-telecomunicacoes-passam-a-integrar-o-cadastro-positivo/

Assim, destacam-se algumas das previsões da Lei do Cadastro Positivo, que reforçam a necessidade de garantir que o compartilhamento de dados atenda ao disposto na LGPD e assegure a proteção dos titulares dos dados:

PRINCÍPIOS DO LIVRE ACESSO, TRANSPARÊNCIA, QUALIDADE DOS DADOS

Art. 5º São direitos do cadastrado:
I - obter o cancelamento ou a reabertura do cadastro, quando solicitado;
II - acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado;
IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais;
VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.
Art. 8º São obrigações das fontes:
(...)
III - verificar e confirmar, ou corrigir, em prazo não superior a 2 (dois) dias úteis, informação impugnada, sempre que solicitado por gestor de banco de dados ou diretamente pelo cadastrado;
IV - atualizar e corrigir informações enviadas aos gestores, em prazo não superior a 10 (dez) dias;
V - manter os registros adequados para verificar informações enviadas aos gestores de bancos de dados; e
VI - fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de bancos de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros bancos de dados.
Parágrafo único. É vedado às fontes estabelecer políticas ou realizar operações que impeçam, limitem ou dificultem a transmissão a banco de dados de informações de cadastrados.

PRINCÍPIO DA FINALIDADE E NECESSIDADE

Art. 7º As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para:
I - realização de análise de risco de crédito do cadastrado; ou
II - subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.

PRINCÍPIO DA TRANSPARÊNCIA E NÃO DISCRIMINAÇÃO

Art. 7º-A Nos elementos e critérios considerados para composição da nota ou pontuação de crédito de pessoa cadastrada em banco de dados de que trata esta Lei, não podem ser utilizadas informações:
I - que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e às convicções políticas, religiosas e filosóficas;
II - de pessoas que não tenham com o cadastrado relação de parentesco de primeiro grau ou de dependência econômica; e
III - relacionadas ao exercício regular de direito pelo cadastrado, previsto no inciso II do caput do art. 5º desta Lei.
§ 1º O gestor de banco de dados deve disponibilizar em seu sítio eletrônico, de forma clara, acessível e de fácil compreensão, a sua política de coleta e utilização de dados pessoais para fins de elaboração de análise de risco de crédito.
§ 2º A transparência da política de coleta e utilização de dados pessoais de que trata o § 1º deste artigo deve ser objeto de verificação, na forma de regulamentação a ser expedida pelo Poder Executivo.

II.5. Compartilhamento de dados com parceiros comerciais

O compartilhamento de dados com parceiros comerciais pode ser compreendido em 3 (três) principais categorias: i) captação de novos clientes; ii) armazenamento e tratamento; e iii) desenvolvimento de produtos e serviços de dados e de inovação, exploração de novas frentes de negócio.

Conforme abordado no item 6 da Parte I, um dos objetivos do compartilhamento de dados é a captação de novos clientes. Além de se fundamentar

nas bases legais da LGPD, o compartilhamento para essa finalidade deve cumprir com os princípios legais da necessidade, proporcionalidade, finalidade e transparência.

Uma importante iniciativa do setor para abordar esse tema foi a elaboração de Código de Conduta para a oferta de Serviços de Telecomunicações por meio de Telemarketing (Normativo SART 01/2019), que foi apresentado para a Anatel em 2019. Destacam-se as seguintes recomendações do referido Normativo:

- Apresentar os agentes e identificar a prestadora de forma clara, informando o objetivo da ligação
- Respeitar a vontade do consumidor sempre que ele manifestar a sua contrariedade quanto ao prosseguimento da ligação, encerrando a ligação e liberando a linha imediatamente
- Não realizar ligações por meio de robôs apenas para verificar a disponibilidade do consumidor em atender
- Realizar ligações apenas em horários oportunos, compreendidos no período de 9 às 21 horas nos dias úteis e das 10 às 16 horas nos sábados
- Não realizar ligações nos domingos e feriados nacionais
- Não ligar de forma insistente para os consumidores, limitadas ao máximo de duas chamadas por dia e 15 ligações por mês

Além das medidas que vêm sendo desenvolvidas pelo setor para endereçar eventuais abusos cometidos nas práticas de captação de clientes, sugere-se a utilização do previsto no Protocolo para garantia do direito dos titulares no item IV.

Em relação aos serviços de armazenamento e tratamento em *cloud* ou outras tecnologias e o desenvolvimento de produtos e serviços de dados e de inovação, exploração de novas frentes de negócio, é importante frisar que ambas as atividades por vezes exigem o compartilhamento de dados pessoais para a sua implementação.

No caso dos serviços de armazenamento e tratamento em *cloud* ou outras tecnologias, a sua utilização pode ser realizada de diversas formas, podendo ser utilizada apenas para gestão ou segurança da infraestrutura interna da prestadora, inclusive para finalidades e tipos de tratamento que não envolvem dados pessoais, bem como ser um serviço prestado para clientes que armazenam informações variadas de seu interesse. Em relação ao oferecimento do serviço para os clientes, a realização do armazenamento em nuvem pode ocorrer sem que seja possível o acesso das informações armazenadas.

Em relação ao desenvolvimento de novas frentes de negócio, estas podem se dar por meio da criação de produtos baseados em dados (como *scores* antifraude e de crédito mencionados no item anterior) ou de outros tipos de soluções tecnológicas inovadoras. Apesar do tratamento de dados pessoais nem sempre ser necessário para tais produtos, é importante que a prestadora avalie a aplicabilidade da LGPD nessas hipóteses, garantindo a adequação às bases legais, aos princípios e aos direitos dos titulares nos termos da legislação.

Na hipótese de aplicação da LGPD, é importante também que sejam criados mecanismos de restrição de acesso quando do desenvolvimento de novas tecnologias, de modo a impedir que dados desnecessários sejam acessados. É fundamental, ainda, que sejam adotadas, no contexto de compartilhamento, as medidas conhecidas como *privacy by design* ou privacidade desde a concepção, previstas nos arts. 46, §20, e 49 da LGPD[15]:

15 Tradução livre de: CAVOUKIAN, Ann. *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*. Disponível em: http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

1. Proatividade e não reatividade; prevenção e não reparação
2. Privacidade como padrão
3. Privacidade incorporada ao design
4. Total funcionalidade — resultados positivo, e não soma zero
5. Segurança do começo ao final — proteção do ciclo de vida
6. Visibilidade e transparência
7. Respeito pela privacidade do usuário

Por fim, em relação à realização de transferências internacionais no bojo do compartilhamento de dados com parceiros comerciais, deve-se buscar a adoção do Protocolo de Transferência Internacional previsto no item III. Tratando-se de hipótese de compartilhamento de dados que possa causar elevados riscos para o titular, far-se-á necessária a realização de um relatório de impacto, nos termos do Protocolo do item VII, conforme aplicável.

III - PROTOCOLO PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS

III.1. Introdução

O fluxo de dados pessoais não encontra limites fronteiriços, considerando o contexto da economia globalizada e o cenário descentralizado do desenvolvimento de tecnologias. Nesse sentido, para garantir a proteção adequada dos dados pessoais, inclusive após a saída do território nacional, diversas jurisdições somente autorizam transferências internacionais de dados se um grau de proteção semelhante ao nacional for comprovado.

Conforme identificado por Fernanda Mascarenhas e Theófilo Aquino[1], a preocupação com a transferência internacional de dados consubstanciada na LGPD originou-se de três principais aspectos, suscitados no bojo das contribuições enviadas à redação do Anteprojeto de Lei do Ministério da justiça: i) oposição entre modelo geográfico, que utiliza critérios de equivalência e adequação para análise da legislação de terceiros, e modelo de responsabilização, que desloca o ônus da responsabilização do poder público para o privado e visa responsabilizar as empresas independentemente da localização geográfica; ii) desafios na substituição do consentimento pela aferição de nível de proteção; e iii) discricionariedade da ANPD para autorizar a transferência.

A escolha legislativa brasileira pelos requisitos de proteção da transferência internacional sofreu influências do Regulamento Europeu de Proteção de Dados, mas manteve diferenças importantes, principalmente considerando a maior abrangência e generalidade das hipóteses de transferência na LGPD.

1 O regime de transferência internacional de dados na LGPD: delineando as opções regulatórias em jogo. In: Bioni et al (Coords.) *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

Nesse sentido, buscando conferir um grau de proteção similar ao que é exigido no tratamento de dados que ocorre em território nacional e, ao mesmo tempo, possibilitando que nem todas as hipóteses precisem passar pelo crivo da ANPD, o art. 33 da lei estrutura três regimes de tutela dos dados quando da transferência internacional de dados[2]: i) declaração de existência de grau de proteção adequado; ii) existência de garantias de cumprimento com os preceitos da lei; e iii) derrogações específicas que tem como objetivo a promoção de interesse público. Dessa forma, a LGPD lista os seguintes instrumentos de transferência internacional de dados pessoais:

- Países ou organismos internacionais proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD (inciso I)
- Demonstração de garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados (inciso II)
- Transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional (inciso III)
- Transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso IV)
- Autoridade nacional autorizar a transferência (inciso V)
- Transferência resultar em compromisso assumido em acordo de cooperação internacional (inciso VI)
- Transferência for necessária para a execução de política pública ou atribuição legal do serviço público (inciso VII)
- Consentimento (inciso VIII)
- Para atender as hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD (inciso IX)

2 PRATA DE CARVALHO, Angelo. Transferência internacional de dados na lei geral de proteção de dados - força normativa e efetividade diante do cenário transnacional. In: Gustavo Tepedino et al (Coords). *A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. 1ª ed., São Paulo: Thomson Reuters Brasil, 2019, p. 624.

Será apresentado a seguir uma breve descrição de cada um dos requisitos para a transferência internacional para esclarecer o seu âmbito de aplicação e os aspectos pendentes de regulamentação pela autoridade. Antes, contudo, é necessário introduzir uma breve explicação sobre quando se configura uma transferência internacional.

III.2. Hipóteses de configuração da transferência internacional de dados

O art. 5º, inciso XV, define a transferência internacional como aquela realizada "para país estrangeiro ou organismo internacional do qual o país seja membro". A transferência internacional de dados pode ser realizada na modalidade direta ou indireta[3], a depender do nível de participação do titular no processo.

A transferência direta é aquela realizada entre o titular e a importadora dos dados diretamente, hipótese na qual o próprio titular contrata um serviço e participa do processo de transferência internacional. Esse seria o caso, por exemplo, da contratação pelo titular de um serviço de *cloud* de um fornecedor internacional.

Já a transferência internacional indireta pode ocorrer de duas formas. A primeira delas é a transferência de dados entre aquele que possui relação com o titular de dados e um terceiro, sem a participação direta do titular. Essa hipótese se aplica aos casos nos quais, por exemplo, a prestadora utiliza serviços de *cloud* para fazer o seu *backup* e, dentre esses dados, estão os do titular. Outro exemplo que pode ser citado nessa modalidade é a transferência de dados de RH para o controlador de empresa brasileira que está localizado em outro país.

A segunda hipótese da transferência internacional indireta é caracterizada pelo uso de dados pessoais públicos, não existindo relação direta com o titular nem com outras empresas. Ressalta-se que, ainda nesse caso, o tratamento de dados tornados manifestamente públicos pelo titular dispensa o seu consentimento, mas os seus direitos e os princípios da LGPD devem ser observados, de acordo com o art. 7º, §4º, da LGPD.

3 MASCARENHAS, Fernanda; AQUINO, Theófilo. O regime de transferência internacional de dados na LGPD: delineando as opções regulatórias em jogo. In: Bioni et al (Coords.) *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 302.

Cada uma dessas hipóteses de transferência pode ser enquadrada em diferentes instrumentos legais autorizativos. Assim, passa-se à breve análise de cada uma das previsões do art. 33 da LGPD. Para compreensão sobre o âmbito de aplicação, analisaremos três aspectos: i) participação do titular na transferência; ii) necessidade de intervenção da autoridade; e iii) atendimento de interesse público.

III.3. Instrumentos legais para a transferência internacional de dados

a) Países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado (inciso I)

Conforme apontado no item introdutório, existiam dois tipos de modelos em pauta nas discussões do projeto da LGPD, o modelo geográfico e o modelo de responsabilização. O modelo geográfico foi o escolhido para subsidiar a hipótese prevista no art. 33, I, uma vez que se trata de hipótese de autorização da transferência internacional quando "países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado".

Nesse caso, a transferência dos dados independe da participação do titular no processo, mas o nível de proteção do país necessita de análise pela ANPD ou ao menos requer que a autoridade determine de forma mais detalhada quais requisitos devem ser levados em consideração, nos termos do art. 34 da LGPD. O que se sabe é que a definição quanto à adequação do nível de proteção do país do importador requer tempo, e mesmo a União Europeia – que possui uma metodologia de avaliação das hipóteses de transferência desde a Diretiva de 1995 – emitiu até hoje apenas 12 decisões de adequação.[4]

Independentemente dos parâmetros específicos definidos pela autoridade, o art. 34 prevê que a decisão de adequação será pautada nos seguintes critérios: I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; II - a natureza dos dados; III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; IV - a adoção de medidas de segurança previstas em regulamento; V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI - outras circunstâncias específicas relativas à transferência.

Após definição pela ANPD dos países que possuem nível de proteção adequado, os controladores poderão realizar transferências internacionais para esses países sem que seja necessário a aprovação pela autoridade, ou o cumprimento das outras hipóteses do art. 33.

Ademais, também é importante ressaltar que o recebimento de dados pessoais por meio do envio por outros países depende da avaliação da política de transferência de dados pessoais do país de origem, sendo necessária a avaliação dos requisitos de compatibilidade ou adequação das legislações estrangeiras. A União Europeia, por exemplo, também possui diversos instrumentos que possibilitam a transferência internacional de dados, incluindo a hipótese de avaliação do nível de proteção do país por meio de decisão da Comissão Europeia. Nessa hipótese, caso fosse decidido que o Brasil possui um nível adequado de proteção, seria possível que exportadores enviassem dados para o Brasil sem que fossem necessárias garantias suplementares ou condições adicionais previstas no GDPR.

b) Garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD (inciso II)

O inciso II do artigo 33 prevê que a transferência internacional pode ocorrer quando o controlador garantir o cumprimento do regime de proteção de dados da LGPD, por meio de a) cláusulas contratuais específicas; b) cláusulas contratuais padrão; c) normas corporativas globais; d) selos, certificados e códigos de conduta. Já o art. 35 da LGPD prevê que "a **definição do conteúdo** de cláusulas-padrão contratuais, bem como a **verificação** de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, **será realizada pela autoridade nacional".**

Ademais, os parágrafos do art. 35 também preveem que i) deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei; ii) na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional,

4 Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário; iii) a autoridade nacional poderá designar organismos de certificação para a realização do previsto no art. 33; iv) os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, podem ser submetidos a revisão ou anulados; v) as garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46[5] da LGPD.

Observa-se que a redação do caput do artigo 35 apresenta duas formas de atuação da autoridade na análise das garantias: **i) definição de conteúdo das cláusulas contratuais padrão; ii) verificação de cláusulas contratuais específicas, normas corporativas globais, selos, códigos de conduta etc**. Percebe-se a partir da redação desse dispositivo que é possível, a partir de uma regulamentação mais flexível e ao mesmo tempo protetiva, estabelecer alguns critérios para a definição de tais cláusulas. Isso permitiria manter a autonomia dos agentes que desejem utilizar contratos como base para a transferência, evitaria um processo excessivamente burocrático e possibilitaria, ainda, a garantia de um padrão de proteção adequado.

As cláusulas padrão remetem ao sistema das *Standard Contractual Clauses* – SCCs da União Europeia, nas quais o conteúdo pré-aprovado das cláusulas deve ser utilizado nos exatos termos propostos pela autoridade. Destaca-se que o rígido modelo europeu das SCCs não precisa ser necessariamente seguido pelo Brasil, o que pode ser demonstrado pelo sistema da Nova Zelândia. Este país, a despeito de ter desenvolvido um sistema de transferência internacional mais flexível do que o europeu, obteve decisão favorável de adequação da UE.

5 Art. 46 - § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Essas duas hipóteses diferem, ainda, do previsto no inciso IX, que faz referência ao art. 7º, V, que trata da execução contratual ou de procedimentos do qual o titular seja parte e que seja feito a pedido do próprio titular. Nos casos previstos neste inciso (II), compreende-se que o nível de participação do titular não é requisito para a transferência.

Como exemplo, podemos utilizar os casos em que uma prestadora de telecomunicações brasileira é contratada por determinada pessoa jurídica para a prestação de serviços de *cloud service*. Nessa situação, a cliente, empresa brasileira, é considerada a controladora desse tratamento, mas pode contratar uma empresa internacional para oferecer a infraestrutura que possibilita o armazenamento das informações do titular na nuvem, sendo a organização estrangeira considerada a operadora dos dados pessoais. O mesmo se aplica caso a prestadora nacional realize o mesmo serviço.

Em relação às normas corporativas globais e aos selos, certificados e códigos de conduta, também não está claro de que forma a autoridade realizará a verificação dessas garantias: se serão estipulados requisitos que podem ser livremente avaliados pelos agentes de tratamento, ou se a avaliação deve ser feita de forma prévia pela ANPD. Ademais, conforme previsto no parágrafo 3º do art. 35, a autoridade pode se utilizar de organismos de certificação para a avaliação das garantias.

De qualquer forma, esse é um aspecto que gera grande insegurança jurídica para os agentes, de modo que, até que a autoridade se posicione sobre o tema, outros instrumentos devem ser utilizados sempre que possível.

c) Proteção da vida ou da incolumidade física do titular ou de terceiros (inciso IV)

A hipótese prevista no art. 33, inciso IV, deve ser utilizada excepcionalmente, apenas quando a vida do titular ou do terceiro dependa do tratamento de dados possibilitado pela transferência internacional. Não é possível, nesse caso, realizar interpretação ampla sobre proteção da vida, assim como na aplicação do art. 7º VII e 11, II, e, da LGPD.

d) Autorização pela ANPD (inciso V)
Essa hipótese prevê que as transferências internacionais podem ser realizadas quando a ANPD autorizar, possibilitando que, caso o tratamento pretendido não esteja alinhado com as hipóteses previstas no art. 33, a autoridade pode analisar as especificidades do caso de forma particular. Assim, trata-se de hipótese ampla que possibilita casos não previstos em lei também possam ser autorizados.

e) Compromisso assumido em acordo de cooperação internacional (inciso VI)
A transferência internacional de dados também pode ser realizada sem a autorização da autoridade ou relação direta com o titular quando resultar em compromisso assumido em acordo de cooperação internacional. Tal hipótese é importante para garantir que os instrumentos de cooperação não sejam submetidos a procedimentos excessivamente burocráticos que podem comprometer relações diplomáticas.

g) Execução de política pública (inciso VII)
A execução de políticas públicas é um exemplo claro das hipóteses nas quais o interesse público é levado em consideração na permissão do tratamento de dados. Tal hipótese deve ser utilizada pelos agentes que possuem prerrogativas para tanto, não sendo necessária a sua submissão à ANPD.

h) Consentimento (inciso VIII)
Uma das hipóteses de autorização da transferência internacional de dados é o consentimento do titular, nos termos do art. 7º da LGPD. Este, para ser válido, deve ser livre, informado e inequívoco. Para tanto, é importante que o titular seja informado sobre a possibilidade de não fornecer o consentimento e quais as consequências dessa negativa (art. 18, LGPD).

Para a validade do consentimento no caso de transferências internacionais, é necessário que o titular tenha sido informado especificamente sobre esse tratamento e tenha direcionado seu aceite para esse tratamento, inclusive pela previsão do §1º do art. 7º, da LGPD, de necessidade de informação prévia, transparente e de forma clara e inequívoca sobre as informações que subsidiaram o consentimento.

Esse instrumento de transferência é mais comumente utilizado nos casos em que a organização internacional que irá receber os dados do titular se recusou a adotar salvaguardas de segurança e a empresa brasileira não consegue comprovar o nível adequado de proteção aos dados dessa organização parceira.

Contudo, nem sempre o consentimento do titular será a base mais adequada para o caso concreto, devendo ser avaliada a utilização das outras hipóteses expostas nesse protocolo, em especial o disposto no art. 33, IX, que possibilita a transferência internacional amparada nas bases legais do contrato, da obrigação legal ou regulatória e no exercício regular de direitos.

Quando o consentimento for coletado, é obrigação dos agentes de tratamento oferecer o gerenciamento do consentimento, com a possibilidade de o titular revogá-lo a qualquer momento (art. 8º, §5º, LGPD). Também é possível que o titular requeira a cópia integral de seus dados pessoais tratados com base no consentimento (art. 19, §3º, LGPD) ou a eliminação de seus dados, salvo as exceções legais previstas no art. 16. Contudo, é necessário considerar que, nos casos envolvendo transferências internacionais, toda a gerência do consentimento pode demorar mais do que quando o tratamento fica restrito ao território brasileiro ou, ainda maiores, do que nos casos em que o tratamento é feito completamente internamente.

i) Hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD (inciso IX)
Conforme exposto, essa categoria de derrogações possui relação direta com as bases legais que já permitem a realização de tratamento de dados em território nacional, quais sejam: i) cumprimento de obrigação legal ou regulatória (art. 7º, II, da LGPD); ii) execução de contrato do qual o titular seja parte (art. 7º, V, da LGPD); e iii) exercício regular de direitos (art. 7º, VI, da LGPD).

A primeira hipótese já foi discutida neste Código, especialmente no Protocolo de Compartilhamento, sendo essencial para os prestadores de serviços de telecomunicações. Essa hipótese prevê que se a transferência internacional for determinada pelo próprio órgão regulador ou pela legislação, não é necessária a participação direta do titular ou a autorização da ANPD.

Em relação à "ii) execução de contrato do qual o titular seja parte", para utilização dessa hipótese é necessária a relação direta com o titular dos dados com o contrato executado. Utilizando o exemplo do serviço de *cloud* que foi mencionado no tópico "III.3. b) Garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD (inciso II)" supra, essa base seria aplicável se o titular fosse o contratante do serviço de *cloud* de empresa estrangeira, que armazena seus dados no exterior.

Por fim, o exercício regular de direitos pode ser compreendido também nos termos do art. 7º, tendo em vista que se trata de hipótese na qual o controlador precisa dos dados para assegurar seu contraditório ou mesmo para o seu direito de petição. Nesse caso, também não é necessária a participação direta do titular, tampouco a autorização da ANPD.

III.4. Boas práticas para transferência internacional de dados

De forma geral, independentemente do instrumento legal adotado, sugere-se que as partes envolvidas na transferência busquem meios de assegurar que os princípios da legislação serão cumpridos, em especial o da minimização.

Caso as cláusulas contratuais sejam adotadas, é importante que haja previsão no instrumento contratual sobre a transferência internacional, inclusive para o cumprimento do princípio da transparência. A principal obrigação do controlador em relação a esse ponto é garantir que a informação sobre a transferência internacional seja repassada ao titular e que seja possível comprovar que aquele indivíduo teve acesso a essa informação antes de firmar o contrato.

Nesses casos, é recomendado que os contratos entre os agentes de tratamento contenham cláusulas contratuais prevendo salvaguardas para a segurança dos dados, de forma a assegurar o nível adequado de proteção. Também é através do instrumento contratual que será definida a posição de cada organização (controlador ou operador) e as principais obrigações de cada um desses. Além disso, é incentivado o reforço das informações sobre as transferências internacionais realizadas pela organização nas políticas de privacidade disponibilizadas pela empresa, principalmente em relação aos serviços que dependem desses tratamentos transfronteiriços para a sua realização.

III.5. Próximos passos para a regulamentação da transferência internacional de dados

Observa-se que a maioria dos instrumentos acima analisados dependem de regulamentação da ANPD, cuja atuação será fundamental para constituir um ambiente adequado e seguro, que viabilize as frequentes transferências internacionais tão necessárias para a economia globalizada.

Como exemplo de um sistema simplificado, a Autoridade da Nova Zelândia oferece uma ferramenta[6] de criação automática de cláusulas contratuais que preveem a adoção de salvaguardas que garantem a proteção dos dados, além da publicação de guia para criação de documentos que sejam suficientes para justificar a transferência internacional de dados[7]. Ressalte-se que esse modelo já teve seu nível de adequação reconhecido pela União Europeia, sendo um modelo que prioriza a liberdade contratual do titular e das organizações, além de se basear principalmente em mecanismos de *accountability* para possibilitar o fluxo transfronteiriço dos dados pessoais.

Nesse contexto, é fundamental que a ANPD adote um processo eficiente e simples, que facilite a realização de transferências internacionais, com enfoque em instrumentos particulares, garantindo ao mesmo tempo a proteção dos dados pessoais. A existência de um processo simplificado permitiria maior segurança jurídica em situações nas quais o consentimento não pode ser coletado ou que sua coleta seria inviável dada a natureza da atividade de tratamento, como é o caso da contratação de serviço de *cloud* para armazenamento externo dos dados tratados pelas prestadoras.

6 Disponível em: https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/model-clause-agreement-builder/.

7 Disponível em: https://privacy.org.nz/assets/DOCUMENTS/IPP12-guidance/2.-IPP-12-Model-Clauses-Guidance-Document-web-Oct.pdf.

IV - PROTOCOLO PARA GARANTIA DO DIREITO DOS TITULARES

IV.1. Introdução

A criação de ordenamento específico para a proteção de dados pessoais tem o condão de garantir que, mesmo diante da eventual impossibilidade de ter maior controle sobre os tratamentos de dados por meio do mecanismo do consentimento e de sua revogação, em determinados contextos seja garantido ao titular a transparência e o conhecimento sobre o fluxo de dados pessoais. Em linha com esse entendimento, o artigo 17 da LGPD é inequívoco ao prever que "toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade".

Nesse contexto, a LGPD assegura procedimentos que visam garantir o controle de seus dados pelo titular, entre os quais estão incluídos os direitos de Acesso; Retificação; Cancelamento e Oposição (tradicionalmente conhecidos pela sigla "ARCO"). Ademais, também serão incluídos os direitos à transparência, portabilidade de dados e de revisão de decisões automatizadas, previstos nos arts. 18, V[1], e 20[2] da LGPD. Tendo em vista a ausência de procedimentos e requisitos mínimos estabelecidos pela

1 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

2 Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

ANPD, neste protocolo serão apresentadas soluções para garantia de tais direitos com base nas melhores práticas internacionais[3].

Ademais, também consideramos as disposições específicas da legislação setorial que possui diversas obrigações relacionadas ao acesso a informações pelos usuários.

Os direitos do titular de dados não são absolutos, devendo ser interpretados considerando outros direitos fundamentais, bem como o contexto em que se inserem[4]. Como exemplo, tem-se a experiência do Reino Unido, por meio da *Information Commissioner's Office* (ICO), que entende que o direito de acesso a dados pode ser limitado se o titular já tiver os dados, se o fornecimento das informações for impossível ou exigir esforço desproporcional, o acesso prejudicar o próprio tratamento de dados ou o controlador estiver submetido a uma norma de sigilo[5].

É possível também que existam outras limitações ao exercício desses direitos, tais como a proteção de interesse de terceiros, proteção aos segredos comerciais e industriais, a proteção contra fraude, ou mesmo o risco de que o acesso às informações possa prejudicar investigação em processo criminal ou administrativo.[6]

Ademais, embora a maioria dos titulares de dados exerça esses direitos de modo leal, é possível que haja abuso de direito, se eles forem exercidos contrariando a boa-fé, não sendo o controlador obrigado nessa hipótese ao seu cumprimento, se comprovar esse abuso.[7] Entende-se relevante que a Autoridade Nacional de Proteção de Dados especifique essas situações que podem gerar abuso de direito, de modo a trazer maior segurança jurídica para tais situações.

IV.2. Transparência e políticas de privacidade

A transparência é um dos princípios norteadores da LGPD que traz a obrigação de os agentes de tratamento garantirem informações claras, precisas e facilmente acessíveis aos titulares sobre os tratamentos, controlador e operador. Essa imposição encontra limites na observância dos segredos comercial e industrial, respeitados pela lógica da LGPD.

Diante disso, uma das formas de garantir a comunicação facilitada dessas informações adotadas pelas organizações é a disponibilização de políticas de privacidade em meios de fácil acesso (como sites, aplicativos). Esses documentos devem informar as principais formas de coleta de dados pessoais, os tratamentos mais corriqueiros ou sensíveis, os compartilhamentos de dados e quem recebe tais informações, quais medidas de segurança são adotadas e os direitos do indivíduo em relação à proteção de seus dados pessoais. Também são boas práticas a disponibilização de informações referentes ao uso de tecnologias de rastreamento, decisões automatizadas, diferenças relacionadas aos tratamentos com clientes e potenciais clientes e quaisquer outras informações que possam interessar ou afetar o titular.

Além disso, caso exista alguma mudança significativa da política de privacidade, é dever da organização comunicar publicamente tal fato, preferencialmente no sítio eletrônico do controlador, a fim de que o máximo de titulares afetados tome conhecimento de tais alterações e possa tomar as providências que achar adequadas, inclusive com a possibilidade de exercer o direito à oposição caso considere as mudanças ilegítimas.

Essas políticas são relacionadas tanto aos titulares que possuem relacionamento com a organização quanto aqueles que não possuem nenhuma

3 Este protocolo foi elaborado com base nos requisitos apresentados no Código de Boas Práticas para Prestadores Privados de Saúde da CNSaúde, disponível em: http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/. Tais requisitos se basearam nos seguintes códigos: AEPD. *Código tipo de la unió catalana d'hospitals*. 2020. Disponível em: https://www.aepd.es/sites/default/files/2020-01/ct-uch-cat.pdf; FARMAINDÚSTRIA. *Codigo tipo de farmaindustria de proteccion de datos personales en el ambito de la investigacion clinica y de la farmacovigilancia*. Nov/2009; ANEIMO; AEDEMO. *Codigo de Conducta para el tratamiento de datos de caráter personal por organizaciones de investigación de mercado, social, de la opinión y del análisis de datos*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/; https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf.

4 CIPL. O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://wpcdn.idp.edu.br/idpsiteportal/2020/08/pt_cipl-idp_whitepaper_anpd-1.pdf.

5 ICO. *Guide to the General Data Protection Regulation*. 2021. P. 101. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf.

6 CIPL. O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD) Disponível em https://wpcdn.idp.edu.br/idpsiteportal/2020/08/pt_cipl-idp_whitepaper_anpd-1.pdf , p. 15 a 17.

7 Ibidem, p. 17.

forma de relação estabelecida com a companhia. Contudo, tais políticas não são suficientes para observância do princípio da transparência em relação aos colaboradores da empresa (p.ex.: empregados, terceirizados, prestadores de serviço) e, por essa razão, também é uma boa prática a adoção e disponibilização de avisos de privacidade internos com informações relativas aos tratamentos dos dados desses indivíduos.

Para cumprir com as exigências legais, é necessário que esses documentos adotem uma linguagem acessível. Também devem adotar textos curtos e podem utilizar imagens ou outras formas interativas que garantam a compreensão de todas as informações pelos mais distintos titulares.

Veja-se que a acessibilidade das informações pode ser importante mesmo fora das políticas de privacidade disponibilizadas nos sites, conforme elucida o conceito "*user-centric transparency*" (transparência voltada para o usuário)[8]. Trata-se de um conceito efetivamente voltado para a compreensão do conteúdo pelo usuário e não somente destinado ao cumprimento de requisitos impostos pelos reguladores. Para tanto, é necessário que a transparência seja centrada no usuário, específica para o contexto, flexível, dinâmica e passível de adaptações, possibilitando que o usuário obtenha informação de forma clara e compreensível, mesmo nas situações em que o consentimento não seja a base legal aplicável.

Assim, sugere-se que todas as informações apresentadas aos titulares sigam esse conceito, apresentando esclarecimentos adaptados aos contextos específicos do tratamento de dados e por meio da utilização de outros mecanismos além da linguagem escrita puramente descritiva.

IV.3. Acesso

O titular tem direito de acessar e receber uma cópia de seus dados pessoais, bem como outras informações que sejam pertinentes ao tratamento de seus dados. Tal pedido pode ser realizado pelos canais oficiais disponibilizados pelas próprias prestadoras, especialmente pelo canal de contato com o encarregado ou indicado no sítio eletrônico do controlador, não sendo possível cobrança de nenhuma natureza pela prestadora para o exercício desse direito, sob pena de impedimento indireto de acesso.

Ressalta-se que caso se trate de pedido excessivo ou que possa comprometer direitos relativos aos segredos comerciais ou industriais das empresas, a LGPD resguarda o direito da empresa de não fornecer tais informações (art. 6º, VI).

Conforme orientação da Autoridade Nacional de Proteção de Dados do Reino Unido (Information Comissioner's Office - ICO), caso sejam solicitadas informações a respeito do compartilhamento de dados com outras entidades e a informação sobre sua identidade combinada tiver o potencial de revelar segredo comercial ou industrial, o controlador pode optar entre informar o nome da organização ou a categoria na qual se enquadra, a depender de qual delas pode representar risco menor[9].

Ademais, o direito de acesso está diretamente relacionado ao princípio do livre acesso, transparência e prestação de contas, de modo que a recusa em prestar as informações solicitadas deve ocorrer tão somente em situações fundamentadas. Dessa forma, recomenda-se que algumas medidas sejam tomadas pelas prestadoras ao preparar o procedimento de atendimento às solicitações de informação, tais como:

Estabelecer fluxos para quando for solicitado o direito de acesso e meios para identificar um pedido de informação.
Registrar a data do recebimento do pedido.
Ter uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.

8 CIPL. *Reframing data transparency*. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/reframing_data_transparency.pdf. CIPL. *Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR*. 2017. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

9 Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Estabelecer prazos para atender os pedidos de informação, respeitando o limite de 15 (quinze) dias estabelecido no art. 19 da LGPD e hipóteses de interrupção do prazo quando são necessárias informações adicionais impeçam o atendimento do pedido.
Estabelecer os limites das informações que não podem ser prestadas, identificando quais informações são relativas a segredos comerciais e industriais.
Possuir sistemas de gerenciamento de informações eficientes que permitam a identificação e localização das informações.
Identificar quando um pedido de informação pode envolver dados de outros titulares.
Criar um procedimento de autenticação do titular dos dados que está recebendo as informações, para evitar o compartilhamento indevido de informações.
Possuir procedimentos de autenticação do titular dos dados.
Identificar se os dados solicitados são pertinentes e informar, ao menos: i - finalidade específica do tratamento; ii - forma e duração do tratamento, observados os segredos comercial e industrial; iii - identificação do controlador; iv - informações de contato do controlador; v - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; vi - responsabilidades dos agentes que realizarão o tratamento; vii – direitos do titular especificados no art. 18 da LGPD.

IV.4. Retificação

O art. 18, III, LGPD garante o direito de retificação de dados que sejam incorretos, incompletos ou desatualizados, em consonância ao princípio da qualidade dos dados, que garante que os dados dos titulares sejam exatos, claros, relevantes e atualizados. Da mesma forma que o pedido de acesso, o pedido pode ser recusado tão somente em hipóteses excepcionais.

Por isso, as prestadoras devem buscar adotar, no atendimento do direito de retificação, os seguintes procedimentos:

Estabelecer quando o direito de retificação se aplica e como identificar um pedido de retificação.
Registrar a data do recebimento do pedido.
Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.
Estabelecer prazos para atender o pedido de retificação e hipóteses de interrupção do prazo quando são necessárias providências adicionais.
Possuir procedimentos de autenticação do titular dos dados.
Ter sistemas de gerenciamento de informações eficientes que permitam a retificação das informações.

IV.5. Cancelamento de operações de tratamento

O titular dos dados tem o direito de solicitar o cancelamento de operações de tratamento que não cumpram os requisitos legais, bem como a exclusão de dados pessoais tratados a partir do consentimento. Assim, o titular também tem direito de cancelar dados que foram armazenados de forma indevida ou cujo consentimento foi revogado, quando a base legal do consentimento for aplicável. Observa-se que este item se correlaciona a outros direitos previstos na LGPD como o princípio da minimização e impossibilidade de tratamento de dados em desconformidade com a legislação, bem como com o direito de revogação de consentimento, sendo necessário interpretá-lo em conjunto com outros dispositivos.

Nesse sentido, os seguintes procedimentos fazem parte do atendimento dos pedidos de cancelamento das operações:

Estabelecer quando o direito de cancelamento se aplica, como identificar um pedido de cancelamento e com quais outros dispositivos da LGPD ele pode estar relacionado.

Registrar a data do recebimento do pedido.

Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.

Estabelecer prazos para atender o pedido de cancelamento ou exclusão e hipóteses de interrupção do prazo quando são necessárias providências adicionais.

Identificar se foi dado o consentimento para o tratamento do dado e se é possível revogá-lo, de acordo com as normas setoriais.

Possuir procedimentos para informar outros operadores que porventura também realizem o tratamento em nome do controlador acerca do cancelamento ou com quem o dado tenha sido compartilhado.

Possuir sistemas de gerenciamento de informações eficientes que permitam o cancelamento das informações e sua eliminação física.

Possuir procedimentos de autenticação do titular dos dados.

IV.6. Oposição

De acordo com o art. 18, § 2º, da LGPD, o titular tem o direito de oposição ao tratamento, mesmo que o consentimento não tenha sido coletado, em caso de descumprimento aos dispositivos legais. Assim, os seguintes procedimentos compõem o atendimento das solicitações:

Identificar a oposição ao tratamento de dados e quando esse direito é aplicável.

Registrar a data do recebimento do pedido.

Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.

Estabelecer prazos para atender à oposição ao tratamento e hipóteses de interrupção do prazo quando são necessárias providências adicionais.

Possuir sistemas de gerenciamento de informações eficientes que permitam a efetivação do direito de oposição, como o cancelamento, a retificação e outros tipos de alterações relativas aos dados pessoais.

Possuir procedimentos de autenticação do titular dos dados.

IV.7. Decisões automatizadas

Nos termos do art. 20 da LGPD, o titular dos dados tem direito a solicitar a revisão de decisões quando estas foram tomadas unicamente com base em tratamento automatizado de dados pessoais, sem intervenção humana significativa, que afetem seus interesses. Assim, tendo em vista a possibilidade de as prestadoras utilizarem recursos automatizados próprios para definição de perfis de consumo e de crédito, é importante, nesses contextos, que seja garantido um conjunto de regras para aferição e análise, possibilitando o devido processo para revisão de tais decisões.

Para além do direito de revisão, a lei prevê um direito à explicação. Isto é, o titular deve ter acesso ao esclarecimento sobre como funcionam as decisões automatizadas, bem como sobre os tipos de dados e critérios utilizados nessas decisões. Contudo, tal direito de explicação deve ser exercido respeitados os segredos comerciais e industriais das prestadoras (art. 20, § 2º, LGPD).

É necessário que este direito seja comunicado por meio das políticas de privacidade e outras formas de comunicação, de modo a informar o titular sobre a utilização de tais decisões automatizadas, quais os critérios utilizados, bem como as suas consequências para o titular.

Considerando também o princípio da não discriminação (art. 6º IX, LGPD), é preciso assegurar que as decisões automatizadas não tenham efeitos discriminatórios, visto que a lei veda tanto a discriminação abusiva quanto a ilícita.

IV.8. Oferta de produtos e serviços por meio de contato telefônico

Conforme mencionado na Parte I, a programa "www.naomeperturbe.com.br" constitui iniciativa para conciliar os interesses dos consumidores, que não querem receber abordagens do telemarketing das prestadoras, e das prestadoras que necessitam se comunicar com os consumidores para expandir os seus negócios. Essa iniciativa está alinhada com os direitos dos titulares expostos neste protocolo, tendo em vista que possibilita uma forma facilitada de cancelamento/bloqueio de uma atividade de tratamento de dados que pode gerar os contatos das prestadoras.

Nesse sentido, é necessário ressaltar que são objeto de bloqueio apenas as ligações de telemarketing, "realizadas diretamente pelas prestadoras de Serviços de Telecomunicações participantes, pelas Instituições financeiras participantes ou por terceiros autorizados[10], destinadas à divulgação de serviços e produtos com a intenção de venda ao usuário. Desta forma, não serão afetados por este cadastro as demais ligações, destinadas ao relacionamento entre o usuário e a prestadora de Serviços de Telecomunicações/Instituições Financeiras"[11].

Também não são abarcados pelo programa os contatos necessários para a efetiva prestação do serviço contratado (como os contatos realizados por prestadoras de telefonia para avisar sobre a indisponibilidade do sistema) ou mesmo ligações realizadas confirmar visitas ou procedimentos necessários para a manutenção do serviço contratado. Ademais, não entram no escopo do projeto o envio de mensagens de texto, tampouco é possível impedir que sejam realizadas ligações de setores que não fazem parte do programa.

Para se cadastrar no serviço, o titular que tiver interesse em bloquear os contatos indesejados deve realizar o cadastro no site www.naomeperturbe.com.br, fornecendo e-mail, nome, CPF e telefone e o bloqueio dos contatos telefônicos realizados para o número telefônico cadastrado ocorrerá em até 30 dias corridos a partir da data de solicitação.

10 Ressalta-se que a realização de contatos telefônicos por terceiros não autorizados pelas prestadoras não se enquadra no referido programa, tendo em vista que as prestadoras não possuem qualquer ingerência sobre as suas ações ou relação com esses agentes.

11 Disponível nos Termos e Condições de Uso do website www.nãomeperturbe.com.br.

V - PROTOCOLO PARA REGISTRO DE OPERAÇÕES DE TRATAMENTO

Passo essencial no processo de adequação à LGPD é o mapeamento dos tratamentos de dados pessoais, previsto no art. 37 da LGPD[1]. É a partir desse processo que será possível definir o embasamento legal referente a cada atividade de tratamento, a criação de política de privacidade completa e encontrar os fluxos que precisam de reformulação. Após o mapeamento inicial, é necessário o registro constante de novos fluxos ou produtos, além da atualização de processos já existentes.

Como fruto desse procedimento, recomenda-se a manutenção de registro das operações de tratamento (também chamado de "*Record of Processing Activities*" – ROPA). Isso pode ser realizado de diferentes formas, como por meio da utilização de *softwares* específicos ou até por meio da elaboração de tabelas, desde que sejam constantemente atualizadas e que a organização seja capaz de comprovar que a avaliação dos tratamentos é realizada de forma contínua. Esse material é relevante para qualquer avaliação que vier a ser feita pela ANPD, e deve ser elaborado tanto pelos controladores quanto pelos operadores de dados.

Ainda que a LGPD não tenha determinado qual conteúdo mínimo deve ser mapeado, o controlador deve descrever o mais detalhadamente possível quais dados são tratados e quais são as atividades de tratamento realizadas em cada área de negócio, tendo em vista que cada área pode ter finalidades distintas de tratamento para o mesmo dado. Nesse sentido, também é necessário compreender o fluxo interno dos dados, para que fique evidente se os princípios estão sendo cumpridos ao longo de toda a cadeia de tratamento.

1 Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Importante ressaltar que o nível de detalhamento para o mapeamento de dados dos controladores e dos operadores não é o mesmo, sendo o documento dos operadores mais sucinto. No caso dos operadores, sugere-se que, inicialmente, seja identificado o controlador dos dados e que o detalhamento dos processos deixe claro quais dados estão sendo tratados, quais as suas finalidades, medidas de segurança que são adotadas etc.

Nesse sentido, com base nas melhores práticas internacionais[2] e do setor, recomendamos que o registro de operações possua informações como:

Informações sobre fluxos de dados	Processo de tratamento
	Área de negócio responsável
	Finalidade do tratamento
Informações sobre os dados pessoais tratados	Tipo de dados
	Categoria dos dados (se é ou não sensível)
	Categoria do titular dos dados
	Finalidade do tratamento de cada dado coletado
Informações sobre coleta e compartilhamento de dados	Onde o dado foi coletado?
	O dado é compartilhado internamente?
	O dado é compartilhado com terceiros?
	O dado é transferido para outros países?
Armazenamento	Onde os dados são armazenados?
	Existe controle de acesso?
	Existe uma política de exclusão dos dados?
	Se embasada em norma legal, descrever
Embasamento	Base legal
	Se utilizado o consentimento, ele pode ser retirado?
	Se utilizada obrigação legal ou regulatória, descrever
	Se utilizado legítimo interesse, foi realizada a avaliação de Legítimo Interesse?

2 Nesse sentido ver: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/.

VI - PROTOCOLO PARA AVALIAÇÃO DE LEGÍTIMO INTERESSE

Por se tratar de hipótese autorizativa considerada ampla, a Avaliação de Legítimo Interesse - LIA é um passo importante para garantir a aplicação correta da base legal prevista no art. 7º, IX, cumprindo com os termos do art. 10[1], da LGPD. Importa ressaltar que não existe hierarquia na utilização de bases legais, de modo que bases como consentimento não são superiores ao legítimo interesse, tampouco este deve ser considerado o "último recurso"[2]. É necessário, contudo, considerar as finalidades do tratamento e o tipo de dado tratado, uma vez que dados sensíveis não podem ser tratados sob essa base legal.

Especialmente quando comparada à base legal "consentimento", o legítimo interesse pode trazer vantagens para o tratamento, tendo em vista que o consentimento pode não ser facilmente coletado ou pode ser passível de revogação. Isso sem falar das recentes discussões sobre a fadiga do consentimento, que argumentam que a utilização excessiva do consentimento como fundamento legitimador do tratamento de dados pode comprometer a sua efetividade e o seu papel como ferramenta de garantia da autodeterminação informativa.[3]

1 Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

2 CIPL. *How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation*. Disponível em> https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf

3 SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, v. 126, pp. 1880-1903, 2013. SCHWARTZ, Paul M. Internet Privacy and the State. *Connecticut Law Review*, v. 32, pp. 815-859, 2000. CATE, Fred e MAYER-SCHÖNBERGER, Viktor. Notice and Consent in a World of Big Data, In: *International Data Privacy Law*, 2013, Vol. 3, No. 2.

Nesse sentido, ainda que a ANPD não tenha se manifestado acerca dos parâmetros para utilização da base legal do legítimo interesse, recomenda-se a utilização do LIA antes que o tratamento seja iniciado ou quando a finalidade do tratamento for modificada. Esse procedimento baseia-se nas melhores práticas do setor, bem como nas melhores práticas internacionais[4], sendo o modelo Europeu a base para o protocolo proposto. Assim, sugere-se que, os seguintes elementos sejam observados:

- Contexto, propósito e benefício das atividades de processamento de dados, além dos riscos de não realizar o processamento
- O interesse legítimo do controlador, terceiros ou grupos de indivíduos ou da sociedade, assim como seus direitos e liberdades e outros direitos relativos à proteção de dados
- Interesses, liberdades e direitos dos titulares, bem como suas expectativas legítimas nas quais estão fundadas a sua relação com o controlador
- Riscos e danos que podem resultar do tratamento ou da ausência de tratamento, bem como a gravidade que tais danos podem causar aos titulares

Para análise desses elementos, pode ser utilizado um teste de 3 (três) etapas, para que seja verificado: i) a finalidade, ii) a necessidade e iii) a proporcionalidade. Repise-se, ainda que esses três testes não tenham sido oficialmente internalizados pela ANPD, sugerimos que seus parâmetros sirvam como base para reflexão para utilização dessa base legal.

4 EDPB. Disponível em: https://iapp.org/media/pdf/resource_center/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf; ICO. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/; CIPL. Disponível em> https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf ; IAPP Disponível em: https://iapp.org/resources/article/guidance-on-the-use-of-legitimate-interests-under-the-eu-general-data-protection-regulation/.

Parte 1 – Identificando o legítimo interesse
Qual o propósito do processamento de dados?
Qual o benefício que se espera do processamento?
O tratamento de dados pessoais é realizado por terceiro para atender um legítimo interesse da Companhia?
Por que esse processamento é importante para o controlador?
Algum interesse público pode ser atingido com o processamento?
Existe algum problema ético ou discriminatório no processamento?

Parte 2 – Teste da necessidade
Este processamento irá auxiliar no propósito buscado?
Este propósito pode ser atingido de outras formas?
É possível atingir o mesmo objetivo utilizando menos dados ou processando esses dados de forma menos invasiva?

Parte 3 – Teste da proporcionalidade
Há expectativa do titular de que esses dados sejam tratados?
Qual a natureza da relação entre o titular dos dados e o controlador?
Quais os possíveis impactos do tratamento de dados nos titulares e o quão graves eles podem ser?
Algum dos titulares está vulnerável de alguma forma?
Os dados foram obtidos diretamente dos titulares?
É possível oferecer o "*opt-out*" ao titular sem que o tratamento seja comprometido?
Informações sobre o tratamento de dados são fornecidas ao titular? A comunicação é clara e anterior aos propósitos do tratamento de dados?
É possível adotar salvaguardas?

Ao final do teste, o controlador deve decidir se deve ou não realizar o processamento com a base legal do legítimo interesse. Não há uma fórmula que possibilite uma resposta exata ao final do teste, contudo, é necessário identificar se os benefícios gerados pelo processamento não serão superados pelos riscos. Ademais, caso não tenham sido adotadas, sugerimos

que salvaguardas e controles, como anonimização, controle de acesso aos dados, mecanismos de autenticação, inventário com acessos aos registros de conexão e acesso a aplicações, sejam adotadas sempre que possível.

Conforme exposto no art. 10, § 3º, da LGPD, na utilização da base legal do legítimo interesse, a ANPD pode solicitar a apresentação de Relatório de Impacto, que deve ser apresentado nos termos do Protocolo para Elaboração de Relatório de Impacto apresentado a seguir.

VII - PROTOCOLO PARA ELABORAÇÃO DE RELATÓRIO DE IMPACTO

O Relatório de Impacto é o documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (art. 5º, XVII, da LGPD). Assim como ocorre na elaboração do LIA, as hipóteses de utilização e o modelo do Relatório de Impacto (RIPDP) ainda não foram objeto de regulamentação pela ANPD, mas o tema foi trabalhado em reuniões técnicas que foram realizadas com o objetivo de discutir sua elaboração[1]. Dessa forma, utilizaremos as melhores práticas setoriais e internacionais para propor este protocolo, em especial o Relatório do *Article 29 Data Protection Working Party.*

Ainda que o RIPDP seja mencionado nos arts. 10, § 3º e 38[2] da LGPD, as hipóteses nas quais a ANPD pode solicitar o relatório de impacto ainda são amplas, tendo em vista a ausência de endereçamento na legislação. A legislação brasileira difere, nesse sentido, da europeia, uma vez que o art.

1 ANPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-inscricoes-para-participacao-em-reuniao-tecnica-sobre-relatorio-de-impacto-de-protecao-de-dados-pessoais.

2 Art. 10. (...) § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

35 da GDPR[3] apresenta um rol exemplificativo com atividades que deveriam ser precedidas da realização de relatório de impacto, tendo em vista que esse pode ser um instrumento de mitigação de riscos.

Enquanto a ANPD não determina a metodologia de elaboração de RIPDP e as hipóteses de elaboração obrigatória, sugere-se que a metodologia de elaboração do relatório seja aquela associada à perspectiva de risco, nos termos da orientação do Relatório do *Article 29 Data Protection Working Party*. O relatório deve ser preenchido sempre que atividades de tratamento de dados pessoais puderem oferecer alto risco aos direitos fundamentais e liberdades dos titulares.

Nesse último caso, podem ser utilizados como parâmetros de atividades de risco as seguintes hipóteses: i) controle sistemático dos titulares de dados ou *scoring*; ii) realização de decisão automatizada com efeitos jurídicos; iii) *profiling*; iv) processamento de dados pessoais em larga escala tendo em vista, número de titulares envolvidos, volume de dados, duração da atividade e dimensão geográfica da atividade de tratamento; v) realização de correspondências ou combinação de dados diferentes – enriquecimento de bases de dados; vi) tratamento envolvendo dados de pessoas vulneráveis (crianças, idosos ou pessoas com necessidades especiais); vii) uso ou aplicação inovadoras de soluções técnicas ou organizacionais; e viii) tratamentos de dados que possam impedir ou dificultar que titulares de dados exercitem seus direitos ou usem um serviço/contrato.

Ademais, na elaboração de um Relatório de Impacto sugere-se passar pelas seguintes etapas[4]:

3 Art. 32. (1) Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. (2) Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado. (3) A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.o 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala.

4 Adaptação do esquema apresentado pelo Relatório do Article 29 Data Protection Working Party, fl 19.

Informações do Relatório de Impacto à Proteção de Dados Pessoais	
Descrição da atividade e dos dados pessoais	Finalidade do tratamento de dados.
	Quem são os titulares dos dados?
	Qual a relação do controlador com o titular?
	Quais dados são utilizados no tratamento?
	São tratados dados sensíveis?
	O titular possui informações sobre o tratamento de dados?
	Os dados pessoais são compartilhados com terceiros?
	Os dados foram coletados diretamente dos titulares?
	O tratamento de dados é realizado com base em bases enriquecidas?
	Os titulares possuem acesso ao relatório de dados tratados?
	Os dados são tratados por meio de decisões automatizadas?
	O tratamento de dados pode levar a tratamento discriminatório?

Informações do Relatório de Impacto à Proteção de Dados Pessoais	
Ricos e mitigação	Existem riscos que podem afetar a qualidade ou confidencialidade dos dados? Se sim, quais?
	Identificar a fonte do risco.
	Quais são os eventos potencialmente lesivos?
	Existem controles, salvaguardas ou planos de ação capazes de mitigar os riscos?
	Qual a avaliação da gravidade (impacto) e probabilidade (de ocorrência) do risco?
Avaliação DPO	Avaliação de proporcionalidade e necessidade.
	Avaliação sobre existência de atendimento aos direitos do titular.
	Avaliação sobre a estratégia de mitigação de riscos proposta.

VIII - PROTOCOLO PARA SEGURANÇA DA INFORMAÇÃO

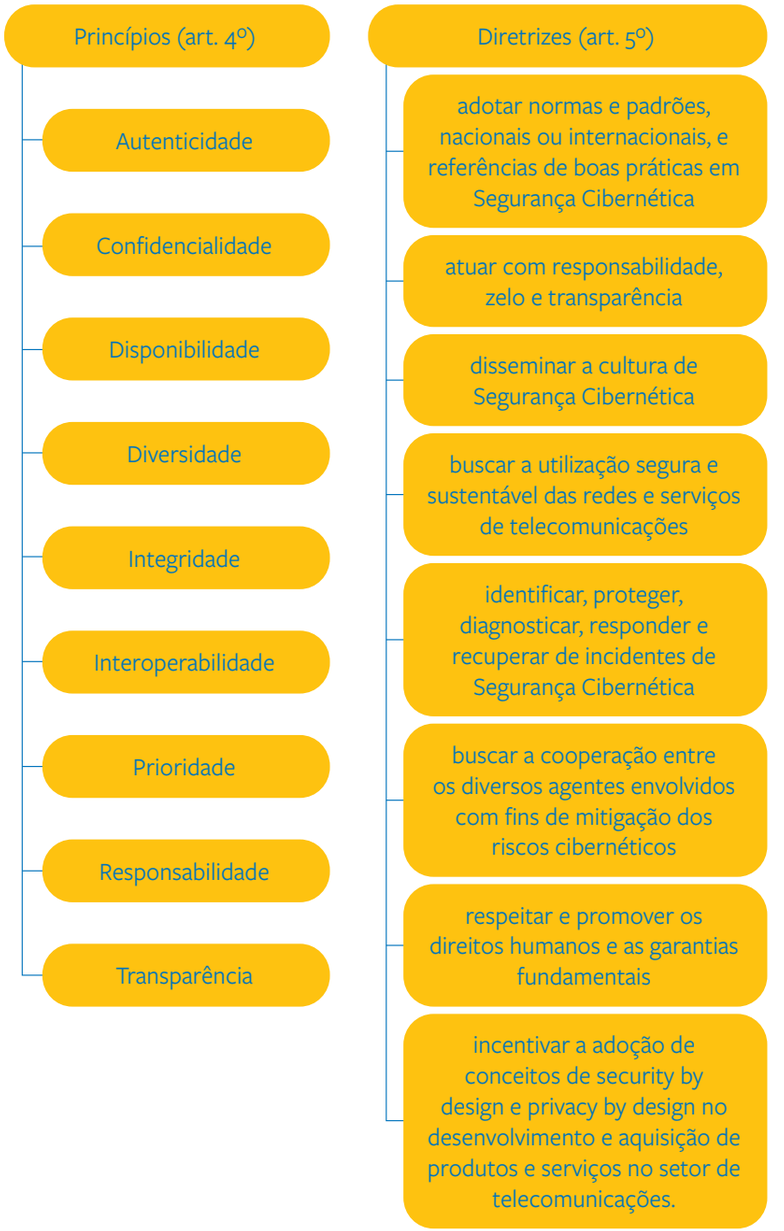
VIII.1. Introdução

O Protocolo para Segurança da Informação pauta-se nos princípios da segurança (art. 6, VII, LGPD) e da prevenção (art. 6º, VIII, LGPD), que estabelecem a obrigação de que os dados pessoais sejam protegidos por meio de medidas técnicas e administrativas, bem como a de que é necessário prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. O princípio da segurança da informação é reforçado por meio de obrigações específicas previstas no art. 46 da LGPD.

Adicionalmente, caso as medidas adotadas não sejam suficientes e um incidente de segurança ocorra, a Lei estabelece a obrigação de notificação do incidente por parte dos controladores dos dados. Para tanto, os agentes devem adotar medidas para identificar se dados pessoais foram afetados e se o incidente pode acarretar risco ou dano relevante aos titulares dos dados pessoais (art. 48, LGPD[1]). Nesse sentido, este protocolo baseia-se em três fases relacionadas à segurança da informação:

1 Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Importa notar que, conforme mencionado no item 5 da Parte I, tendo em vista a quantidade de dados pessoais tratada no setor de telecomunicações, a Anatel vem adotando medidas para garantir a segurança dos usuários mesmo antes da entrada em vigor da LGPD. Após a aprovação da lei, foi redigido o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (Resolução nº 740/2020 da Anatel), que estabeleceu princípios e diretrizes para segurança nas redes e serviços de telecomunicações, que está sendo implementada e discutida pelas prestadoras. São eles:



Nesse sentido, o art. 14 da Resolução nº 740/2020 da Anatel determina

que a Política de Segurança Cibernética deve adotar os princípios e requisitos acima expostos e cumprir com requisitos procedimentais (art. 13) como estabelecer estrutura interna responsável pela política (III); ser aprovada pelo conselho de administração ou equivalente da empresa (inciso V), ser periodicamente atualizada e revisada (inciso VI) e estar disponível à Anatel sempre que necessário (inciso VII).

Além disso, a política deve ser publicizada, por meio de um extrato em sua página com informações não sensíveis, e contemplar, pelo menos (art. 14), aspectos como: (i) plano de ação com medidas para a conscientização e educação de seus usuários sobre aspectos de Segurança Cibernética (inciso IV); (ii) procedimentos relativos ao armazenamento seguro dos dados de seus usuários, nos termos da legislação e regulamentação (inciso V); (iii) procedimentos e controles adotados para a identificação e a análise das vulnerabilidades, das ameaças e dos riscos associados à Segurança Cibernética, às Infraestruturas Críticas de Telecomunicações e à continuidade dos serviços de telecomunicações (inciso VI); (iv) o plano de resposta a incidentes, definindo ações, recursos e responsabilidades (inciso XI); e (v) procedimentos relativos ao compartilhamento de informações sobre incidentes relevantes e outras informações relativas à Segurança Cibernética (inciso (XII), dentre outros.

VIII.2. Segurança da informação: aspectos preventivos

Para que sejam adotados os aspectos preventivos do protocolo de segurança, 3 (três níveis) de requisitos devem ser adotados. Assim, foram estabelecidos 3 (três) níveis de prioridade para implementação dos requisitos de segurança: i) **requisitos mínimos**; ii) **requisitos prioritários** – que, caso não tenham sido implementados, devem ser iniciados imediatamente ou podem estar em fase de implementação; iii) **requisitos avançados** – devem ser implementados assim que os requisitos prioritários estiverem cumpridos.[2]

2 Divisão semelhante foi adotada no Código de Boas Práticas editado pela CNSAÚDE. Disponível em: http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/ Acesso em 30/07/2021.

REQUISITOS DE SEGURANÇA MÍNIMOS	
Políticas e Conscientização	Criar, revisar e comunicar diretrizes considerando melhores práticas para assegurar a proteção e privacidade dos dados pessoais.
Gestão de Identidades e Acessos	Fornecer acessos somente as pessoas autorizadas e revogá-los quando não forem mais necessários ou a pessoa não trabalhar mais na empresa ou mudar de função. Proteger os *logins* de acesso evitando a exposição desses acessos a pessoas não autorizadas. Adotar um segundo fator de autenticação sempre que possível.
Gestão de Backups	Garantir que os dados relevantes para o negócio tenham uma cópia de segurança, devidamente protegida contra acessos não autorizados.
Gestão de Ativos	Inventariar os ativos que tratam dados pessoais e garantir os requisitos mínimos de segurança.
Gestão de Segurança *Endpoint*	Garantir que todos os ativos que tratam dados pessoais tenham uma solução de *antimalware* e *personal firewall* instalada e atualizada periodicamente.

REQUISITOS DE SEGURANÇA PRIORITÁRIOS	
Monitoramento e Gestão de Incidentes	Monitorar o comportamento dos acessos e da segurança dos ativos envolvidos no tratamento dos dados. Esteja preparado para identificar comportamentos e/ou acessos não autorizados.
Gestão de Fornecedores	Avaliar se o fornecedor contratado possui cláusulas contratuais de segurança e privacidade quanto ao tratamento de dados pessoais e adequar os contratos caso elas não existam.
***Log* de sistemas críticos**	Avaliar e garantir que sejam registradas as atividades de tratamentos dos dados: data, horário, duração, identidade do funcionário/responsável pelo acesso e a ação executada/processada.

REQUISITOS DE SEGURANÇA PRIORITÁRIOS	
Controle para Vazamento de Informações	Prevenir o vazamento dos dados pessoais em todo o seu ciclo de tratamento.
Segurança Física	Garantir a segurança do acesso físico às informações tratadas em mídias eletrônicas, papel e sistemas.
Gestão de Vulnerabilidade / *Pentest*	Avaliação a execução de testes de segurança nos sistemas que tratam dados pessoais, priorizando os sistemas expostos na Internet.
Transferência de Dados	Garantir a segurança na comunicação durante os processos de transferências de dados.
Desenvolvimento Seguro	Avaliar se o produto ou sistema estão integrados na esteira atual que contempla análise e implementação de requisitos de segurança para o desenvolvimento seguro.

REQUISITOS DE SEGURANÇA AVANÇADOS	
Arquitetura de Segurança	Identificar e analisar melhorias para a proteção dos dados pessoais envolvendo a arquitetura de tecnologias que suportam os produtos/sistemas, incluindo *Cloud*.
Exclusão de Dados Tratados	Excluir dados pessoais quando solicitado pelo titular ou quando o tratamento chegar ao final
Mascaramento de Dados	Avaliar o uso de mascaramento de dados quando aplicável.
Pseudonimização	Avaliar o uso de pseudonimização quando aplicável.
Mapeamento da localização dos dados	Mapear a localização dos dados pessoais tratados e realizar inventário de ativos que tratam dados pessoais
Criptografia	Avaliar a utilização de recursos de criptografia de dados pessoais quando necessária.

Ressalta-se que cada empresa possui seu próprio ecossistema de segurança da informação, de modo que as soluções e diretrizes devem ser definidas de acordo com as necessidades particulares de cada uma, sendo de responsabilidade das prestadoras a realização desta avaliação. Nesse sentido, os requisitos acima expostos devem servir apenas como orientação para priorização de algumas medidas que consideramos estratégicas.

VIII.3. Segurança da informação: identificação de incidente de segurança e análise de risco

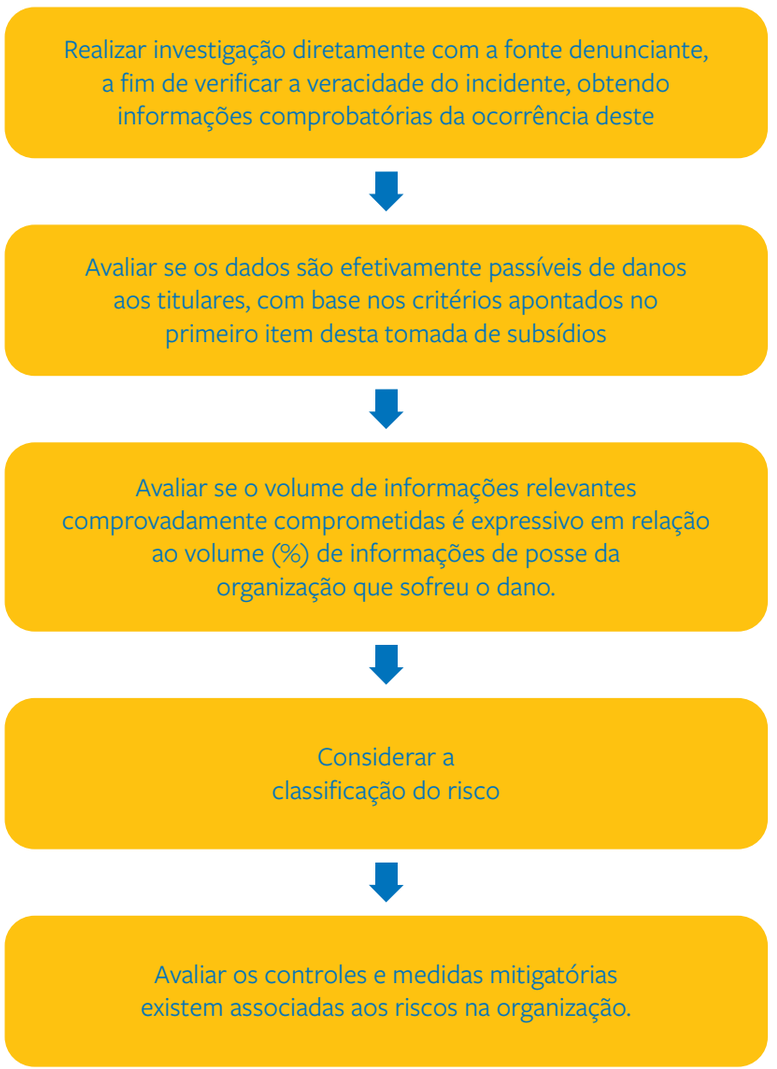
O estudo sobre as melhores práticas para identificação de incidente de segurança e análise de risco foi uma das primeiras iniciativas tomadas pela ANPD quando de sua criação. Foi realizada tomada de subsídios sobre "Incidentes de Segurança nos termos do art. 48 da LGPD", proposta pela Nota Técnica nº 3/2021/CGN/ANPD. Esse passo é de suma importância, tendo em vista que nem todo incidente de segurança afeta dados pessoais, por isso é necessária a identificação de risco representado ou danos que o incidente pode ter causado para os titulares.

A grande dúvida suscitada pelo formulário da tomada de subsídios permeia a dificuldade de criar critérios objetivos para classificação de risco e dano relevante em caso de um incidente de segurança[3]. Assim, diante da ausência de definição de critérios por parte da autoridade, sugere-se a adoção dos critérios propostos pela Conexis em sua contribuição para a consulta pública da ANPD.

Nos termos da contribuição, um incidente de segurança pode acarretar **risco ou dano relevante** ao titular quando houver vulnerabilidades ou *bug* que caracterizem ameaças e sejam explorados ocasionando acessos não autorizados ou situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais. Tais situações podem ser identificadas, por exemplo, em caso de vazamento de: i) dado sensível não público até a data da ocorrência do incidente para ambiente externo ou; ii) dado pessoal identificável não público até a data da ocorrência do incidente para ambiente externo, passível de perda financeira ao titular ou danos não materiais identificáveis.

3 Nos termos expostos nas orientações para comunicação de incidentes de segurança, a ANPD afirma que: "Critérios mais objetivos serão objeto de futura regulamentação e não poderão ser aqui exigidos sob pena de se inovar na LGPD. De toda forma, pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados".

Para **avaliação de risco ou de dano relevante**, sugere-se adotar métricas e parâmetros para a realidade brasileira. Com o objetivo de verificar a criticidade de um incidente, o Controlador deverá considerar uma combinação da gravidade do impacto potencial (I) sobre os direitos e liberdades dos indivíduos e a probabilidade da sua ocorrência (P). Assim, temos que: [criticidade do incidente = P x I]. Nessa avaliação, os seguintes passos devem ser realizados:



Ademais, além de se avaliar a natureza, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis, é necessário verificar os seguintes aspectos:

Volumetria	Tipologia	Exposição
Indica a quantidade de registros vulnerados no incidente de segurança envolvendo dados pessoais. Quanto maior o número de registros e titulares impactados, mais crítico será o evento.	Indica a categoria de dado pessoal vulnerado no evento, de acordo com a definição estabelecida pela própria LGPD (dados pessoais e pessoais sensíveis).	Identifica o ambiente no qual o evento em questão foi descoberto ou acabou sendo exposto. A Exposição poderá ser interna, externa e pública, sendo esta última a que indica maior criticidade para o evento, levando em consideração a eventual disseminação de dados pessoais, sobretudo na internet.

Natureza, sensibilidade e volume de dados pessoais:

Perda de integralidade de dados Indisponibilidade de dados

Veracidade do incidente

Facilidade da identificação dos titulares

Dados anonimizados e/ou criptografados Titulares relacionados às chaves de criptografia dos dados violados Dados relacionados às credenciais de autenticação (matrícula, por exemplo) das partes interessadas

Nível de atualização e validade dos dados

Severidade das consequências aos titulares

Características especiais dos titulares

Características do controlador

Número de titulares afetados

Grau de exposição de dados vulnerados (ambiente interno, externo e público)

Medidas técnicas, organizacionais e administrativas adotadas para mitigar o impacto sobre os titulares

Aspectos relacionados à violação de segurança para acesso aos dados (intencional, não intencional ataque cibernético)

Se o responsável pelo dado objeto do incidente auferiu, direta ou indiretamente, vantagem com o ocorrido

Se o ambiento afetado pelos incidentes está relacionado ao país de operação de negócio do controlador/operador

VIII.4. Segurança da informação: comunicação de incidente de segurança

Em relação a esse aspecto a Conexis também apresentou sua contribuição no bojo da Tomada de Subsídios 02/2021, sendo necessário ressaltar que a autoridade deve buscar uniformidade para que não tenha uma miríade de prazos entre setores e hipóteses. Nesse sentido, a fim de evitar prejuízos ou prazos inviáveis para determinados setores e hipóteses de aplicação, sugere-se que o prazo adotado seja maior do que o inicialmente apresentado pela autoridade brasileira e também maior do que o prazo europeu[4].

Isso porque, considerando a complexidade técnica e a necessidade de uma investigação e análise da equipe de Segurança da Informação (interna ou terceirizada) para apurar os detalhes e vulnerabilidades do incidente, o Controlador poderá ter até 30 dias, a contar da ciência e comprovação do incidente, para avaliar, concluir e informar a ANPD se o evento em concreto poderá acarretar risco ou danos aos Titulares.

As instruções dadas pela autoridade[5] recomendam a comunicação das seguintes informações em caso de incidente de segurança:

Identificação e dados de contato de:
• Entidade ou pessoa responsável pelo tratamento. • Encarregado de dados ou outra pessoa de contato. • Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

4 Com a vigência do GDPR, somente 18% das organizações europeias acreditavam estar preparadas para cumprir com o prazo de 72 (setenta e duas) horas para notificação de um incidente de segurança. Disponível em: https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/organizations-struggle-comply-gdpr.aspx

5 Para mais informações acessar: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso em: 31/07/2021.

Informações sobre o incidente de segurança com dados pessoais
• Data e hora da detecção. • Data e hora do incidente e sua duração. • Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros. • Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados • Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento. • Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados. • Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD. • Resumo das medidas implementadas até o momento para controlar os possíveis danos. • Possíveis problemas de natureza transfronteiriça. • Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

VIII.5. Segurança da informação: plano de ação após a comunicação de incidente de segurança

Após a comunicação de um incidente de segurança, recomenda-se que seja elaborado um plano de ação para corrigir possíveis falhas e evitar que novos incidentes venham a ocorrer. Nesse sentido, sugere-se que as seguintes medidas administrativas e técnicas sejam adotadas:

Medidas administrativas no âmbito da governança
• Políticas corporativas; • Treinamentos, capacitação de colaboradores, comunicação e aculturamento; • Contratos: inclusão de anexos de SI e LGPD; revisão; cláusulas; DPA; • Comitês de Crise e Executivo; • Políticas de privacidade, de *cookies*, termos de uso para sites e aplicativos; • Controles, entre outros.

Medidas técnicas adotadas no âmbito da Tecnologia da Informação
• Análise e seleção de fornecedores por meio de processo de *Vendor Assessment*; • Utilização de ferramenta de *Data Loss Prevention* (DLP); • Simulados de incidentes de segurança, a fim de verificar a aderência ao nosso Plano de Gerenciamento de Incidentes; • Realização de testes de invasão dentro do processo de desenvolvimento com o objetivo de que as aplicações sejam publicadas com a menor quantidade possível de vulnerabilidades; • Mapeamento das superfícies de ataque interna e externa visando identificar ativos não documentados e vetores de ataques ao ambiente; • Testes de invasão nos ativos críticos legados e/ou que não estejam integrados à esteira *DevSecOps;* • Monitoramento contínuo dos sistemas por meio de testes recorrentes nestes sistemas/aplicações em ambiente produtivo; • Realização de testes visando a fortalecer os mecanismos de monitoramento, detecção e resposta frente a ameaças cibernéticas; • Processo de identificação de vulnerabilidades por meio de ferramentas automatizadas; • Governar o processo de aplicação de patches por meio do monitoramento de patches de segurança lançados e avaliação do ambiente para aplicação destes patches de acordo com suas criticidades e impactos para o negócio.

CONCLUSÃO

A LGPD instituiu um regime geral de proteção de dados no Brasil, modernizando a regulação do fluxo dos dados pessoais, ao ampliar a transparência, o controle do titular e a segurança da informação no tratamento de dados. O novo paradigma foi reforçado com a recente inclusão da proteção de dados pessoais no rol de direitos fundamentais da Constituição Federal por meio da Emenda Constitucional nº 115, que estabeleceu também a competência exclusiva da União para regular a proteção de dados.

O Código de Boas Práticas de Proteção de Dados para o setor de Telecomunicações estabelece padrões para o tratamento de dados pessoais, facilitando a correta aplicação da LGPD e auxiliando a interpretação sistemática com outras normas relacionadas a esse tema.

O presente texto é fruto de grupo de trabalho, coordenado pela Conexis, do qual participaram especialistas em proteção de dados e representantes do setor de telecomunicações, unindo expertise técnica com o conhecimento prático do cotidiano empresarial.

Seu ponto de partida é de que o cumprimento das normas de proteção de dados constitui, para além de uma obrigação legal, um importante passo para a construção da confiança do cidadão no setor de telecomunicações e em cada uma das empresas que o compõe. Tal confiança é especialmente relevante para o setor de telecomunicações, que provê para a sociedade uma infraestrutura essencial para todos os serviços de comunicação e informação.

Na economia movida a dados, a implementação de medidas para proteção da privacidade representa, por um lado, a mitigação de riscos, como o de incidentes de segurança, regulatórios e judiciais e, por outro lado, a

obtenção de retornos financeiros e reputacionais a partir da confiança gerada pela adoção de boas práticas no tratamento de dados. Essas medidas estão cada vez mais associadas a ganhos de reputação, imagem, estimulando a expansão da marca e dos resultados financeiros.[1]

Como evidencia o *Data Privacy Benchmark Study 2020* publicado pela Cisco, o investimento em privacidade pode trazer um retorno financeiro positivo para as organizações, sendo possível traçar uma correlação entre a implementação da *accountability* na organização e a redução do número de incidentes de segurança e diminuição nos atrasos nas vendas.[2] O estudo também demonstra que mais de 40% das organizações internacionais percebem o dobro de retorno do que o que foi gasto para implementação de programas de privacidade e proteção de dados pessoais.

Conforme explorado no relatório publicado pelo CEDIS/IDP e CIPL[3], há inúmeros benefícios que as empresas que implementam um programa de governança de privacidade podem obter. Entre esses benefícios estão a criação de uma cultura de privacidade dentro da organização; a fidelização de clientes; o surgimento de novas oportunidades de negócios; o aumento da confiança de todos que se relacionam com a organização, como a imprensa, investidores, reguladores, consumidores e funcionários; a manutenção das vantagens competitivas de tal modo que a organização se diferencie das demais; e a diminuição de riscos das ações sancionatórias ou a redução do impacto financeiro das sanções, a partir da demonstração dos seus esforços de adequação.[4]

Para tanto, é fundamental que o cumprimento das regras de proteção de dados não seja visto como mero obstáculo pontual a ser superado pelas empresas, mas sim possa ser encarado a partir uma postura proativa de mudança da cultura de privacidade dentro da organização, conduzindo a uma verdadeira transformação dos processos internos, desde a concepção dos serviços até as práticas comerciais. O presente Código pretende auxiliar nessa transformação e pode se constituir em uma importante ferramenta para as empresas, para os consumidores e para todos aqueles que buscam uma interpretação técnica e prática da LGPD.

1 IBM. *Why data privacy is much more than compliance.* Em: https://www.ibm.com/security/digital-assets/data-privacy-matters/.

2 https://www.cisco.com/c/en_uk/products/security/security-reports/data-privacy-report-2020.html

3 CIPL e CEDIS/IDP. *Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD).* Acessível em: https://www.idp.edu.br/projeto-lgpd/.

4 Idem, p. 5.

REFERÊNCIAS

11
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

23
https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

24
https://lapin.org.br/2021/04/09/cartilha-controlador-ou-operador-quem-sou-eu

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf

26
https://lapin.org.br/2021/04/09/cartilha-controlador-ou-operador-quem-sou-eu/

31
https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados

39
https://www.gov.br/anatel/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais

41
https://www.gov.br/anatel/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais/aviso-de-privacidade

59
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en

73
https://www.abrtelecom.com.br/a-abr-telecom

74
https://www.abrtelecom.com.br/entidades/portabilidade-numerica

https://www.gov.br/anatel/pt-br/consumidor/destaques/cadastro-nacional-de-nao-me-perturbe-para-servicos-de-telecomunicacoes-esta-disponivel-a-partir-de-16-7

https://www.naomeperturbe.com.br/politica.html

75
https://front.abrtelecom.com.br/public/arquivos/1611078934518.pdf

https://front.abrtelecom.com.br/public/arquivos/1611079055547.pdf

79
https://conexis.org.br/operadoras-de-telecom-aderem-ao-cadastro-positivo/

https://conexis.org.br/operadoras-de-telecomunicacoes-passam-a-integrar-o-cadastro-positivo

83
http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

88
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

95
https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/model-clause-agreement-builder

https://privacy.org.nz/assets/DOCUMENTS/IPP12-guidance/2.-IPP-12-Model-Clauses-Guidance-Document-web-Oct.pdf

98
http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude

https://www.aepd.es/sites/default/files/2020-01/ct-uch-cat.pdf

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr

https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf

https://wpcdn.idp.edu.br/idpsiteportal/2020/08/pt_cipl-idp_whitepaper_anpd-1.pdf

https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

100
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/reframing_data_transparency.pdf

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

101
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

106
www.nãomeperturbe.com.br

109
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf

110
https://iapp.org/media/pdf/resource_center/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf

https://iapp.org/resources/article/guidance-on-the-use-of-legitimate-interests-under-the-eu-general-data-protection-regulation

113
https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-inscricoes-para-participacao-em-reuniao-tecnica-sobre-relatorio-de-impacto-de-protecao-de-dados-pessoais

120
http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude

127
https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/organizations-struggle-comply-gdpr.aspx

https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso em: 31/07/2021

132
https://www.ibm.com/security/digital-assets/data-privacy-matters

https://www.cisco.com/c/en_uk/products/security/security-reports/data-privacy-report-2020.html

https://www.idp.edu.br/projeto-lgpd