PROTEÇÃO DE DADOS

GUIA DE CONFORMIDADE LEGAL PARA A SOCIEDADE CIVIL

RedeFOLHA
EMPREENDEDORES SOCIOAMBIENTAIS

SZAZI BECHARA STORTO REICHER FIGUEIREDO LOPES ADVOGADOS

PLATAFORMA MROSC

Financiado pela União Europeia

FICHA TÉCNICA

Live Lgpd

Iniciativa: Projeto “Fortalecimento e Regionalização da Plataforma por um Novo Marco Regulatório das Organizações da Sociedade Civil” (CSO-LA/2018/399-177)

Coexecução: Cáritas Brasileira e Elo

Financiamento: União Europeia

Consultoria Jurídica: Szazi, Bechara, Storto, Reicher e Figueiredo Lopes Advogados

Equipe responsável:

Laís de Figueirêdo Lopes

Paula Raccanello Storto

Maraísa Rosa Cezarino

Rebeca de Oliveira Souza

Thais Schiavon

Natalia Toito Galli

Vinícius Fidelis

Projeto Gráfico: Mateus Leal

Supervisão Técnica: Laís de Figueirêdo Lopes, Paula Raccanello Storto e Maraísa Rosa Cezarino

Revisão: Stella Reicher

RedeFOLHA
EMPREENDEDORES SOCIOAMBIENTAIS

SZAZI BECHARA STORTO REICHER FIGUEIREDO LOPES ADVOGADOS

PLATAFORMA MROSC

Financiado pela União Europeia

SUMÁRIO EXECUTIVO

APRESENTAÇÃO

Construímos esse Guia com o intuito de desmistificar, desconcentrar o conhecimento e ajudar a promover a mudança cultural de proteção de dados requerida pela Lei n° 13.709/2018 - Lei Geral de Proteção de Dados, a "LGPD".

O público-alvo deste documento são as Organizações da Sociedade Civil e os Negócios de Impacto, que figuram entre os destinatários da LGPD, trazendo uma camada regulatória que se sobrepõe às leis específicas que regulamentam as suas atividades como pessoas jurídicas.

Inicialmente, foi possível perceber uma grande incerteza em torno de como proceder com a adequação a essa lei, totalmente nova, que regula o uso e a transmissão de dados pessoais, matéria prima de praticamente todas as atividades de interação com o público.

A incerteza surge do desconhecido e socializar o conhecimento sobre proteção de dados ajuda a gerar mais segurança e engajamento, além de ser ferramenta para promover a aplicação mais adequada da lei, criada para proteger os cidadãos brasileiros das consequências do uso abusivo dos seus dados pessoais.

Nesse sentido, é importante destacar que o direito à proteção de dados foi reconhecido como direito fundamental por meio da PEC 17/2019. Após a sua aprovação, pelo Senado, no dia 20 de outubro de 2021, a PEC seguiu para promulgação em sessão do Congresso Nacional.

Em 2020, o Supremo Tribunal Federal já tinha reconhecido a proteção de dados como direito fundamental na sua jurisprudência, no julgamento da ADI nº 6.387, quando consolidou o entendimento de que a proteção de dados era uma derivação natural do direito fundamental à inviolabilidade, da intimidade, da vida privada, da honra e da imagem das pessoas (prevista no artigo 5º, X, da Constituição).

A afirmação da proteção de dados como direito fundamental fortalece todo o arcabouço de direitos previstos na LGPD. Isso quer dizer que, mais do que nunca, só é possível tratar dados pessoais para uma atividade quando existir o consentimento específico dos titulares de dados ou quando esse tratamento estiver encaixado em uma das hipóteses de tratamento que a LGPD expõe nos artigos 7º para dados pessoais e no 11º para dados sensíveis.

No momento em que grandes empresas se valem de recursos de inteligência artificial, para processar e monetizar, em larga escala, os dados pessoais dos cidadãos com o objetivo de prever os seus comportamentos e fornecer produtos, conteúdos e serviços de forma direcionada, a positivação da Proteção de Dados como direito fundamental aumenta a responsabilidade pela construção de uma agenda de atuação pautada pela preocupação coletiva de proteção deste direito.

É importante lembrar que, além das chamadas Big Techs, cujo impacto sobre as democracias modernas tem sido amplamente criticado entre especialistas, o Estado muitas vezes apresenta iniciativas questionáveis relacionadas, principalmente, a projetos que envolvem o tratamento de dados para a finalidade de eficiência de mecanismos de segurança pública.

Nesse sentido, pode-se citar as diversas iniciativas que envolvem a ampliação da captação de dados pelo Estado, com o intuito de aumentar o seu poder de vigilância sobre os cidadãos, por exemplo: a criação de Cadastro Básico de Cidadão, via decreto; a tentativa de emplacar uma criticada Estratégia Brasileira de Inteligência Artificial; a elaboração de um anteprojeto de lei sobre o tratamento de dados e segurança pública; e o crescente uso, pelos Estados, de mecanismos de reconhecimento facial como instrumento de segurança pública.

O retrato da problemática envolvendo a ampliação da vigilância estatal foi retratado em pesquisa recentemente produzida pelo Data Privacy Brasil e pelo Instituto LAUT, na qual é possível encontrar uma sistematização daquilo que se vem conceituando como "tecno autoritarismo", ou seja, a ampliação desmedida da captação de dados pelo Estado para a finalidade de controle da população.

Segundo Ingo Wolfgang Sarlet[1], o direito fundamental à proteção de dados havia sido incorporado nas Constituições portuguesa (1978) e espanhola, (1976), mas esses países são uma exceção, já que muitos outros ainda não trazem esse direito expressamente em suas constituições. No âmbito da ONU, o direito à proteção de dados tem sido interpretado como derivação do direito à privacidade, embora eles não se confundam.

O direito à Privacidade é um direito que se exerce pela possibilidade de isolar determinados aspectos do âmbito público, tratando do direito de não ser incomodado, de não ter determinadas partes da sua vida expostas ao público. Por outro lado, o direito à proteção de dados é um direito positivo, da pessoa que é titular de dados, de exercer controle sobre o fluxo dos dados pessoais que dizem sobre ela. Isso é, significa o direito de saber e conseguir exercer um controle mínimo sobre o fluxo tais dados, inclusive, demandando que ele seja interrompido se for o caso.

Em 1981, a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares, conhecida como "Convenção de Estrasburgo", reconheceu o direito à proteção de dados como direito fundamental, quando realizado por meios totalmente automatizados. Essa convenção foi um passo importante para a consolidação do debate sobre proteção de dados pessoais que, mais tarde, desembocou na GDPR (*General Data Protection Regulation),* promulgada em 2016. A regulação europeia de proteção de dados influenciou, em larga medida, a construção das disposições da LGPD.

Nesse sentido, a aprovação de uma lei robusta, capaz de efetivar a proteção dos titulares de dados, foi objeto de grande mobilização das organizações do terceiro setor e do setor privado entre 2010 e 2018 quando a LGPD foi aprovada. Considerando o escopo de atuação e os interlocutores das OSCs e dos negócios de impacto, a quem se dirige este Guia, efetivar o direito à proteção de dados significa um compromisso de cuidado e respeito com as populações de grupos socialmente vulneráveis que normalmente são o público atingido pelos seus projetos.

Assim, o estabelecimento de uma nova cultura de tratamento de dados, pressuposto para a efetivação da LGPD, parte da compreensão de quem é o foco de proteção da lei: todos nós, titulares de dados. A LGPD é construída sobre a premissa de que os dados, para efeito de proteção jurídica, devem ser compreendidos como uma projeção da personalidade das pessoas a quem eles pertencem. Desse modo, ao proteger os dados das pessoas, a LGPD protege as próprias pessoas e o livre desenvolvimento

1 http://genjuridico.com.br/2021/10/08/protecao-dos-dados-pessoais-privacidade/

da sua personalidade, uma vez que o processamento massivo de dados tem permitido uma série de decisões sobre elas sem que necessariamente os cidadãos sejam informados sobre como isso ocorre.

Neste documento, encontram-se conceitos básicos e relevantes sobre a proteção de dados, dicas de como se adequar à LGPD e, também, uma discussão sobre as possibilidades de disputa interpretativa da lei, que abrem espaço para pensar numa calibragem da sua aplicação às possibilidades e recursos disponíveis aos agentes de pequeno porte.

Este material foi elaborado a partir de uma solicitação da Plataforma por um Novo Marco Regulatório das Organizações da Sociedade Civil para a suas consultoras jurídicas, Laís de Figueirêdo Lopes e Paula Raccanello Storto, sócias de SBSA Advogados, entendendo ser este um tema relevante para a atuação das OSC no Brasil e de interesse da Pltaaforma, que pretende difundir informação qualificada para suas mais de 2.000 signatárias com sobre a nova Lei que trata da regulação de dados pessoais.

Os questionamentos e dúvidas que este material procura responder foram levantados a partir de solicitações da Plataforma e suas OSC signatárias em atividades locais, regionais e nacionais que tem realziado nos útlimos anos. Tem origem também em um workshop realizado entre a Rede Folha de Empreendedores Socioambientais e SBSA Advogados - que há mais de 10 anos é pareiro do Prêmio - que contou com a presença de finalistas e vencedores do Prêmio Empreendedor Social. Os mais de cem líderes de organizações e negócios sociais receberam em primeira mão parte deste conteúdo, agora ampliado e destinado a todo o ecossistema de impacto social.

Estes processos participativos permitiram a clara identificação da sinergia existente entre o universo das OSC e dos Negócios de Impacto no que diz respeito à pauta de regulação de dados pessoais. Foi assim que com esta parceria de peso, nasceu a ideia de unificar os conteúdos neste único Guia, que esperamos possa inspirar o processo de adequação da cultura organizacional de OSCs e dos negócios de impacto à LGPD, apoiando a mudança de comportamento a nova lei traz como um convite ao cuidado e garantia do direito fundamental à proteção de dados pessoais no nosso país.

Boa Leitura!

Plataforma por um novo Marco Regulatório das Organizações da Sociedade Civil

SBSA Advogados

Prêmio Empreendedor Social da Folha de S.Paulo

01

ORGANIZAÇÕES DA SOCIEDADE CIVIL (OSC) E NEGÓCIOS DE IMPACTO (NI)

A LGPD, Lei n° 13.709/2018, em seu artigo 3°, dispõe que devem observar suas disposições para a realização do tratamento de dados as pessoas naturais ou jurídicas de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que (i) a operação tenha sido realizada em território nacional; (ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Dessa forma, a LGPD é aplicável ao Poder Público, às empresas, às Organizações da Sociedade Civil (OSC) e aos Negócios de Impacto. Contudo, como o próprio título deste Guia já anuncia, esse material tem um escopo mais direcionado da aplicação da LGPD a estes últimos: Organizações da Sociedade Civil e Negócios de Impacto.

SUMÁRIO

As OSCs, de acordo com a Lei nº 13.019/2014, conhecida como Marco Regulatório das Organizações da Sociedade Civil (MROSC), são entidades de direito privado sem fins lucrativos – como associações e fundações - que revertem a totalidade de eventuais resultados, sobras e excedentes patrimoniais auferidos no exercício de suas atividades, para a consecução de seu respectivo objetivo social que deve observar a promoção de atividades e finalidades de relevância pública e social (art. 2º, inciso I, alínea "a" e art. 33, inciso I), além das sociedades cooperativas e das organizações religiosas que se dediquem a atividades ou a projetos de interesse público e de cunho social distintas das destinadas a fins exclusivamente religiosos (art. 2º, inciso I, alíneas "b" e "c").

As pessoas jurídicas "sem fins lucrativos" não são impedidas de desenvolver atividade econômica ou de obter resultado financeiro positivo (superávit) mas, ao obtê-lo, não devem distribuí-lo entre os seus associados, conselheiros, diretores, empregados, doadores ou quaisquer terceiros, como numa empresa, mas reaplicá-lo nas suas finalidades de relevância pública. Segundo o MROSC, as OSCs devem manter a escrituração de acordo com os princípios fundamentais de contabilidade e com as Normas Brasileiras de Contabilidade.

Os negócios de impacto, por sua vez, são definidos pelo Decreto Federal nº 9.977/2019, que criou a Estratégia Nacional de Investimento e Negócios de Impacto (ENIMPACTO). A definição não cria um tipo jurídico societário novo, mas admite o enquadramento de diferentes tipos jurídicos com ou sem finalidade lucrativa, a partir do impacto socioambiental e resultado financeiro positivo de forma sustentável. Com esta definição também não se qualificou a natureza de pessoas jurídicas no país. Ou seja, não houve qualquer mudança nas regras para abertura ou funcionamento das empresas, associações, fundações e sociedades cooperativas que se enquadrem como um "negócio de impacto" ("NI").

Tanto as OSCs quanto os Negócios de Impacto, a depender da natureza das atividades que desempenham, podem lidar com uma grande quantidade de dados pessoais e dados sensíveis dos beneficiários

Desta forma, dois requisitos são exigidos para que um empreendimento se enquadre neste conceito do Decreto: (i) deve se propor a solucionar um problema socioambiental e, ao mesmo tempo, (ii) ter resultado financeiro positivo de forma sustentável – ou seja, a sua atividade deve ser capaz de se "sustentar" sem o necessário apoio de doadores e financiadores. Se a sua organização ou a sua empresa cumpre com os dois requisitos do decreto federal, já pode ser considerada um negócio de impacto.

Atuando com matérias variadas e, em geral, com um olhar para públicos específicos, como a população negra, idosa, pessoas com deficiência, crianças e adolescentes, mulheres, povos e comunidades tradicionais, sendo muitas vezes necessário coletar dados e informações para atuar na promoção os direitos dessas populações e/ou interagir com os beneficiários nos projetos que desenvolvem.

Nessa lógica, selecionamos nos quadros abaixo alguns tipos de atividades e os dados que são normalmente captados no seu desenvolvimento, a fim de ilustrar a aplicação da LGPD:

ATIVIDADES DE GESTÃO:

São as atividades necessárias ao atingimento dos objetivos finais de sua atuação, mas não são o objetivo em si, por exemplo:

- Contratação e gestão de funcionários, estagiários e voluntários;
- Contratação de serviços prestados por pessoas físicas como autônomos ou *freelancers*;
- Monitoramento de impacto dos projetos;
- Gestão dos contratos e instrumentos de parcerias com outras organizações, empresas ou com o Poder Público;
- Captação de recursos.

DADOS NORMALMENTE CAPTADOS:

DADOS PESSOAIS: nome, e-mail, telefone, endereço, cargo atual, nível de escolaridade, experiência prévia de trabalho, informações requisitadas pela CLT, pela Lei de Estágio ou pela Lei do Voluntariado, dados necessários para a concessão de benefícios, situação econômica da pessoa, etc.

DADOS PESSOAIS SENSÍVEIS: dados de saúde, origem ética/racial, orientação sexual, orientação político-filosófica, etc.

ATIVIDADES DE PROJETOS

São as atividades finalísticas que traduzem os objetivos para a qual foram criadas, como:

- Realização de pesquisas sobre o impacto de políticas públicas na região onde atuam;
- Realização de cursos e formações para o público da organização/ negócio;
- Mobilização das pessoas da região de atuação em torno de um tema;
- Oferta de serviços e atendimento de saúde em parceria com o poder público;
- Divulgação de iniciativas e problemas de determinados grupos vulneráveis com os quais a organização/negócio atue.

DADOS NORMALMENTE CAPTADOS

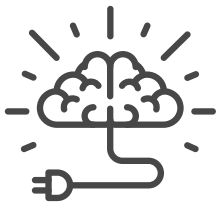
DADOS PESSOAIS: histórico de saúde mental, histórico de violência, histórico de uso de mecanismos de assistência social, participação em organizações, dados referentes à identidade de gênero, raça e etc.

Além de dados cadastrais como nome, e-mail, telefone, endereço, nível de escolaridade, é comum, a depender do tipo de projeto, captar dados sobre a utilização de mecanismos da assistência social, dados sobre situação econômica da pessoa e etc.

DADOS PESSOAIS SENSÍVEIS: dados de saúde, origem ética/racial, histórico de situação de violência / vulnerabilidade, orientação sexual, orientação político-filosófica e etc

ATIVIDADES DE COMUNICAÇÃO	DADOS NORMALMENTE CAPTADOS
Normalmente, nos eventos de aparição pública, há a captação de dados pessoais, notadamente na: • Realização de eventos e *lives;* • Divulgação de materiais produzidos pela organização/negócio; • Divulgação dos projetos implementados pela organização/ negócio.	**DADOS PESSOAIS:** nome, email, telefone e endereço ou organização/negócio. **DADOS PESSOAIS SENSÍVEIS:** raça e orientação político-filosófica

Mas você já parou para pensar se realmente precisa de todos esses dados? Sempre que você estiver diante de um formulário para captação de dados é importante pensar se você precisa mesmo dos dados que estão sendo solicitados. O ideal é que seja evitada a captação de dados desnecessários, sem correspondência com a finalidade que se busca a informação.



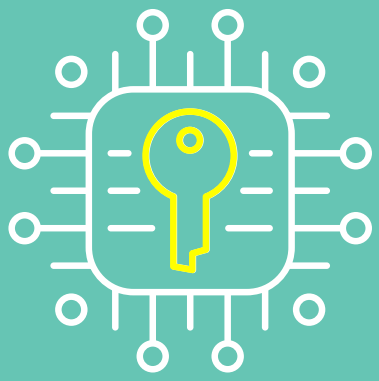
ATENÇÃO!

Em cada uma dessas atividades, é necessário implementar mecanismos para efetivar os princípios e direitos previstos na LGPD, por isso recomendamos:

- Construir uma relação de **transparência** e **confiança** com os seus colaboradores internos e beneficiários dos serviços, encarando a LGPD como uma **oportunidade de revisitar** e aperfeiçoar fluxos, processos e projetos da organização/negócio para melhor atingir seus resultados.
- Estruturar a sua governança para promover a cultura de proteção de dados, garantir os direitos dos titulares e responder **requisições** da Agência Nacional de Proteção de Dados (ANPD), a respeito das informações em seu poder, evitando ser **responsabilizada** em caso de incidentes de proteção de dados, e tendo capacidade de resposta caso venha a ser demandada **administrativamente** ou **judicialmente** pelo descumprimento da lei.

Ou seja, a LGPD também deve ser observada por todas as pessoas jurídicas, incluindo as Organizações da Sociedade Civil e os Negócios de Impacto, como uma oportunidade de melhoria da sua atuação, tanto na perspectiva da proteção e promoção de direitos quanto no olhar da gestão dos seus projetos e atividades.

02



CONHECENDO A **LGPD**

2.1 Histórico da LGPD

Em 2010, o Ministério da Justiça deu início à discussão sobre a regulação da proteção de dados pessoais no Brasil ao promover a primeira consulta pública sobre o Anteprojeto de Lei nacional. Apesar da iniciativa, a temática ganhou novo fôlego e importância em 2013, quando Edward Snowden, ex-funcionário da agência de segurança nacional dos EUA, revelou para o mundo que a agência de espionagem tinha acesso a dados pessoais de milhares de indivíduos por meio servidores grandes empresas da internet como Google e Facebook. Dados divulgados por ele revelavam escutas a então Presidenta Dilma Rousseff e, tamanho escândalo desencadeou na aprovação do Marco Civil da Internet no Brasil.

Em 2014, com a promulgação do Marco Civil da Internet, diversos ativistas dos direitos na internet se uniram para criar organizações que pudessem mobilizar o debate público e criar condições para um uso saudável da rede mundial de computadores. Essa foi a época do surgimento de organizações como a Codin Rights, o InternetLab, o ITSRio, o IPRec, o IRIS-BH entre outras, além de uma atuação mais constante de organizações como o IDEC para a mobilização em torno da promoção dos direitos humanos na internet.

SUMÁRIO

Desde então, junto do Comitê Gestor da Internet (CGI) e do Núcleo de Informação e Coordenação do Ponto BR (Nic.br), os profissionais que trabalhavam com essa pauta se engajaram em amplas campanhas de mobilização da sociedade civil, das autoridades e de empresários em torno da pauta da proteção de dados pessoais, buscando a aprovação de uma lei geral de proteção de dados, para compor o ecossistema de regulação do uso da internet.

Assim, a discussão sobre proteção de dados pessoais já havia atingido um nível muito mais qualificado em 2015, no lançamento do segundo processo de consulta pública. Em razão da experiência adquirida sobre a temática, e nas vésperas de seu afastamento, a Presidenta Dilma Rousseff encaminhou o texto do anteprojeto à Câmara dos Deputados, que a transformou no PL 5276/2016.

De 2016 a 2017, a Comissão Especial realizou 11 audiências públicas e um seminário internacional, proporcionando engajamento dos parlamentares e permitindo a conciliação de posições antagônicas até então, por meio da mobilização promovida principalmente pelas organizações da sociedade civil focadas nas pautas da internet. Enquanto isso, ainda em 2017, o grupo de reformas microeconômicas da Comissão de Assuntos Econômicos do Senado, se manifestou sobre a importância do Brasil instituir sua própria lei de proteção de dados pessoais.

o atraso regulatório que já impedia o ingresso do Brasil na Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE), bem como gerava sérias perdas econômicas e de investimentos ao Brasil

Em 2018, era visível o atraso regulatório do Brasil em relação ao tema e isso já impedia o ingresso do país na Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE). Além disso, esse atraso vinha ocasionando sérias perdas econômicas e de investimentos ao Brasil. Por fim, o escândalo da violação de dados de mais de 50 milhões de usuários para fins políticos e eleitorais pela Cambridge Analytica, foi um acontecimento que gerou um senso de urgência em relação à necessidade da aprovação da LGPD.

Após o incidente, em 24 e 28 de maio, Senado e Câmara, respectivamente, aprovaram requerimentos de urgência para a apreciação dos projetos de lei sobre dados pessoais em tramitação. Mais rápida, a Câmara dos Deputados aprovou por unanimidade o substitutivo apresentado pelo Deputado Orlando Silva que também foi aprovado sem qualquer alteração em seu teor pelo Senado. Por essa razão, foi enviado diretamente à sanção do Presidente Michel Temer.

Em 14 de agosto 2018, Temer sancionou a LGPD, mas com diversos vetos e, o mais importante deles, vetando a criação da Autoridade Nacional de Proteção de Dados (ANPD) justificando a existência de vício de competência: órgão como este não poderia ser criado pelo Legislativo. Apenas nos últimos dias de seu mandato, Temer cumpriu com sua promessa e criou a ANPD por meio da MP 869/2018.

Diante do contexto de criação, das disputas encerradas e dos escândalos de vazamento de dados, fica mais fácil de compreender que a Lei Geral de Proteção de Dados foi criada para devolver às pessoas físicas o controle sobre a sua personalidade[2]. Do ponto de vista jurídico, a personalidade é compreendida pela aptidão para fruição de direitos e aquisição de deveres, sendo reconhecida a todo ser humano, independentemente da consciência ou vontade do indivíduo, como um atributo inseparável da pessoa.

Os direitos da personalidade, portanto, são aqueles que dizem respeito à dignidade e à integridade da pessoa humana, protegendo tudo o que lhe é próprio, como a vida, a liberdade, a privacidade, a imagem, a intimidade, entre outros[3]. Sendo assim, como nos dias de hoje a vida acontece tanto virtualmente quanto no mundo físico, é de se esperar que essa personalidade, bem como os direitos e deveres que dela decorrem, definam-se por sua movimentação e pelos dados compartilhados na internet.

Toda vez que navegamos na internet, ou fazemos cadastros para acessar serviços e produtos diversos, trocamos dados com as empresas que estão do outro lado da nossa tela. A partir das nossas movimentações no mundo *online*, por exemplo, por meio dos cliques, dos *likes*, dos conteúdos que consumimos e dos produtos que compramos, as instituições e empresas conseguem identificar e mapear quais são os nossos gostos, concepções sobre os mais diversos assuntos e prever qual seria nosso próximo passo como consumidor dos mais diversos serviços e conteúdos.

É por isso, que, vez ou outra, recebemos indicações de conteúdos, propagandas e serviços que parecem ter sido feitos sob medida para o que queremos ou necessitamos.

---

2 O código civil brasileiro (Lei n° 10.406/2002) dispõe em seus artigos 1° e 2° sobre a capacidade de direito e de gozo, bem como da personalidade civil da pessoa: "art. 1º Toda pessoa é capaz de direitos e deveres na ordem civil; art. 2º A personalidade civil da pessoa começa do nascimento com vida; mas a lei põe a salvo, desde a concepção, os direitos do nascituro."

3 Conforme preceitua a Constituição Federação de 1988, em seu artigo 5°, caput e incisos X: *"Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."*

Isso quer dizer que os rastros digitais que deixamos têm sido utilizados pelos nossos interlocutores para inferir e embasar nossas decisões, impactando diretamente em nossas vidas e no exercício de nossa cidadania, dentro e fora das redes.

Nesse sentido, a Lei Geral de Proteção de Dados foi criada para regular justamente esse ecossistema de tratamento de dados, conferindo proteção a nós, titulares de dados, de finalidades do uso de nossos dados pessoais que possam gerar prejuízos ao desenvolvimento da nossa personalidade e da integridade de tudo que lhe é próprio, como a privacidade e a liberdade , dentre outros direitos intransponíveis. A LGPD busca devolver o controle da formação dessa personalidade para os titulares de dados, tornando a relação entre eles e os controladores de seus dados mais horizontal e paritária.

2.2 LGPD em si

A Lei nº 13.709/2018, ou a Lei Geral de Proteção de Dados – LGPD , estabelece princípios e diretrizes para o manuseio e tratamento de dados pessoais com o objetivo de proteger os direitos de seus titulares, sendo considerada especialmente importante para conferir aos indivíduos um maior controle sobre o desenvolvimento de sua própria personalidade na atual era da digitalização.

Em linhas gerais, a LGPD determina as regras aplicáveis ao tratamento, armazenamento e compartilhamento de dados pessoais, que são informações que podem tornar uma pessoa identificada ou identificável, como, por exemplo, o nome completo, número de documento, endereço, referências específicas (EX: Maria, dirigente da Organização/negócio “X” que atua com crianças e adolescentes em comunidade de baixo IDH).

Todas as pessoas físicas ou jurídicas que tratem dados pessoais são consideradas agentes de tratamento de dados (controladores ou operadores).

O QUE A LEI QUER DIZER COM “TRATAR” OS DADOS?

Tudo! São considerados “tratamento” todos os procedimentos realizados com os dados pessoais, tais como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A LGPD determina as regras aplicáveis ao tratamento, armazenamento e compartilhamento de dados pessoais

2.2.1. Dados pessoais x dados pessoais sensíveis

É muito comum existir uma confusão entre esses dois conceitos. Dados pessoais, de forma ampla, são quaisquer dados que identifiquem, **ainda que indiretamente**, os seus titulares. Portanto: CPF, RG, endereço, telefone, etc.

Já os dados pessoais sensíveis são aqueles que, **atrelados à pessoa natural**, podem trazer para ela ou para o grupo ao qual ela pertença, uma possibilidade de discriminação. O inciso II do art. 5º da lei estabeleceu uma lista de quais dados seriam esses:

Filiação de organizaçao de caráter religioso, filosófico ou político

Origem racial ou etnica

Filiação a sindicato

Opinião política

Dado referente à saúde ou vida sexual

Dado genético ou biométrico

Convicação religiosa

TITULAR DOS DADOS

Mas é possível entender que outros dados pessoais também sejam considerados sensíveis, mesmo estando fora dessa lista. Por exemplo, o uso de idade de mulheres, para evitar contratar mulheres que venham a ter filhos durante o vínculo de trabalho: Neste caso, vemos a combinação de dois dados que não são sensíveis por natureza: o gênero e a idade, para realizar uma decisão que gera a discriminação do grupo de mulheres que podem vir a ser mães em breve. Assim é que o uso discriminatório dos dados faz com que estes sejam revestidos de sensibilidade, a depender do contexto específico.

Princípios da LGPD:

O tratamento dos dados pessoais deve ser feito observando os seguintes princípios**:**

FINALIDADE:

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

A pessoa física titular do dado tem que saber exatamente por que a OSC ou o NI precisa coletar os dados e o que será feito com essa informação.

ADEQUAÇÃO:

compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

A OSC ou o NI só poderá tratar os dados conforme a finalidade informada ao(a) titular do dado.

NECESSIDADE:

limitação do tratamento 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.

A OSC ou o NI deve sempre se perguntar “Eu realmente preciso desses dados?”. Se a resposta for não, nem peça. Elimine e simplifique os campos desnecessários dos formulários. A OSC ou o NI deve ter (e tratar) o mínimo necessário de dados para a finalidade que eles serão usados

LIVRE ACESSO:

garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

A OSC ou o NI deve disponibilizar aos titulares um meio fácil e gratuito para que identifiquem quais são os dados que mantém e quais tratamentos são realizados a partir deles.

QUALIDADE DOS DADOS:

garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

A OSC ou o NI deve garantir que os dados que estejam em sua base sejam adequados à realidade. Ou seja, devem sempre refletir a realidade mais atualizada do(a) titular de dados. É importante ter mecanismos para realizar essa atualização ativamente e permitir que, se possível, as próprias pessoas realizem essa atualização. Isso pode ser feito por meio da promoção de recadastramento periódico ou da manutenção de espaço aberto para que o próprio(a) titular de dados atualize suas informações ou possa remetê-las ao encarregado(a) de proteção de dados da organização para que faça isso.

TRANSPARÊNCIA:

garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Durante todo o processo de tratamento, é necessário prezar pela transparência na relação com o(a) titular do dado, o que significa dizer que os tipos de tratamento que são realizados a partir dos dados do(a) titular devem ser demonstrados a ele(a) com exatidão e clareza.

SEGURANÇA:

utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

A OSC ou o NI deve sempre utilizar de medidas técnicas e administrativas, para evitar o vazamento e o acesso não permitido de terceiros à sua base de dados. Isso inclui não apenas sistemas de tecnologia da informação, mas também o treinamento das pessoas, direta ou indiretamente envolvidas no tratamento dos dados, porque muitos incidentes acontecem por causas internas como o despreparo da equipe.

PREVENÇÃO:

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Atrelada à segurança, indica que a OSC ou o NI deve adotar medidas para prevenir a ocorrência de danos, e isso inclui também o treinamento de quem, direta ou indiretamente, trata os dados pessoais.

NÃO DISCRIMINAÇÃO:

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Você não pode tratar os dados, especialmente os dados sensíveis, para fins ilícitos ou para promover qualquer tipo de discriminação negativa, em relação à raça, gênero, deficiência, orientação sexual ou quaisquer outros tipos. Registre-se que estamos falando de discriminação negativa e não a positiva presente em ações afirmativas e inclusivas em processo seletivo, por exemplo. Isso porque as positivas são consideradas discriminações benéficas aos titulares de dados pessoais e não estão entre as vedações do espírito da lei.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:

D*emonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*

Junto com a transparência, deve-se comprovar que estão sendo cumpridas todas as normas de proteção de dados pessoais com eficácia. Para isso, recomendam-se algumas ações como: criar um canal de comunicação direta com o(a) encarregado(a) de proteção de dados da instituição, fazer um mapeamento dos fluxos de dados dentro da organização/negócio para entender como eles ocorrem, criar política de privacidade que confira a devida transparência aos tratamentos de dados realizados dentro da organização/negócio, criar políticas internas (de segurança da informação, plano de incidente de segurança, política de resposta aos titulares) capazes de nivelar o que é esperado da equipe no momento de tratar dados pessoais e receber requisições de titulares e autoridades, para dar concretude à Política Geral de Proteção de Dados presente no site.

ATENÇÃO!

É importante mencionar que no caso de OSCs ou Negócios de Impacto que trabalham com grupos vulneráveis, vazamentos de dados podem acarretar em ataques discriminatórios e de perseguição, tanto de forma *online,* quanto *offline,* o que reforça, ainda mais, a atenção à segurança e à necessidade de existência de uma estrutura de governança de dados.

03

COMO IMPLEMENTAR EM **10 PASSOS**

A LGPD nos convida a acrescentar mais um pilar dentro da estrutura de governança interna da pessoa jurídica, para que os dados sejam tratados adequadamente no exercício de suas atividades. É por isso que, para além da construção de uma arquitetura da segurança da informação e de da utilização de sistemas seguros, também é essencial um ponto focal interno capaz de mobilizar a equipe e responsável por realizar treinamentos constantes, conscientizando a todos das obrigações e limites impostos pela LGPD.

Dessa forma, não basta alterar os contratos, inserindo cláusulas sobre a LGPD. É necessário mudar a cultura organizacional. Vamos lembrar como foi quando o cinto de segurança passou a ser um item obrigatório nos carros? Inicialmente foi uma mudança difícil de mentalidade sobre a importância do equipamento para a segurança de quem estava dentro do veículo, mas virou corriqueiro depois que, para além da indução da lei, as pessoas compreenderam a sua importância de ordem prática. Quando a chave mudar para as pessoas, teremos de fato organizações e negócios mais engajados na proteção dos dados pessoais!

E o que fazer para se adequar? Existem etapas até a conclusão de um processo de adequação à LGPD. Contudo, algumas ações podem ser empreendidas desde logo. Pensando em construir mecanismos mínimos para cumprir as disposições da LGPD, abaixo expomos os tópicos chave para adequação de uma OSC ou de um NI a esta nova lei!

“Adequação em 10 passos”

Fonte: SBSA Advogados.

1. **Criação de um canal de comunicação** sobre proteção de dados no site
2. **Workshop de sensibilização sobre a lei**
3. Designação de **ponto focal (encarregado(a) ou Comitê de Dados)**
4. **Mapeamento dos fluxos de dados pessoais**
5. Atribuição de **bases legais para justificar os tratamentos** de dados atualmente realizados
6. **Revisão de sites e aplicativos a partir** dos padrões de privacidade e proteção de dados
7. Adoção de medidas de **segurança da informação pela área de TI**
8. Construção de **políticas** para proteção de dados pessoais
9. Elaboração / revisão de **cláusulas contratuais** e acordos padrão
10. **Capacitação periódica** sobre proteção de dados **e monitoramento da conformidade**

3.1. Criação de um canal de comunicação sobre proteção de dados no site:

A primeira coisa...

O racional por trás da construção da LGPD é justamente devolver para o(a) titular de dados o **controle** sobre suas informações. Contudo, isso só é possível se houver um caminho evidente para o **exercício dos direitos** previstos na LGPD.

Nesse sentido, o **canal de comunicação** específico sobre proteção de dados é uma maneira efetiva de demonstrar que existe uma estrutura sendo construída para endereçar eventuais requisições de exercício de direitos previstos nos artigos 17 a 22 da LGPD.

Ao facilitar o exercício dos direitos de titulares, os agentes de tratamento evitam que esta pessoa recorra à ANPD ou ao Judiciário para exercer os seus direitos.

Sugerimos que seja disponibilizado no site um email que funcione como canal de comunicação com os titulares de dados de imediato.

3.2. Workshop de sensibilização sobre a lei:

Quando falamos em "tratar dados pessoais" dentro de uma pessoa jurídica, estamos nos referindo ao fato de que os seus integrantes – dirigentes, funcionários, voluntários, estagiários e/ou prestadores de serviços – dentro do exercício de suas funções colaboram para esta tarefa.
Nesse sentido, é preciso que essas pessoas compreendam os principais conceitos de proteção de dados, para que saibam operar corretamente os dados pessoais com os quais tiverem contato.

De nada adianta ter uma Política de Privacidade completa e **na prática** diária os dados serem tratados sem nenhum cuidado ou atenção em relação às disposições da lei. Assim, é fundamental que todos compreendam a lei e que sejam implementadas práticas e processos para a efetivação de suas disposições.

Sugerimos que a sensibilização de dirigentes, funcionários, voluntários, estagiários, prestadores de serviços e outros que façam uso de dados pessoais, sobre a lei e os seus conteúdos, destacando-se pontos de atenção que precisarão ser detalhados em momentos posteriores.

3.3. Designação de ponto focal (encarregado(a) ou Comitê de Dados):

É preciso definir na sua estrutura quem será o ponto focal de comunicação com a ANPD para responder sobre questões relacionadas a tratamento de dados, que fará a comunicação com os titulares de dados e que internamente mobilizará o tema. A essa pessoa, dá-se o nome de " encarregado(a) pelo Tratamento de Dados Pessoais", também conhecido pela nomenclatura em inglês "Data Protection Officer" (DPO).

EXISTEM VÁRIAS MANEIRAS PARA DEFINIR QUEM SERÁ O(A) ENCARREGADO(A) DE PROTEÇÃO DE DADOS:

A

O(A) encarregado(a) pode ser uma pessoa que trabalhe na própria organização, que receba formação técnica, ou seja, a quem seja dada a possibilidade de realizar cursos, formações, mentoria contratada ou até acesse uma certificação, que aprimore suas competências para executar as suas atividades;

B

O(A) cargo de encarregado(a) pode ser atribuído formalmente a uma única pessoa, que pode ser apoiada por um comitê de proteção de dados. Para apoiar o trabalho deste profissional, esse comitê deve conter pessoas de diversas áreas que somarão os seus conhecimentos aos do o(a) encarregado(a) de proteção de dados, permitindo que ele tome decisões de forma apoiada. Também se recomenda que essas pessoas recebam formação técnica ou auxílio de pessoas especialistas do assunto no formato de mentoria para que não haja decisões contrárias à legislação.

C

O cargo de o(a) encarregado(a) pode ser endereçado por um comitê de forma coletiva sem atribuição específica a uma única pessoa para o exercício dessa função, co responsabilizando todos os seus membros. Nesse caso, acontece o mesmo que na hipótese de cima, isto é, recomenda-se que o comitê seja composto por várias pessoas as quais possam somar conhecimentos para endereçar as atribuições de o(a) encarregado(a) de proteção de dados de forma coletiva. Também recomenda-se que essas pessoas recebam formação técnica ou ajuda de pessoas especialistas do assunto no formato de mentoria para que não haja decisões contrárias à legislação;

D

O(A) encarregado(a) pode ser um terceiro, ou seja, é possível contratar uma pessoa jurídica ou física de fora da organização ou do negócio, seja uma empresa ou um escritório de advocacia, que reúna competências prática e teórica em proteção de dados, para realizar essa função.

Além de ser um ponto de contato, o(a) encarregado(a) de Proteção de Dados deve zelar pela conformidade geral da OSC à LGPD.

O Comitê de Proteção de Dados pode fazer as vezes de o(a) encarregado(a) ou apenas apoiar o o(a) encarregado(a) na tomada de decisões sobre proteção de dados. Essa estrutura faz muito sentido, pois segue a lógica da governança mais colegiada presente nas organizações e nos negócios de impacto.

Essas são formas interessantes para viabilizar o exercício das atribuições inerentes ao cargo de encarregado(a) de Proteção de Dados de forma coletiva e para gerar conhecimento conjunto.

Sugerimos que, depois de tomada a decisão, seja inserido em local visível no site e divulgado nas redes sociais como contatar o Comitê de Proteção de Dados ou o(a) encarregado(a) de Proteção de Dados para tratar de assuntos relacionados!

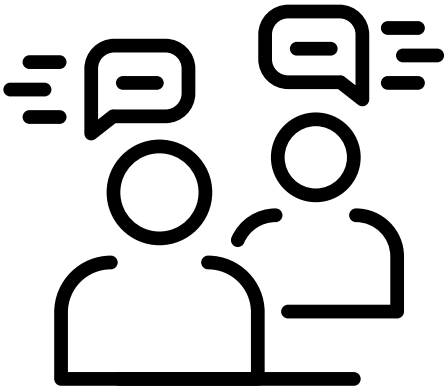
Também deve-se deixar claro nas políticas que forem elaboradas, ou até mesmo no Estatuto Social (no caso da OSC) ou no Contrato Social (no caso dos NI), formalizando o tema da proteção de dados como função que faz parte da sua governança.

3.4. Mapeamento dos fluxos de dados pessoais:

Mas como obter a visão integral dos fluxos de dados da sua organização/negócio?

À primeira vista, falar em mapeamento de dados em poder da organização/negócio pode parecer algo impossível. Contudo, com o avanço da legislação sobre proteção de dados, foi desenvolvida uma metodologia para facilitar o mapeamento das finalidades de uso dos dados, que consiste em compreender de forma aprofundada:

(i) quais dados entram na organização/negócio;
(ii) por qual via eles adentram,
(iii) como são tratados;
(iv) como ou se os dados são compartilhados dentro e com entes de fora e;
(v) como os dados são descartados.



Para entender o "caminho" dos dados na organização/negócio, normalmente se usa uma tabela, preenchida por pessoas de diferentes áreas, na qual as linhas representam as atividades que contém tratamento de dados pessoais e as colunas contém perguntas sobre esse fluxo de dados.

ATENÇÃO!

Para estar adequado à lei é preciso entender quais as finalidades de uso dos dados que entram na organização/negócio;

Para a redação de uma política de privacidade eficiente é preciso que haja ampla compreensão sobre como ocorrem os fluxos de dados de uma organização/negócio.

Roteiro de perguntas para o Mapeamento de Dados:

1. Qual a atividade que você está analisando?
2. Qual a finalidade do uso de dados pessoais dentro desta atividade?
3. Há outras finalidades de uso dos dados diferentes das que foram informadas para o(a) titular de dados?
4. Quais dados são tratados nesse processo? Há tratamento de dados pessoais sensíveis?
5. Qual o perfil do(a) titular dos dados? Eles são adolescentes (pessoas menores de 18 anos) ou crianças (pessoas menores de 12 anos)?
6. Quais sistemas/aplicações são utilizados no tratamento destes dados pessoais? Por quais programas os dados passam, por exemplo: os dados são inseridos no google drive, os dados são tratados no software de CRM de gestão de pessoas, os dados passam por algum programa de edição específico.
7. Os dados foram coletados diretamente do(a) titular dos dados ou vieram de um terceiro? Se sim, como eles chegaram até a organização/negócio?
8. Os dados pessoais coletados são estritamente necessários para que a atividade atinja o seu objetivo ou são coletados mais dados do que é preciso para a realização da atividade.
9. O(a) titular de dados é informado quanto das finalidades para as quais os seus dados podem ser utilizados?
10. Existe transferência de dados para fora do país tendo em vista o tratamento realizado dos dados? Isso inclui, por exemplo, se os dados são armazenados em nuvens fora do país.
11. Qual o tempo médio de armazenamento dos dados? Eles ficam na organização/negócio após atingir a finalidade para a qual foram coletados?
12. Onde os dados estão armazenados? Local físico e software utilizado para armazenar.
13. Os dados ficaram armazenados além da sua organização/negócio com algum parceiro ou prestador de serviço que teve acesso a esses dados?
14. Há alguma forma de anonimização dos dados? Eles são desvinculados do(a) titular para permanecer na base de dados?
15. Os dados são compartilhados com outras organizações ou parceiros para atingir a finalidade informada ao(a) titular ou por outras razões?
16. Como os dados são descartados?

ATENÇÃO!

Para um mapeamento completo, sugerimos que todas as atividades que envolvem o tratamento de dados pessoais sejam sistematizadas e que as perguntas sejam respondidas sobre cada uma das atividades. A partir desta fotografia completa dos tipos de tratamentos de dados realizados pela sua organização/negócio será possível atribuir as bases legais mais adequadas para legitimar os tratamentos de dados pessoais que são realizados. São atividades comuns que envolvem o tratamento de dados pessoais, a captação de dados nos sites com espaços para "Contato", "fale conosco", "doe aqui", "newsletter", "trabalhe conosco". Cada um desses espaços para o preenchimento de dados pessoais deve contar um aviso informando para o(a) titular a finalidade de uso dos dados pessoais. Não necessariamente todos os dados vão precisar do consentimento. Na verdade, a partir do mapeamento de dados é que será possível compreender quais tratamentos podem ser justificados pelo consentimento e quais tratamentos podem ser encaixados em outras justificativas legais que os legitimem.

3.5 Atribuição de bases legais para justificar os tratamentos de dados atualmente realizados.

Surge então a questão: depois de mapeados, como encontrar a justificativa legal adequada para tratar cada atividade que envolve dados?

A legislação de proteção de dados pressupõe que só se pode tratar dados pessoais nas hipóteses autorizadas por Lei. Assim, qualquer tratamento deve ter uma **base legal** que o autorize, o que deve ser feito a partir das características e finalidades de cada uso de dados, e da relação estabelecida entre controlador e titular.

Assim, um mesmo dado, como o CPF de uma pessoa, pode ser usado para diversas finalidades, por exemplo: para cadastro do usuário no site, ou emissão de um recibo de doação, e, portanto, o controlador justificará seu uso de maneira diferente em cada uma dessas hipóteses.

Tratar os dados pessoais sem uma finalidade evidente ou sem uma base legal pode ser considerado uma violação à LGPD.

Diversas são as justificativas (ou "bases legais") que podem ser empregadas. De acordo com o art. 7º da LGPD, o tratamento de dados pessoais somente poderá ser realizado:

a) mediante o consentimento do titular;
b) para cumprimento de obrigação legal ou regulatória pelo controlador;
c) para a execução de políticas públicas pela administração pública;
d) para realização de estudos por órgão de pesquisa;
e) para execução de contrato ou procedimentos preliminares a ele relacionados, em que o(a) titular seja parte;
f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
g) para a proteção da vida ou da incolumidade física do(a) titular, ou de terceiro;
h) para a tutela da saúde por parte de profissionais de saúde, serviços de saúde ou autoridade sanitária;
i) para atendimento aos interesses legítimos do controlador ou de terceiro; e
j) para a proteção do crédito.

A nossa legislação não dá preferência a nenhuma delas. Isso quer dizer que **o consentimento não é sempre a base legal mais apropriada**. A escolha deve se dar caso a caso, considerando os riscos, exigências e facilidades que aquela base legal trouxer consigo no caso concreto, como veremos mais detalhadamente nos tópicos seguintes.

A fórmula abaixo ilustra quais fatores devem repercutir nessa escolha:

ATENÇÃO!

(ORIGEM DO DADO + TIPO DO DADO + FINALIDADE) X PRINCÍPIOS = BASE LEGAL

3.5.1 Bases Legais para Tratamento de Dados Pessoais Sensíveis

O tratamento de dados pessoais sensíveis é diferente, e nem todas as justificativas apresentadas podem ser utilizadas. Excluem-se como bases legais apropriadas para esse tipo de tratamento: a execução de contratos, o legítimo interesse do controlador e a proteção ao crédito.

Além disso, no caso de dados pessoais sensíveis, é possível utilizar a justificativa de prevenção à fraude à personalidade do(a) titular para coletá-los, por exemplo, na coleta de biometria para a marcação do ponto dos trabalhadores. Na tabela abaixo, destacamos em laranja as bases legais para dados pessoais sensíveis que não podem ser utilizadas para tratar dados pessoais sensíveis.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses	**Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:**
I - mediante o fornecimento de consentimento pelo titular;	I - quando o titular ou seu responsável legal consentir, de **forma específica e destacada**, para finalidades
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;	II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei	b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas prevista
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;	c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sen
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;	**JUSTIFICATIVA INDISPONÍVEL PARA DADOS PESSOAIS SENSÍVEIS**
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;	d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;	e) proteção da vida ou da incolumidade física do titular ou de terceiro
VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;	f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou	**JUSTIFICATIVA INDISPONÍVEL PARA DADOS PESSOAIS SENSÍVEIS**
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.	**JUSTIFICATIVA INDISPONÍVEL PARA DADOS PESSOAIS SENSÍVEIS**
	g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção

Independentemente da base legal utilizada, o tratamento do dado pessoal segue sujeito aos princípios, fundamentos e garantias da LGPD, como os princípios da necessidade e da transparência. Essa noção é reforçada no art. 7º, parágrafo 6º, da lei:

> *"§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei,* ***especialmente da observância dos princípios gerais e da garantia dos direitos do titular****."*

Informar a base legal aos titulares de dados é uma boa prática de transparência ativa (de acordo com a Nota técnica nº 02/2021/CGTP/ANPD, da Autoridade Nacional de Proteção de Dados), mesmo que a LGPD não estabeleça expressamente esta obrigação.

Vamos a cada uma delas!

Bases Legais para Tratamento de Dados Pessoais (art. 7º da LGPD)

- **Consentimento**
- **Obrigação legal-regulatória**
- **Execução de políticas públicas**
- **Realização de estudos por órgão de pesquisa**
- **Execução de um contrato**
- **Exercício regular do direito em processos**
- **Proteção da vida**
- **Tutela de saúde**
- **Legítimo interesse**
- **Proteção ao crédito**

Consentimento

A base legal do consentimento se refere à oportunidade em que o(a) titular expressamente autoriza que façam uso de seus dados. De acordo com o art. 5º, inciso XII, trata-se de:

> *"manifestação livre, informada e inequívoca pela qual o(a) titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".*

E como coletar o consentimento de forma a legitimar os usos de dados da organização/negócio?

Para ser válido, o consentimento deve ser **LIVRE, INFORMADO** e **INEQUÍVOCO**.

Livre: significa que a pessoa que é titular dos dados deve poder discordar do tratamento e seguir utilizando o serviço ou acessando a plataforma/site. A pessoa deve ser realmente livre para dizer não, ou seja, ela não pode ser obrigada a fornecer os dados. Se isso acontecer, é preciso utilizar outra justificativa para legitimar o tratamento de dados pessoais.

Informado: se refere à ciência, da pessoa que está informando os dados, quanto às finalidades para as quais serão utilizados, de forma específica; não é possível informar de forma genérica, por exemplo: "usamos os dados para melhorar a sua experiência". Essa é uma frase que pode abarcar diversas finalidades de uso das informações e, por isso, não cumpre a função de informar o titular. A finalidade tem que ser evidente e pessoa titular dos dados precisa concordar com ela.

Por último, **inequívoco:** o adjetivo inequívoco se refere a ausência de dúvida quanto à livre vontade da pessoa titular de dados em fornecer as informações para as finalidades que lhe foram informadas pelo controlador. A ausência de sua manifestação não pode ser tida como consentimento. A vontade tem que ser realmente expressa pela pessoa titular de dados.

Para cumprir com os três requisitos é importante revisar os fluxos de dados pessoais tratados com base nessa justificativa para garantir:

i. **Que a pessoa titular dos dados não foi obrigada a consentir**, ou seja, que tinha opção de seguir utilizando o serviço/plataforma sem fornecer os dados e optou por consentir com o tratamento sem esse tipo de pressão.

Exemplo: Durante a inscrição em um evento online, existem dados que são essenciais para viabilizar a participação no evento, como nome e email. Normalmente muitas instituições costumam formar bases de contatos para envio de mensagens posteriormente para aquele titular de dados que se inscreveu no evento. Contudo, é possível permitir que a pessoa decida livremente se deseja ou não

fazer parte dessa base de contatos. Assim, o ideal é que ela não seja automaticamente inserida nesse *mailing*, mas sim decida livremente participar. Isso é um exemplo ideal de consentimento livre, pois a pessoa é informada de que será inserida no mailing se consentir com isso. (art. 7º, I, da LGPD)

ii. **Que a pessoa tenha sido efetivamente informada da finalidade de uso dos seus dados pessoais**, ou seja, que existe um aviso evidenciando para ele essa finalidade e permitindo que ele decida sobre o consentimento realmente ciente dessa finalidade e das implicações da decisão pelo não consentimento.

Exemplo: Essa imagem precisa vir acompanhada de um aviso informando o porquê a foto do perfil pode ser fornecida pela pessoa. Assim ela pode escolher se deseja ou não fornecer a foto a partir da finalidade de uso da imagem.

iii. **Que não tenha existido equívoco no momento do consentimento**, ou seja, que a pessoa titular de dados pessoais decidiu ativamente fornecer o consentimento.

Exemplo:

⚠ Caixas pré-selecionadas não permitem compreender até que ponto o(a) titular de dados realmente consentiu com o tratamento de dados para o envio de mensagens, ou mesmo se leu a Política de Privacidade antes de assinalar a caixa de seleção, o que não permite afirmar que o consentimento seja inequívoco.

Há mais algumas diretrizes relevantes que devem ser observadas quando se faz o tratamento de dados utilizando-se o consentimento como base legal.

O consentimento deve estar destacado, separado das demais cláusulas contratuais, para garantir que o(a) titular esteja de acordo com aquele uso em específico, e não com a política de privacidade como um todo. **Logo, o consentimento não pode ser concedido genericamente (algo como "autorizo o tratamento de meus dados pessoais por tal organização/negócio"). Ao contrário, deve estar expressamente referindo-se a finalidades específicas.**

Por exemplo, no caso do uso de dados de raça para ações afirmativas, esse tipo de tratamento pode estar justificado pelo consentimento, uma vez que o dado não é necessário para participar de um processo seletivo, apenas para participar da ação afirmativa. **Assim, é possível deixar o(a) titular decidir se deseja ou não dar o seu dado para essa finalidade, porque participar do processo seletivo não depende desse dado, somente a participação da ação afirmativa**. Os dados necessários para participar do processo seletivo estariam justificados pelo uso da base legal que possibilita o uso dos dados sem consentimento devido à sua necessidade para procedimentos preliminares ao fechamento de um contrato, de acordo com o art. 7º, VII, da LGPD. No caso, o consentimento estaria sendo corretamente captado por meio da desobrigação quanto ao preenchimento deste campo e mediante um aviso, indicando que os dados só serão utilizados para aquela finalidade de priorizar candidatos não brancos, ou seja, para a ação afirmativa.

Obtido o consentimento de forma adequada, nos moldes acima expostos, caso se deseje ou precise compartilhar os dados do titular com terceiros, será necessário obter um novo consentimento para essa finalidade específica de compartilhamento, ou então utilizar uma das outras bases legais que justifiquem esse compartilhamento adequadamente.

ATENÇÃO!

Para utilização de dados pessoais de acesso público, em que a exigência do consentimento é dispensada (art. 7º, parágrafo 4º) deve-se considerar a finalidade, a boa-fé, e o interesse público que justificaram sua disponibilização.

Apesar de sua aparente simplicidade, a utilização da base legal do consentimento exige desdobramentos operacionais para obtê-lo, mantê-lo atualizado e assegurar o direito do titular revogá-lo, o que pode feito a qualquer momento. No que se refere aos direitos dos titulares, quando o dado é tratado com base no consentimento, é direito do(a) titular solicitar cópia eletrônica integral de seus dados pessoais, na forma do art. 19, parágrafo 3º da LGPD.

Obrigação legal-regulatória

Essa base legal, com previsão no art. 7°, inciso II da LGPD, é utilizada nos casos em que o tratamento de determinado dado pessoal é necessário ao cumprimento de uma obrigação legal ou regulatória do controlador. O exemplo mais comum é o das relações trabalhistas entre a organização/negócio e seus colaboradores. Para que esta cumpra com a legislação trabalhista e previdenciária deve ter acesso a documentos oficiais de identificação, como carteira de trabalho, RG e CPF, informações sobre salário, entre outros.

Discute-se se a obrigação decorreria apenas de lei em sentido estrito, como aquelas votadas no âmbito do Poder Legislativo, e de normas emitidas pelas agências reguladoras. O entendimento majoritário tem sido o de que qualquer normal de caráter impositivo autoriza o tratamento de dados com base nesse dispositivo da LGPD.

Execução de políticas públicas

Prevista no art. 7°, inciso III da LGPD, essa base legal é utilizada para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas. A política pública em si deve estar prevista em leis, regulamentos, contratos, convênios ou instrumentos similares. Neste sentido, é muito importante adequar os instrumentos de parceria para que neles conste a transferência voluntária de dados do Poder Público para as entidades privadas sem fins lucrativos.

A lei traz parâmetros interessantes para o compartilhamento de dados pessoais por parte do poder público com as entidades privadas, que será permitido nos casos de:

a) execução descentralizada de atividade pública que exija a transferência para fim específico e determinado;
b) previsão legal ou transferência respaldada em contratos, convênios ou instrumentos congêneres; e
c) na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do(a) titular dos dados.

A despeito da previsão clara de compartilhamento do Poder Público, há discussão sobre a possibilidade de se utilizar essa base legal também para fundamentar o tratamento de dados pelas organizações que atuam em parceria com a administração pública para execução de políticas públicas. O inciso III do art. 7º da LGPD é expresso ao estabelecer que esta base legal é prerrogativa do poder Público. Nesse sentido, é possível entender que as organizações que tenham firmado um termo ou acordo com órgãos públicos, atuem na condição de mandatárias do Poder Público para a execução dos projetos ou atividades previstos nos planos de trabalho acordados. Assim, agindo como mandatárias ou delegados da administração pública, é possível que no caso concreto a OSC estejam autorizadas a tratar os dados pessoais repassados pelo Poder Público, com fundamento na base legal de execução de políticas públicas, sem necessidade portanto de captar o consentimento dos titulares.

De toda forma, entendemos que, para além da execução de políticas públicas, o tratamento de dados por uma OSC no âmbito da implementação de atividades numa relação de parceria com o Poder Público pode ser justificado, nos termos da LGPD, com base na execução do contrato, sempre que os dados captados forem necessários para a finalidade prevista no instrumento.

Realização de estudos por órgão de pesquisa

O tratamento de dados fundamentado com a base legal de realização de estudos por órgão de pesquisa, prevista no art. 7°, inciso IV da LGPD, é prerrogativa exclusiva de órgãos de pesquisa na realização de estudos e levantamentos. Mas o que caracteriza um órgão de pesquisa? Apenas órgãos públicos ou qualquer entidade que realizar estudos estaria enquadrada? Vejamos.

A LGPD define órgão de pesquisa como:

> "órgão ou entidade da administração pública direta ou indireta ou **pessoa jurídica de direito privado sem fins lucrativos** legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em **sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada** de caráter histórico, científico, tecnológico ou estatístico"

Portanto, para utilização dessa base legal, é necessário que a entidade seja de fato um órgão de pesquisa, exigindo-se para tanto que a organização sem fins lucrativos tenha em seu Estatuto Social como parte de seus objetivos sociais a pesquisa básica ou aplicada, de caráter histórico, científico, tecnológico ou estatístico. Desta forma, as entidades que tenham identidade com este tipo de atuação devem certificar-se de que seu estatuto expresse a pesquisa como um dos objetivos. Esta base não pode ser utilizada por empresas privadas com fins lucrativos.

Assim, esta base legal não se aplica aos Negócios de Impacto revestidos da forma jurídica empresarial, mesmo que incumbidos institucionalmente da realização de pesquisas.

Cabe lembrar ainda que sempre que possível, deve-se realizar a anonimização dos dados pessoais tratados, de maneira a impossibilitar a associação (direta ou indireta) daquele dado a uma pessoa.

Execução de um contrato

De acordo com o art. 7°, inciso V, essa base legal se refere à autorização do tratamento de dados pessoais para o cumprimento de obrigações relacionadas **ao contrato, no qual o(a) titular seja parte.**

Um caso comum no âmbito de uma organização/negócio seria o contrato firmado com um prestador de serviço. Para operacionalizar essa obrigação e o pagamento da contrapartida, seria necessário tratar dados bancários do prestador de serviço. Não seria necessário pedir seu consentimento específico, pois o tratamento desses dados é pressuposto para execução do contrato.

Outro exemplo é o do fornecimento de *newsletter*. Para entregar o boletim informativo é necessário tratar os dados pessoais das pessoas que decidiram recebê-lo, independentemente do consentimento.

A contraprestação de fornecer a *newsletter* e o acordo de vontade envolvido no seu fornecimento pode ser considerado um contrato que deve ser honrado junto ao titular.

É com justificativa nesta base legal que podemos enquadrar o tratamento de dados pessoais de usuários de serviços públicos providos por Organizações da Sociedade Civil, quando esses dados são necessários para a prestação do serviço.

Exercício regular do direito em processos

Essa base legal com previsão no art. 7°, inciso VI da LGPD, autoriza o uso de dados pessoais para defesa de direitos em processos, sejam eles judiciais, administrativos ou arbitrais. O exemplo clássico é a necessidade de se identificar, na petição inicial, a pessoa contra quem se está ingressando no Judiciário. Não seria possível depender do consentimento dela para isso. É necessário se utilizar de seu nome, RG, CPF, endereço, dentre outros dados. Por meio dessa base legal isso é possível, sem que seja preciso solicitar o consentimento ou "autorização" do(a) titular para tanto.

Proteção da vida

De acordo com o art. 7°, inciso VII da LGPD, essa base legal permite o tratamento de dados pessoais para a proteção da vida ou da incolumidade física do titular, e até mesmo de terceiro que esteja sob algum risco. Por força da pandemia, diversos foram os exemplos da utilização de dados pessoais para contenção da contaminação do coronavírus, como os dados de geolocalização para monitoramento do deslocamento das pessoas.

Tutela de saúde

Essa base legal prevista no art. 7°, inciso VIII da LGPD, permite o tratamento de dados pessoais quando este for necessário para proteção da saúde do titular. A LGPD restringe o uso dessa base legal a profissionais de saúde (elencados em regulamento específico), serviços de saúde e autoridades sanitárias. Um exemplo de aplicação dessa justificativa é a de um hospital que precisa ter acesso ao histórico de um paciente que chegou às pressas no pronto-socorro, coletando diversos dados pessoais na primeira interação da pessoa com o(a) médico(a) para que ele(a) possa efetivar os cuidados necessários ao(à) paciente.

Legítimo interesse

De acordo com o art. 7°, inciso IX, essa base legal pode ser utilizada no atendimento de interesses legítimos do controlador ou de terceiro. Mas o que seria um "legítimo interesse"? Há muita discussão em torno do termo, mas tanto a lei quanto a prática trazem algumas balizas para utilização dessa justificativa.

ATENÇÃO!

O art. 10 da LGPD organiza a ponderação de interesses que deve ser feita e registrada antes da aplicação dessa justificativa. O artigo trata de algumas características que compõem o legítimo interesse, permitindo a sua mobilização para suportar determinada atividade sem o consentimento do titular. Por isso o artigo prevê o que se chama de "teste de legítimo de interesse", que deve ser documentado quando há a sua utilização.

(i) apoio e promoção de atividades do controlador e
(ii) proteção, em relação ao titular, do exercício regular de seus direitos; ou
(iii) prestação de serviços que o beneficiem, respeitadas suas legítimas expectativas.

O legítimo interesse do controlador deve sempre levar em conta as expectativas do(a) titular dos dados em relação ao tratamento de dados que ele deseja realizar utilizando essa base legal, o que chamamos de "Legítima expectativa do titular".

Além disso, conforme os parágrafos 1º e 2º desse mesmo artigo, apenas os dados estritamente necessários para a finalidade pretendidas poderão ser tratados, e deve ser dada total transparência às suas ações.

Na prática, é importante fazer uma avaliação sobre a aplicabilidade dessa base legal pois ela exige um grau maior de registro. O art. 37 da LGPD reforça essa noção ao determinar que:

> *"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**."*

É possível que a Autoridade Nacional de Proteção de Dados (ANPD) solicite relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento o legítimo interesse.

Para avaliação dos riscos e adequação do legítimo interesse ao caso concreto da sua organização/negócio, é possível realizar um "teste de quatro passos":

01

FINALIDADE LEGÍTIMA

Identificar se a finalidade para qual a organização/negócio deseja se utilizar dos dados é lítica, ou há alguma vedação na legislação brasileira para tanto, partindo-se sempre da análise de uma situação concreta.

02

NECESSIDADE

Averiguar ser o legítimo interesse a única base legal possível. E em caso positivo, tratar os dados de acordo com o princípio da minimização, ou seja, tratar o mínimo necessário para determinada finalidade, e ser menos "intrusivo" possível.

03

BALANCEAMENTO

Considerar a legítima expectativa do(a) titular (perguntar-se, por exemplo, se o(a) titular poderia esperar o tratamento de dados para aquela finalidade), bem como seus direitos e liberdades fundamentais.

04

SALVAGUARDA

Dotar o tratamento do máximo de transparência possível, garantindo o direito de oposição do(a) titular("opt-out") e mitigando riscos, como realizar a anonimização, quando possível, e aplicar demais princípios da LGPD

exemplo: se a organização decide continuar usando sua base de e-mails antiga sem pedir novo consentimento para isso, é possível utilizar o legítimo interesse para justificar a continuidade do uso dos dados. Nesse sentido, a necessidade está justificada diante da avaliação de que excluir todas as pessoas que não consentiram ativamente com o uso dos seus dados para o envio de comunicações poderia diminuir consideravelmente a base de dados disponível para isso, sendo que é algo estratégico para qualquer organização.

Assim, é possível utilizar o legítimo interesse e criar um aviso de transparência que deixe claro: como os dados do(a) titular chegaram até a organização, para quais finalidades eles poderão ser utilizados. Como medida de salvaguarda, é possível garantir um caminho fácil para que a pessoa saia daquela comunicação se desejar e, em respeito ao princípio da finalidade, garantir que os dados serão utilizados somente para aquilo que está sendo informado ao(a) titular no mencionado aviso de transparência

Proteção ao crédito

Só pode ser utilizada por instituições financeiras para tratar de dados pessoais com o objetivo de avaliar os riscos envolvendo a concessão de crédito. Cabe dizer que por se tratar no uso de dados pessoais num contexto específico, diversas normas setoriais e consumeristas se aplicam à temática, além da LGPD. Como exemplo, temos o Código de Defesa do Consumidor (Lei nº 8.078/1990) e a Lei do Cadastro Positivo (Lei nº 12.414/2011 e Lei Complementar nº 166/2019, conhecida também como "Nova Lei do Cadastro Positivo"), além de regulamentações próprias do Banco Central (BACEN) e da Comissão de Valores Mobiliários (CVM).

Vale destacar que a princípio, o uso de dados pessoais com fundamento nesta base legal aplica-se também às OSC que atuam com microcrédito, na forma da legislação específica. Isto porque o art. 4º da MP 2172-32, e a Resolução do Banco Central BC 2874, de 26.07.2001, elencam as entidades voltadas ao microcrédito qualificadas como OSCIP entre o rol de pessoas jurídicas autorizadas a este tipo de atividade.

3.6 Revisão de sites e aplicativos a partir dos padrões de privacidade e proteção de dados

O conceito de Privacy by Design – que significa privacidade na concepção da arquitetura desde o princípio – tem como foco a criação de ambientes virtuais cujo design seja efetivo para garantir o direito à privacidade e proteção de dados dos usuários. Dentre os princípios do conceito está a noção de agir proativamente, atuando de maneira a prevenir situações de violação, ao invés de se concentrar apenas na reparação de danos causados pela violação.

Algumas legislações como a GDPR (*"General Data Protection Regulation")*, da União Europeia, adotaram explicitamente a obrigação de incorporar padrões de Privacy By Design em plataformas, sites e outros tipos de ambiente online. A LGPD, por sua vez, não estabelece expressamente a obrigação de Privacy By Design como acontece na GDPR. Assim, a necessidade de implementar esses *standards*, decorre dos fundamentos e princípios da legislação, previstos no seu artigo 6º.

Além disso, há a obrigação específica de criar ambientes que fomentem o exercício do direito à proteção de dados, o que pode ser interpretado como obrigação de observar e aplicar medidas de Privacy By Design:

> *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*
> *(...)*
> *§ 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.*

Assim, a análise da adequação dos sites à Lei Geral de Proteção de Dados é feita a partir de uma conjugação de fundamentos, princípios e definições, como a de consentimento. Isso porque, essas disposições geram consequências práticas sobre a redação e a disposição de textos sobre proteção de dados nos sites, como por exemplo o uso do termo "concordo" ou "entendo" em se tratando do consentimento sobre os Termos de Uso de da Política de Privacidade.

Além disso, utilizamos como baliza para a nossa análise os princípios que orientam o conceito de Privacy by Design (privacidade desde o princípio):

1. Ser proativo e não reativo – atuar para prevenir situações de violação e não atuar para reparar situações
2. Privacidade como configuração disponível ao usuário
3. Privacidade incorporada ao design
4. Funcionalidade do site
5. Segurança de ponta a ponta – Ciclo completo protegido
6. Visibilidade e transparência em relação aos tratamentos de dados
7. Respeito à privacidade do usuário – manter ela/e no centro das ações de design

A existência desses princípios permite a construção de uma análise sobre a adequação dos ambientes digitais construídos pela organização ou negócio para interagir com o seu público, desde sites, até aplicativos, plataformas de educação a distância e etc. Isso é muito importante para a adequação como um todo, uma vez que esses espaços apresentam a "cara" da entidade e têm potencial de indicar logo de início qual o seu nível de conformidade à LGPD e a sua possibilidade de efetivar os direitos dos titulares de dados.

3.7 Adoção de medidas de **segurança da informação pela área de TI**

É impossível garantir a proteção de dados pessoais sem a incorporação, em sua organização/negócio, de medidas mínimas de segurança da informação. Sabendo disso, recentemente, a ANPD emitiu um Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte, que deve ser considerado para a formulação de práticas que visam garantir a Segurança da Informação.

O documento conta com um checklist de boas práticas que deve ser utilizado para garantir a conformidade mínima a padrões mais seguros de tratamento dos dados pessoais.

É importante considerar a incorporação de profissionais de tecnologia da informação à sua equipe, seja por meio da contratação de uma empresa especializada nesse setor ou, pelo menos, da implementação de algumas medidas básicas que possam dar concretude às salvaguardas e princípios da LGPD.

Algumas medidas que podem ser implementadas prontamente para o tratamento dos dados pessoais em seu poder:

a) Orientar os seus colaboradores a não fornecer dados pessoais prontamente quando houver a solicitação de outras organizações, órgãos ou mídia. Sempre questionar sobre o uso dos dados e verificar se isso está alinhado com a finalidade inicial de uso dos dados.

› Pessoas mal-intencionadas podem cometer crimes de falsificação ou fraude causando prejuízos que terão sido responsabilidade da organização/negócio. Por isso só forneça dados a pessoas autorizadas. Se a pessoa não estiver autorizada a receber os dados indique que os colaboradores conversem com seus superiores e com pessoas que estão encarregadas do projeto de adequação da organização/negócio à LGPD.

b) Oriente os seus colaboradores a não utilizarem as credenciais de outras pessoas ou fornecerem suas credenciais para os seus colegas.
c) Oriente seus colaboradores a criar senhas com mais de 8 caracteres que contenham caracteres especiais, números e alternem letras maiúsculas e minúsculas em seu corpo, e que troquem a senha com uma frequência de até 3 meses.

› quanto mais "bagunçada" a senha melhor, pois mais difícil será descobri-la. Assim tente misturar letras maiúsculas, minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase aleatória e pegar a primeira, segunda ou a última letra de cada palavra. Por exemplo: usando a frase "batatinha quando nasce se esparrama pelo chão", podemos gerar a seguinte senha "BqnsepC".

› Procure usar um Gerenciador de senhas para armazenar suas credenciais (Ex.: KeePass, BitWarden, LastPass) ao invés de deixá-las salvas.

d) Classifique os dados de forma diferente de acordo com a sensibilidade e confidencialidade das informações que você trata:

1. Público – Não Rotulado
2. Interno – Pode ser rotulado
3. Confidencial – Deve obrigatoriamente ser rotulado
4. Estritamente Confidencial – Devem obrigatoriamente ser rotulados

› Depois disso, oriente os seus colaboradores a identificarem qual o tipo de dados envolvidos na comunicação de compartilhamento e, se necessário, adotarem medidas especiais de proteção como senhas de acesso, comunicação sobre o compartilhamento ao o(a) encarregado(a) de proteção de dados, etc.

› Além disso, verifique sempre os endereços de e-mail dos destinatários que receberam estas informações sensíveis, para evitar que os dados sejam enviados para pessoas desconhecidas. Ainda, se possível, evite sempre utilizar pen-drives ou compartilhar informações sigilosas via e-mail. Por fim, coloque senha nos arquivos para que somente as pessoas com a senha enviada pela sua organização/negócio consigam abrir os documentos ou bases de dados enviadas pelos colaboradores.

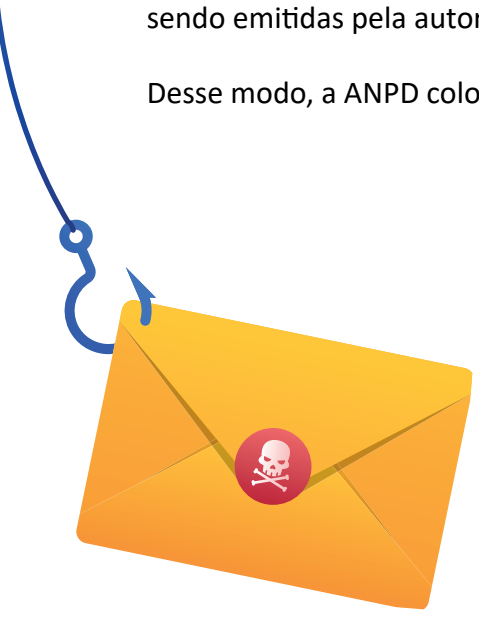
› Implemente a criptografia dos e-mails: isso é feito através do uso de um programa para e-mail chamado Thunderbird e plugins de criptografia como Enigmail. Não há custo para utilizar esse recurso, porém toda a sua equipe deve ser treinada no uso desses aplicativos. O passo a passo para isso pode ser encontrado em **Emailselfdefense.fsf.org.**

e) Identifique quais colaboradores realmente precisam acessar determinados dados pessoais e permita que somente eles acessem determinados dados pessoais em seu poder. Por exemplo, se há muitos dados sensíveis coletados para um programa de diversidade na seleção de novos colaboradores, faça com que o acesso desses dados só ocorra pelas pessoas que realmente avaliarão os candidatos inscritos para o programa de diversidade e não toda a área de RH.
f) Armazene os documentos da organização/negócio apenas nos próprios servidores da organização/negócio e evite o uso de nuvens públicas, como o Google Drive ou o DropBox.
g) Notebooks e celulares devem ser guardados em locais seguros quando não estiverem em sua posse.
h) Não instale programas que você não conhece ou que não estejam aprovados pelo setor de tecnologia de informação, quando este setor existir.
i) Não abra e-mails e arquivos recebidos que você não conhece ou cujo remetente é desconhecido.

> O maior vetor de ataque às organizações/negócios é por meio de Spams e e-mails contendo anexos maliciosos. Grande maioria dos malwares (vírus, adwares, spywares, orms e trojans) são enviados via e-mail como anexos ou links de redirecionamento.

Nesse sentido, a própria Autoridade Nacional de Proteção de Dados expõe a realização de treinamentos constantes como medida administrativa de Segurança da Informação que pode ser implementada por todos os agentes de tratamento de dados pessoais em seu Guia de Segurança da Informação para Agentes de Pequeno Porte. A ANPD enuncia que a conscientização implica informar e sensibilizar os colaboradores de determinada entidade para as obrigações da LGPD e para as normas que forem sendo emitidas pela autoridade para regulamentar a aplicação dessa lei.

Desse modo, a ANPD coloca como informações a serem repassadas aos funcionários:



- como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, como contaminação por vírus ou ataques de phishing[4], que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;
- manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;
- não compartilhar logins e senhas de acesso das estações de trabalho;
- bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- seguir as orientações da política de segurança da informação

4 "Phishing, phishing-scam ou phishing/scam, ´e o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilizacão combinada de meios técnicos e engenharia social. A palavra phishing, do inglês "fishing", vem de uma analogia criada pelos fraudadores, onde "iscas" (mensagens eletrônicas) são usadas para "pescar" senhas e dados financeiros de usuários da Internet." Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

3.8 Construção de políticas para proteção de dados pessoais

Para demonstrar o compromisso com a Lei Geral De Proteção de Dados há a indicação de que alguns documentos sejam feitos, de modo a criar uma estrutura de governança de dados que seja verificável pela Autoridade Nacional de Proteção de Dados ou por agentes do Poder Judiciário.

Isso tem a ver com o princípio da prestação de contas, que explicamos lá em cima. Lembre-se, não basta dizer que está adequado à LGPD, é preciso demonstrar essa adequação!

Não há uma resposta clara na legislação sobre quais políticas devem ser obrigatoriamente criadas. O que se sabe é que, desde 2014, o Marco Civil da Internet exige publicidade e clareza das "políticas de uso de aplicações da internet" (Art. 7º, XI), o que geralmente é interpretado como a obrigatoriedade de criação de Termos de Uso de sites, aplicativos e plataformas.

Os "Termos de Uso" são documentos diferentes das "Políticas de Privacidade". Isso porque, os Termos de Uso têm como objetivo estabelecer as regras entre quem está utilizando o site, serviço ou plataforma e a pessoa física/jurídica que é dona desses "espaços" virtuais. São documentos mais jurídicos, por assim dizer, porque neles estão dispostas as obrigações das partes e as responsabilidades no caso de descumprimento delas, dentre outras regras definidas de acordo com os casos concretos. Por outro lado, a Política de Privacidade tem o intuito de deixar claro como ocorrem os tratamentos de dados feitos pela organização, viabilizando o exercício de direitos por parte do titular.

3.8.1. A Política de Privacidade Externa

Políticas de Privacidade são documentos que visam ao estabelecimento de uma relação de transparência entre o controlador, o operador, e o titular dos dados pessoais. O ideal é que a Política de Privacidade e a os Termos de Uso não sejam apresentados conjuntamente porque a leitura pode ser exaustiva e as pessoas podem não ler tudo, de modo que nem um, nem outro documento cumprirá com a função informativa a qual se destinam.

A Política de Privacidade deve ser feita principalmente em respeito ao princípio da transparência (Art. 6º, da LGPD) e deve trazer para os titulares de dados a garantia de que eles obterão informações precisas, claras e facilmente acessíveis, por parte dos controladores de dados, quanto às finalidades de uso de suas informações.

O artigo 9º da LGPD, expõe em linhas gerais, orientações sobre o que uma Política deve apresentar, minimamente, para os titulares de dados:

> *"Art. 9º O(a) titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:*
>
> *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; e*
>
> *VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei."*

A leitura sistemática do artigo 9º com o artigo 18 da LGPD, que trata dos direitos básicos dos titulares de dados, é interpretada como a obrigação de disponibilizar uma Política de Privacidade acessível e clara aos titulares de dados.

3.8.2. A Política de Privacidade Interna

A Política de Privacidade orientada para o público externo da organização/negócio não se confunde com uma Política de Privacidade Interna, a qual pode prever procedimentos e cuidados específicos para a documentação das atividades de tratamento, em atendimento ao art. 37 da LGPD, que diz "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".

Além disso, essa Política Interna pode apresentar informações sobre quem é o(a) encarregado(a), como contatá-lo, quais os cuidados para obter o consentimento das pessoas, como notificar seus superiores em caso de incidentes de segurança, regras de compartilhamento de informações internas ou para fora da organização/negócio, entre outras regras.

Esse é um documento importante para criar uma cultura de proteção de dados que permita à organização/negócio o cumprimento daquilo que foi exposto para o(a) titular de dados na política externa.

3.8.3. Política de Segurança da Informação e de Incidentes de Privacidade

Apesar de a LGPD não mencionar a necessidade expressa de criação de uma Política de Segurança da Informação e de uma Política de Resposta a Incidentes de Segurança, a lei estimula a criação de uma estrutura de governança que pode e deve, se possível, conter esse tipo de documento.

A política de segurança da informação visa demonstrar o cumprimento dos artigo 46, 47 e 49 da LGPD, que diz:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
>
> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Por outro lado, uma Política que defina o fluxo de ações e o que é um incidente de segurança pode ser feita de modo a endereçar o artigo 48 da LGPD, que diz:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao(a) titulara 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.

Ademais, é possível também fazer uma Política de Proteção de Dados de Funcionários e Colaboradores. Não podemos esquecer que os funcionários e colaboradores também são titulares de dados pessoais e, por isso, é importante que haja transparência da organização/negócio em relação aos tratamentos de dados realizados por ela em relação a esses titulares. Além disso, essa política visa apresentar a equipe quais são seus direitos e como exercê-los em face da organização/negócio.

3.8.4. Política de Cookies

De acordo com a Política de Cookies da FGV, que pode ser considerada um ótimo exemplo do que este documento deve apresentar para o(a) titular de dados, os cookies são:

> "na terminologia da informática, pequenos arquivos de texto depositados por um site servidor no computador do cliente usuário para "memorizar" algumas informações relativas àquela navegação."

Ou seja, os cookies podem ser considerados dados pessoais, porque tem o potencial de identificar o(a) titular de dados através do seu padrão de navegação nos sites, aplicativos e plataformas online.

Normalmente, os cookies podem ser de primeira ou terceira parte. Os cookies de primeira parte são os colocados no site pela própria organização/negócio para fazer a plataforma/site/aplicativo funcionar ou para entender o perfil de quem frequenta as suas páginas/aplicativos e etc. Além disso, pode haver cookies de terceiros, ou seja, estabelecidos por outros domínios, o que normalmente acontece quando um site/plataforma ou aplicativo apresenta elementos de outros sites, como imagens, redes sociais ou anúncios de publicidade.

Os tipos de cookies mais comuns são:

(a) Cookies operacionais/técnicos: que viabilizam a navegação no site permitindo a utilização da página pelo usuário;
(b) Cookies de funcionalidade: permitem que o website forneça uma funcionalidade personalizada ou melhorada e podem ser estabelecidos por você ou por outro terceiro;
(c) Cookies analíticos: registram os dados de uso do site/plataforma ou aplicativo, para que seja possível aprimorar a experiência do usuário e mesmo produzir conteúdo a partir da ciência do que as pessoas mais acessam;
(d) Cookies comportamentais/marketing: servem para entender as preferências do usuário baseado em dados relativos à sua navegação, auxiliando a exibição e criação de anúncios e conteúdos personalizados.

    Por exemplo, uma organização/negócio/negócio que utilize redes sociais como Facebook, Google ou Linkedin para fazer campanhas de marketing. Quando um usuário clica nos ícones dessas páginas dentro do seu site, essas plataformas conseguem cruzar as informações do usuário com os perfis em suas plataformas, mesmo que você não tenha acesso a esses dados depois.

Como os cookies são dados pessoais, é importante informar quais cookies existem na sua página e indicar para o(a) titular como desativá-los se isso for possível. Um primeiro passo nesse sentido, pode ser indicar que dentro de cada navegador é possível limpar/desativar os cookies seguindo alguns passos clicando no nome daquele que você utiliza: Google Chrome, Internet Explorer, Firefox, e Safari.

3.9 Elaboração / revisão de **cláusulas contratuais** e acordos padrão:

3.9.1 A diferença entre o Operador e o Controlador de dados:

Dependendo do papel que a OSC ou o NI exerce dentro do fluxo de tratamento dos dados, sua responsabilidade pode ser maior ou menor - inclusive em caso de eventual incidente que exponha indevidamente os dados.

OPERADOR

- É toda pessoa física ou jurídica, pública ou privada, que realiza o tratamento de dados pessoais **EM NOME E SEGUNDO AS ORDENS** do controlador.

- **Obedece às medidas impostas** pelo controlador no tratamento de dados.

- **Guarda os registros** de acesso e tratamento de dados.

-**Apaga** de forma segura **ou devolve ao controlador** todos os dados pessoais que tenha acesso ao final do tratamento dos dados.

- Dá **apoio e suporte** ao controlador para que ele possa responder e adotar providências perante os órgãos reguladores e Judiciário.

CONTROLADOR

- É toda pessoa física ou jurídica, pública ou privada, **a quem compete as DECISÕES** referentes à finalidade e ao tratamento de dados pessoais.

- **Estabelece todas as medidas** que serão usadas no tratamento de dados – Isso inclusive, deve estar presente no contrato!

- **Guarda os registros** de acesso e tratamento de dados.

-**Conserva dados pessoais** que serão usados, conforme a finalidade, ou que sejam necessários para cumprimento de obrigações legais.

-Responsável por **responder e adotar as providências necessárias** perante os órgãos reguladores e ao Judiciário.

Toda essa relação será avaliada, se for o caso, pela ANPD, que é o órgão regulador do Estado que detém poderes de fiscalização e aplicação de sanções em relação a tratamentos de dados em desconformidade com a LGPD, assim como de estabelecer normas complementares relacionadas ao tema e diretrizes para a Política Nacional de Proteção de Dados Pessoais e de Privacidade.

No geral, a pessoa jurídica será a controladora, mas poderá contratar operadores para atuar em seu nome. Um operador é um agente externo à organização/negócio e que trata dados em seu nome, para as finalidades definidas pela organização/negócio. Por exemplo, se a organização/negócio fornece uma base de dados para uma empresa de publicidade, de modo que ela possa disparar e-mails convite para um evento realizado por ela, essa empresa será operadora dos dados.

ATENÇÃO!

Logo, os operadores não são pessoas subordinadas ao controlador, como funcionárias e colaboradoras da organização/negócio.

Sempre, que o operador tiver finalidades próprias de tratamento dos dados, por exemplo, se a empresa de publicidade utilizar os dados para enviar outros tipos de propaganda para os titulares de dados pessoais, ela será considerada controladora independente dos dados. Nesse contexto, ela deverá definir uma justificativa própria para o tratamento que deseja realizar.

É importante contar com a atenção especial aos contratos com provedores de produtos e serviços que tratam dados pessoais da organização/negócio. Aqui estão incluídos, por exemplo, serviços de publicidade, disparo de e-mails, tecnologia da informação, entre outros.

Para ajustar esse tipo de contrato é necessário entender:

Qual das partes da relação é responsável por definir a finalidade de utilização dos dados pessoais → de forma geral essa parte será a controladora e se as duas partes tiverem diferentes finalidades para o uso dos dados, ambas serão co-controladoras dos dados pessoais.

i. ***Exemplo***: duas organizações criam um aplicativo para mentoria de jovens. Uma delas utilizará os dados de quem se cadastra no aplicativo para finalidade de viabilizar a conexão do jovem com o seu mentor. A outra utilizará os dados para realizar uma pesquisa sobre o engajamento dos jovens em relação à busca pelo avanço profissional. Cada uma tratará os dados para uma finalidade diversa, por isso, elas podem ser consideradas co-controladoras dos dados.

Se uma das partes definir a finalidade de tratamento e contratar a outra parte apenas para viabilizar o atingimento deste objetivo definido por ela, essa parte que apenas opera os dados para o controlador é considerada operadora dos dados.

ii. ***Exemplo***: Uma organização/negócio contrata uma empresa de publicidade para realizar marketing a respeito de uma nova edição de seu curso sobre empreendedorismo social. Essa empresa de publicidade, só poderá utilizar os dados pessoais fornecidos pela organização/negócio para efetivar a comunicação em nome dela. Como ela não define outra finalidade para o uso dos dados ela é considerada operadora dos dados.

3.9.2 Cláusulas padrão de tratamento de dados pessoais:

Os contratos também deverão ser adaptados definindo as regras do jogo no que se refere a proteção de dados. Uma cláusula padrão de tratamento de dados pessoais pode conter os seguintes tópicos:

Reconhecimento pelas partes da existência de tratamento de dados pessoais na relação. Se possível devem ser expostos quais dados são tratados;

Quem são os agentes de tratamento de dados (quem é controlador, operador ou co-controlador), e quais as obrigações das partes a respeito das finalidades informadas ao(a) titular de notificação em caso de utilização dos dados para outros propósitos;

Com quem os dados podem ser compartilhados:

a. Obrigação de que o parceiro imponha a estes terceiros a mesma finalidade de uso dos dados e as mesmas proteções existentes para a relação inicial de tratamento.

b. Obrigação de que o parceiro se responsabilize pelas obrigações de tratamento de dados assumidas em face da organização/negócio mesmo se ele decidiu transferir os dados para tratamento de um terceiro;

Segurança e governança: necessidade de que o parceiro se comprometa a adotar medidas técnicas e organizacionais de segurança da informação e de governança aptas a proteger os dados pessoais.

Incidentes de proteção de dados: definição das responsabilidades no caso de incidente de tratamento de dados, de direito de regresso para reparação dos danos causados pelo incidente, do tempo para notificação da outra parte em relação ao incidente, etc.

Cooperação das partes para a resposta aos titulares e às autoridades legais e regulatórias e de reparação em caso de danos gerados a terceiros.

3.10 Capacitação periódica sobre proteção de dados e monitoramento da conformidade

A implementação da LGPD depende não só da criação de protocolos, do mapeamento, de um canal de comunicação com a organização e da nomeação de um o(a) encarregado(a) de proteção de dados, mas também da mudança de cultura em relação ao tratamento de dados.

O conhecimento sobre proteção de dados ainda é algo muito concentrado, de modo que as pessoas têm dificuldade de compreender exatamente do que estamos falando quando a estrutura de governança de dados é criada.

Assim, é importante promover capacitações periódicas sobre os conceitos, princípios, direitos e obrigações previstos na LGPD para que os colaboradores e prestadores de serviço possam entender o que devem proteger e como fazer isso.

A esses apontamentos podem ser acrescidas:

- a importância e a forma de reportar um incidente de segurança da informação dentro da organização;
- explicação da importância das políticas e do funcionamento da estrutura de proteção criada após o projeto de adequação à LGPD;
- a necessidade de diferenciar dados pessoais e pessoais sensíveis;
- a priorização pela coleta do menor número de dados possível para a construção de determinado projeto;
- a necessidade de dar transparência sobre as finalidades de uso dos dados para os titulares de dados que são interlocutores da organização;
- a importância de não utilizar dados captados para uma finalidade para outro propósito sem notificar o (a) encarregado(a) de dados pessoais da organização e os titulares de dados.

04

4. A APLICAÇÃO DE **SANÇÕES PELA ANPD**

Recentemente a Autoridade Nacional de Proteção de Dados publicou a regulamentação para a aplicação das sanções que a LGPD prevê em caso de violação às suas disposições. A Resolução nº 1, de outubro de 2021, está disponível aqui.

A Resolução regulamenta a aplicação do artigo 52 da LGPD, que traz as seguintes possibilidades de sanção:

> *Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)*
>
> *I - advertência, com indicação de prazo para adoção de medidas corretivas;*
>
> *II - multa simples, 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;*
>
> *III - multa diária, observado o limite total a que se refere o inciso II;*
>
> *IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;*

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - 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

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A LGPD é bem clara ao evidenciar que a aplicação das sanções deverá respeitar sempre a proporcionalidade com o dano causado pela conduta violadora da lei e, também o porte do agente de tratamento assim como outros aspectos como:

a. a gravidade e a natureza das infrações e dos direitos pessoais afetados;
b. a boa-fé do infrator;
c. a vantagem obtida ou pretendida pelo infrator
d. a condição econômica do infrator;
e. a repetição da violação;
f. o grau do dano;
g. a cooperação do infrator;
h. a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
i. a adoção de política de boas práticas e governança;
j. a pronta adoção de medidas corretivas;

Assim, a recente resolução da ANPD traz balizas mais concretas para a aplicação das sanções e regula como pode ocorrer o procedimento de fiscalização dos agentes de tratamento. Note-se que a regulamentação estabelece como deveres dos agentes regulados, ou seja, dos agentes de tratamento de dados:

a. O fornecimento da cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD;

b. A permissão do acesso às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de tratamento de dados pessoais, em seu poder ou em poder de terceiros;

c. Possibilitar que a ANPD tenha conhecimento dos sistemas de informação utilizados para tratamento de dados e informações, bem como de sua rastreabilidade, atualização e substituição, disponibilizando os dados e as informações oriundos destes instrumentos;

d. A submissão dos agentes às auditorias realizadas ou determinadas pela ANPD;

e. A manutenção dos documentos físicos ou digitais, dos dados e das informações durante os prazos estabelecidos na legislação e em regulamentação específica, bem como durante todo o prazo de tramitação de processos administrativos nos quais sejam necessários; e

f. A disponibilização, sempre que requisitado, de representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto.

O regulamento ainda traz disposições de ordem prática como definições sobre o que seja obstrução às atividades de regulamentação, as premissas que a ANPD seguirá para promover a fiscalização dos agentes de tratamento, prazos para resposta à notificação, o recebimento de requerimentos por parte dos titulares de dados, a atividade de orientação da ANPD, a atividade de ordem preventiva, da ANPD entre outros temas que não abordaremos aqui devido à sua extensão.

05

QUESTÕES POLÊMICAS: SOLUÇÕES INOVADORAS

5.1. Dados pessoais de crianças e adolescentes

Frequentemente as OSCs desenvolvem projetos cujo público-alvo são crianças e adolescentes. Apesar de a LGPD ter disposições específicas a respeito do tratamento de dados pessoais desse tipo de titular de dados no seu artigo 14, a verdade é que não há consenso sobre o consentimento de pessoas acima de 12 anos de idade. Explicamos:

A Lei Geral de Proteção de Dados traz o seguinte:

- O tratamento de dados de crianças e adolescentes deve ser realizado em seu melhor interesse;
- Os dados de **crianças** devem ser coletados e tratados com consentimento **específico e em destaque** dos seus pais ou pelo menos de um responsável legal;
- Os controladores devem manter pública, por exemplo em sua política de privacidade, quais dados de menores de idade ele trata e a sua utilização;

- Podem ser coletados de crianças sem o consentimento se eles forem necessários para contatar pais e responsáveis uma única vez, nesse caso, **em nenhuma hipótese podem ser repassados a terceiros sem o consentimento dos responsáveis;**
- O controlador deve empregar esforços razoáveis para verificar o consentimento dos pais das crianças;
- As informações sobre o tratamento de dados de crianças e adolescentes deve ser fornecida de modo adaptado às capacidades de percepção deste público. Vale desenhos, quadrinhos ou vídeos, para que a criança ou adolescente entenda o que está sendo feito com seus dados.

Acontece que a Lei Geral de Proteção de Dados deve ser interpretada em conjunto com as outras leis do nosso país. Dizemos isso porque, de acordo com o Estatuto da Criança e do Adolescente, são consideradas crianças as pessoas de até 12 anos incompletos. Ou seja, se considerarmos esta premissa do ECA, o consentimento dos responsáveis seria necessário somente para pessoas de 12 anos incompletos.

Há uma zona de dúvida no que se refere ao tratamento de dados de pessoas entre 12 e 18 anos. De acordo com o Código Civil, pessoas de 16 anos estão habilitadas para decidirem sobre alguns atos da vida civil. Isso significaria que podem consentir com o tratamento de seus dados? Se sim, poderíamos coletar o consentimento dos pais somente das pessoas menores de 16 anos? Deveríamos coletar consentimento de todos que forem menores de 18 anos?

A verdade é que esse é um dos temas mais debatidos da atualidade e a Autoridade Nacional de Proteção de Dados ainda não se manifestou para indicar o caminho interpretativo que deve ser seguido para estar em conformidade com a LGPD.

Organizações, como o Instituto Alana, que tratam da pauta dos direitos das crianças e adolescentes, colocam uma agenda importante de regulamentação responsável sobre esse tema. A compreensão da vulnerabilidade das crianças e adolescentes, em ambientes de coleta de dados pessoais está relacionada ao período de desenvolvimento físico-cognitivo, vivenciado por elas. Nesse período, elas não têm condições suficientes de compreender a complexidade dos fluxos de dados, as consequências e ameaças que o tratamento dos seus dados pessoais pode provocar futuramente.

Dessa forma, as pessoas menores de idade têm a sua capacidade de defesa dos abusos que podem ocorrer, por meio das atividades de tratamento de dados, reduzida. Nesse sentido, a ideia de que crianças e adolescentes teriam nascido e crescido em ambiente digital, e, por isso já teriam nascido com qualificação para dominar o ambiente digital seria exagerada. Segundo Isabella Henriques e Pedro Hartung, a coleta excessiva e o armazenamento inseguro de dados podem fazer com que crianças e adolescentes sejam mais facilmente contatados por pessoas mal-intencionadas, por meio dos seus dados pessoais expostos ou em tecnologias vulneráveis, o que apresenta perigo para sua integridade física, psíquica e moral. [5]

5 HENRIQUES, Isabella; PITA, Marina e HARTUNG, PEDRO. A Proteção de dados pessoais de crianças e adolescentes in. Tratado de proteção de dados pessoais. / coordenadores Danilo Doneda, Ingo Wolfgang Sarlet, Laura Schaertel Mendes e Otavio Luiz Rodrigues Junior [et al.]. – Rio de Janeiro: Forense, 2021.

É preciso reconhecer que a LGPD, no seu artigo 14, reforça a doutrina de priorização absoluta da proteção de crianças e adolescentes, exposta no artigo 227 da Constituição Federal. Isso porque o artigo 14 da LGPD, coloca em destaque a necessidade de respeito ao "melhor interesse" das crianças e adolescentes em toda e qualquer atividade de tratamento de dados pessoais deste tipo de titular. Assim, o principal fundamento para tratar os dados pessoais deste público seria a garantia de circunstâncias fáticas que efetivem o seu "melhor interesse".

Assim, sobre o tratamento de dados de adolescentes, entre 12 e 18 anos, para o qual a LGPD não expôs claramente se é necessário o consentimento parental ou não, o artigo 14 deve ser interpretado à luz da doutrina da proteção integral, estabelecida pela Constituição e pelo ECA (Estatuto da Criança e do Adolescente). Nesse sentido, para organizações como o Instituto Alana, não faria sentido excluir os adolescentes dessa necessidade de proteção integral, e, por isso deve-se recorrer ao Código Civil para promover os direitos desse grupo etário.

Este código, prevê que, até os 16 anos de idade, compete aos responsáveis legais dar assistência para os adolescentes, consentindo em seu nome. Assim, entende-se que o consentimento parental seria indispensável até os 16 anos de idade. Nesse sentido, para adolescentes entre 16 e 18 anos, seria necessário o consentimento de ambos, do adolescente e do responsável legal.

Isabella Henriques e Pedro Hartung destacam que o consentimento para o tratamento de dados pessoais de crianças e adolescentes é similar ao consentimento utilizado para o tratamento de dados pessoais sensíveis, ou seja, qualificado pelos adjetivos: informado, específico e destacado (Art. 11, I, da LGPD). Diante dessa similaridade de condições, os autores entendem que seria possível a aplicação das bases legais para o tratamento de dados pessoais sensíveis (Art., 11, II da LGPD) em se tratando de dados pessoais de crianças e adolescentes.

No caso da utilização de quaisquer outras bases legais, prevalece uma necessidade robustecida de conferir transparência de forma compreensível às crianças e adolescentes. Isso porque a LGPD, no art. 14 e §6º, expõe a necessidade de que a informação sobre o tratamento dos dados pessoais de crianças e adolescentes seja criada de forma a efetivamente permitir a compreensão de uma pessoa dessa idade sobre o tema. Nesse sentido, ao mencionar a necessidade de adequar a comunicação, é possível interpretar também a importância de efetivar a acessibilidade dessa comunicação, nos termos da Lei Brasileira de Inclusão da Pessoa com Deficiência - Lei 13.146/2015.

Do outro lado, a iniciativa privada, principalmente as redes sociais e plataformas como o YouTube se escoram na interpretação fria da lei, considerando a inexistência da menção expressa quanto à necessidade de consentimento dos pais ou responsáveis para tratar os dados pessoais de adolescentes. Assim, estabelecem que pessoas acima de 12 anos podem navegar e ter seus dados coletados, para as finalidades estabelecidas por esses agentes de tratamento, livremente, o que é amplamente criticado dentro do campo de defesa de direitos humanos de crianças e adolescentes.

Para analisar qual opção de interpretação pode ser adotada pela organização/negócio é preciso avaliar o caso concreto, a finalidade do uso dos dados das crianças, com quem eles serão compartilhados e se todo o tratamento está feito em respeito ao melhor interesse das pessoas menores de 18 anos. A doutrina do melhor interesse, prevista na Constituição, impõe a priorização absoluta da proteção das

crianças e adolescentes e é isso que deve guiar a decisão sobre o que será realizado para garantir o adequado tratamento de dados dessas crianças.

Uma boa saída pode ser a elaboração de um Relatório de Impacto, quando se opta pela utilização dos dados de crianças e adolescentes utilizando outras bases legais do artigo 11, ou seja, sem o consentimento dos seus responsáveis legais. Esse instrumento, previsto no artigo 38 da legislação, pode ser uma forma interessante de mitigar os riscos advindos da dificuldade ou impossibilidade de coleta do consentimento dos pais.

O Relatório de Impacto é um documento que registra a apuração dos riscos que a atividade poderia trazer para os titulares de dados e, principalmente, qual caminho escolhido pela entidade para mitigar esses riscos. Além disso, a elaboração do relatório é um exercício importante de entender se o tratamento de dados que se deseja implementar pode efetivamente colocar crianças e adolescentes em risco, de acordo com o fluxo de dados que será estabelecido dentro da atividade. Note-se que a análise de risco deve ter como referencial o(a) titular de dados, ou seja, deve-se levar em conta os riscos e impactos que a atividade de tratamento trará para os titulares de dados e não para a organização.

É um tema que deverá ser regulamentado com mais profundidade pela ANPD, nos próximos semestres, por isso, tomando por base as recomendações da Autoridade Inglesa de Proteção de Dados[6], entende-se que o relatório de impacto deve conter no mínimo: (i) descrever a natureza, escopo, contexto e finalidades do processamento; (ii) avaliar a necessidade, proporcionalidade e medidas de conformidade; (iii) identificar e avaliar riscos para indivíduos; e (iv) identificar quaisquer medidas adicionais para mitigar esses riscos (tradução livre). Nesse sentido, a autoridade francesa, CNIL, também atuou para criar um modelo de relatório e inclusive disponibiliza um software para auxiliar na produção deste documento.[7]

5.2. Uso de dados pessoais sensíveis em relatórios finais/prestações de contas de projetos

Para prestação de contas, normalmente são elaborados relatórios sobre o objeto, parcial ou final, para verificar o atingimento das metas estabelecidas para aquele projeto ou atividade, assim como para identificar o perfil das pessoas direta e/ou indiretamente impactadas pela ação proposta, seja para uso interno da OSC, como para envio a patrocinadores/financiadores ou utilização em material de divulgação.

Os relatórios de prestação de contas, com frequência, sistematizam dados pessoais sensíveis das pessoas impactadas pelo projeto, especialmente no que tange às especificações de raça, para verificação, dentre outros, dos níveis de diversidade atingidos.

6 Data protection impact assessments | ICO
7 Privacy Impact Assessment (PIA) | CNIL

Se fossem somente dados pessoais comuns, utilizados nos relatórios de prestação de contas, o tratamento de dados poderia ser fundamentado com a base legal do legítimo interesse de terceiro. Contudo, essa base legal não se aplica para tratamento de dados pessoais sensíveis.

Muitas vezes os dados pessoais sensíveis são tratados de forma anonimizada, ou seja, desvinculados do(a) titular de dados. Outras vezes são tratados de forma "pseudonimizada", ou seja, os controladores possuem um repositório que possibilita a reconexão dos dados com os seus titulares. Fato é que, mesmo espelhados nos relatórios de forma anonimizada, em gráficos, ilustrações, tabelas e/ou outros, muitas vezes o tratamento dos dados antes deste resultado é feito sem anonimização, ou podem ser exigidos sem anonimização por financiadores do projeto.

Considerando as bases legais para o tratamento de dados pessoais sensíveis, não há uma justificativa, além do consentimento, que pareça permitir o uso dos dados para essa finalidade, já que a legislação não permite utilizar o legítimo interesse ou a necessidade dos dados para a execução dos contratos como bases legais para tratamento de dados sensíveis, nos termos do artigo 11 da LGPD.

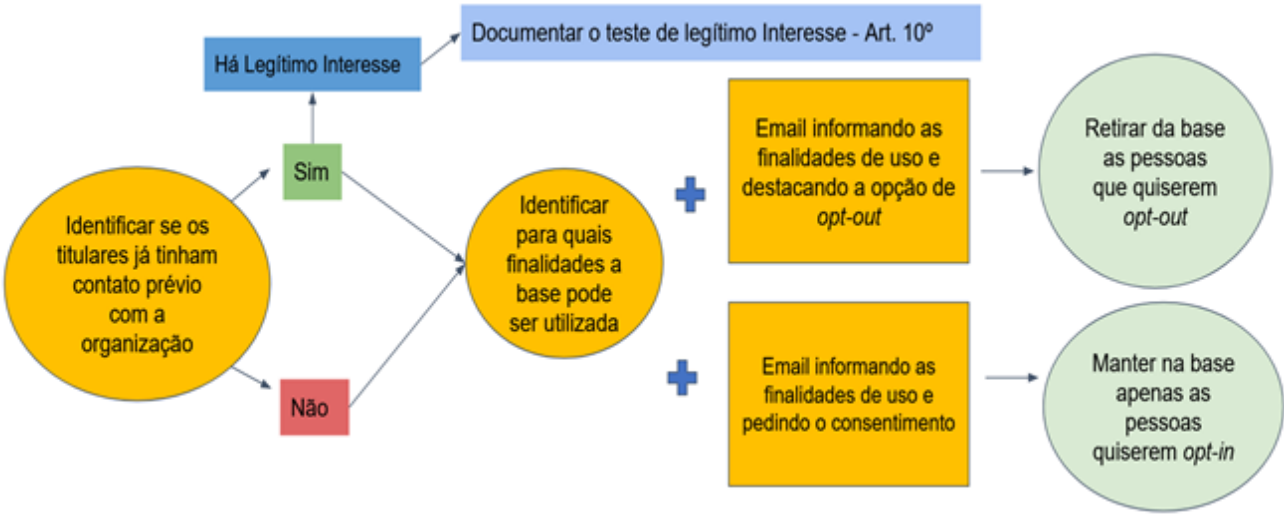
Assim é que para implementar políticas afirmativas das organizações e negócios de impacto, seria possível desenvolver no caso concreto uma justificativa utilizando-se a base legal da "obrigação legal regulatória" para tratar dados sensíveis como raça dos titulares. Isto porque diminuir as disparidades sociais é objetivo fundamental da Constituição brasileira, presente na redação do inciso III do artigo 3º.

Contudo, esta é uma matéria que envolve alguma polêmica e sobre a qual a ANPD ainda não se manifestou, razão pela qual, por hora, o ideal é coletar o consentimento, livre, expresso, informado e destacado do(a) titular para o uso para essa finalidade específica de tratamento, ou seja, o relatório final do projeto, de forma não anonimizada

5.3. Uso de bases de dados antigas

É comum querer aproveitar mailings construídos ao longo de anos, com base de dados antiga, por diversos motivos, desde o interesse em retomar o contato sobre seus projetos, seja para veicular suas ações, para verificar de que forma o impacto foi sentido a longo prazo, ou para convidar essas pessoas a integrar como voluntárias nas novas ações.

A LGPD não traz nenhuma regra específica que trate dos limites para que essa base seja utilizada depois do início de sua vigência. A lei apenas dispõe que a ANPD será a responsável em regular isso (artigo 63), o que, de fato, acaba por deixar um vácuo normativo acerca de como como essas informações podem ser utilizadas pela OSC para, por exemplo, inscrever antigas informações em mailings.



Nesse sentido, existem duas ações que podem ser tomadas dependendo se o(a) titular de dados possuía ou não uma relação anterior com a organização/negócio e, para facilitar a visualização dessas possibilidades, apresentamos o seguinte esquema:

Primeiro é preciso identificar que tipos de titulares de dados pessoais estão presentes nessa base de dados pessoais: são titulares que já tiveram algum contato com a organização ou não? Isso vai indicar a possibilidade de utilizar ou não do legítimo interesse como fundamento jurídico.

Em relação aos (às) titulares de dados pessoais que já possuíam contato com a organização, que já haviam participado de cursos, formações, ou outros eventos da organização é possível pressupor que havia interesse prévio dessas pessoas em receber as comunicações da organização.

Nesse sentido, para validar a base de e-mails, a ação indicada é enviar um e-mail com as finalidades para as quais os dados pessoais poderão ser utilizados, garantindo o reforço à mensagem de que as pessoas podem sair daquela base de dados se quiserem. Assim, quem não responder a essa comunicação, poderá ser mantido na base de dados por força da assunção de que as pessoas gostariam de estar ali desde o princípio, devido ao contato prévio que tinham com a organização.

A ação é diferente no caso de pessoas que não tinham qualquer contato com a organização que está em posse dos seus dados pessoais. Esse é o caso de organizações que compraram bases de dados ou que formaram bases de dados a partir de fontes públicas de dados pessoais, utilizados para pesquisa, por exemplo.

Nesse caso, não é possível pressupor que os(as) titulares de dados gostariam de estar na relação de tratamento e recebendo as comunicações da organização, dessa forma, seria preciso mais que garantir a opção de saída da base de dados, mas garantir que esses titulares de dados querem estar nessa relação, captando o seu consentimento para que eles permaneçam na base de dados da organização. Assim, quem não respondeu a comunicação demonstrando ativamente que deseja permanecer na base de dados, para as finalidades informadas pela organização, deve ser retirado dela.

5.4 Compartilhamento de dados com o Poder Público

As OSCs regularmente celebram parcerias com o Poder Público para o desenvolvimento de seus projetos e, por isso, recebem e precisam enviar informações ao Estado.

Em alguns casos as OSCs recebem muitas informações do Poder Público, para desenvolverem suas atividades junto à população que atendem em nome do Estado. Em outros casos, precisam enviar dados detalhados sobre o público beneficiado pela ação para prestar contas sobre a destinação do recurso público, inclusive em virtude da Lei de Acesso à Informação ("LAI"), o que inclui, por vezes, dados pessoais sensíveis, ainda que anonimizados, a depender das características do projeto.

É importante pontuar, que, em determinados contextos, a exigência de transparência pode expor demasiadamente os titulares de dados. Isso porque, esses titulares de dados podem ser de grupos sociais que sofrem algum tipo de perseguição estatal e a transparência em relação às suas informações deve ser calibrada, considerando-se o contexto social no qual eles estão inseridos, a garantia da sua proteção e o fato de que o fornecimento dos dados pode os vulnerabilizar ainda mais.

É necessário observar que a LGPD é clara ao informar que as transferências do Estado para entes privados só podem ocorrer em hipóteses específicas. Você sabe quais são?

- Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- Nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
- Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;
- Na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do(a) titular dos dados, desde que vedado o tratamento para outras finalidades.

Assim, é importante deixar claro, em acordos de cooperação e outros instrumentos contratuais em que o Estado está transferindo tais dados que essa transferência está legitimada pela LGPD. O ajuste é ainda mais importante se a organização estiver agindo em nome do Estado, como operadora de dados e não como controladora ou co-controladora. A esta altura é importante notar que, se ela for uma controladora conjunta, ou seja, se tiver finalidades para além da política pública, isso deve constar no acordo feito com o poder público e ela deve definir uma justificativa adequada para o tratamento dos dados para essas finalidades.

Além disso, para prescindir do consentimento do(a) titular de dados é possível utilizar a base legal da necessidade dos dados para a efetivação de políticas públicas. Mas como esta é uma base legal que só pode ser utilizada pela administração pública, é recomendável que conste expressamente no instrumento de contratualização a definição do uso dos dados com essa justificativa, pelo poder público.

Nesse sentido, a definição de um protocolo de tratamento de dados pessoais, que pode ser incluído nos Planos de Trabalho de Acordos de Cooperação, Termos de Fomento e Termos de Colaboração,

pode ser importante para regular a transferência de dados do Estado para o ambiente privado. Sugerimos que este tipo de Protocolo aborde os seguintes pontos :

1. Referência clara ao objeto da parceria que justifica a finalidade de uso dos dados;
2. Exposição exaustiva dos tipos de dados e as bases de dados que fundamentam o tratamento de dados por força da execução do objeto da parceria;
3. Identificação do Estado como controlador dos dados e da Organização como operadora ou co-controladora dos dados;
4. Identificação do uso da base legal de tratamento dos dados para a execução de políticas públicas, pela Administração Pública, para justificar a atividade de tratamento, a transferência ou o fornecimento do acesso aos dados, para entes privados;
5. Indicação da base legal utilizada pela OSC para justificar o tratamento dos dados, se a OSC atuar como co-controladora - ou seja, quando ela também pode definir finalidades próprias para o uso dos dados;
6. Identificação da exceção do artigo 26 da LGPD, que viabiliza essa transferência do Poder Público para o setor privado. Normalmente ela ocorre quando os dados já são publicamente acessíveis (Art. 26, §1º, III) ou quando a transferência está prevista em um contrato, convênio ou instrumentos similares (Art. 26, §1º, IV da LGPD);
7. Indicação clara da concordância do Poder Público com a transferência dos dados para eventuais prestadores de serviço que sejam operadores dos dados controlados pela organização, como, por exemplo: softwares, serviços de armazenamento, pesquisadores, consultores, analistas, empresas de TI, empresas de marketing, financiadores e etc.
8. Indicação clara da concordância do Poder Público com a transferência internacional dos dados, se ela existir (por exemplo se a organização tiver sede em outro país) ou fornecimento de uma alternativa para o tratamento dos dados em território nacional, por exemplo para a finalidade de armazenamento. Novamente, a justificativa de transferência internacional para a implementação de Políticas Públicas só pode ser utilizada pelo Estado, de forma que isso deve estar positivado no âmbito de um contrato com a administração pública;
9. Indicação quanto ao procedimento em relação à eliminação ou manutenção dos dados após o final da relação de parceria, principalmente, se eles podem ou não ser mantidos pela organização e sob qual justificativa;
10. O procedimento de notificação em caso de exercício de direitos por parte do(a) titular de dados ou de resposta à ANPD, em caso de fiscalização das atividades de tratamento de dados que ocorrem por força da parceria;
11. A exclusão de responsabilidade da organização caso o Poder Público não garanta a utilização dos resultados dela, de forma que não prejudique os titulares de dados, ou utilize os dados produzidos pela organização para outra finalidade, que não a da parceria;
12. A necessidade de cooperação para a resolução de incidentes de segurança que possam vir a afetar os titulares de dados pessoais beneficiários da parceria.

5.5 Contratação de microempresários individuais para prestação de serviços

Ainda que a LGPD tenha definido que a ANPD regulará sobre a simplificação dos procedimentos previstos na lei para aplicação das microempresas e empresas de pequeno porte (artigo 55-J, XVIII), até o momento em que se publica este material, isso não aconteceu.

A consequência é que quem frequentemente contrata microempresários individuais para prestar serviços ainda não têm um parâmetro específico de como o tratamento dos dados pessoais trocados com esses prestadores de serviços para o objeto da contratação deve se dar.

Está em aberto também se haveria limitação nesse compartilhamento em decorrência da natural precariedade da estrutura de governança de proteção de dados pessoais em microempresas e empresas de pequeno porte ante o alto custo envolvido para sua implantação e manutenção.

Nesse sentido, o ideal é tratar os dados de MEIs como dados pessoais, já que a conexão entre esse tipo de pessoa jurídica e o(a) titular é muito evidente

5.6 Direito de imagem e Propriedade Intelectual

Não raro, ações desenvolvidas pelas OSCs e Negócios de Impacto resultam no desenvolvimento de produtos como materiais gráficos ou audiovisuais, relatórios, livros, filmes, entre outros, sobre os quais incidem direito de imagem e aqueles direitos relativos à Propriedade Intelectual, como é o caso do direito autoral.

Tratando primeiramente do direito de imagem, este é um direito da personalidade, inerente a qualquer ser humano e que parte do pressuposto que todo indivíduo tem direito a controlar o uso e a aplicação de sua própria imagem e voz, autorizando ou não a captação, reprodução e/ou comercialização desses seus atributos individuais e distinguíveis.

Pessoas que têm suas imagens captadas em uma foto ou vídeo, para produção de conteúdo audiovisual, por exemplo, deverão assinar termos de autorização de uso de imagem e voz. Nesses documentos, da perspectiva da LGPD, é importante compreender que as feições do rosto e o som de voz dos titulares podem ser considerados dados pessoais e, portanto, o seu uso deve estar legitimado por uma das bases legais de tratamento de dados do art. 7º (se forem pessoas maiores de idade) e, do art. 11º (se forem crianças ou se, sabidamente, a parte para a qual os dados serão transferidos reunir capacidade tecnológica suficiente para identificar a biometria da face ou da voz dos titulares de dados).

Já quando discutimos a Propriedade Intelectual estamos falando de quem está na redação e na concepção dos projetos que OSCs e Negócios de Impacto desenvolvem. Dessa forma, a Propriedade Intelectual, notadamente o direito de autor, se presta a garantir que os autores de qualquer obra

tenham seus direitos reconhecidos e sejam recompensados por suas criações, ou que possam ceder, transferir e fruir desses direitos como bem entenderem.

Dessa forma, também é muito comum que OSCs e Negócios de Impacto se debrucem sobre as diretrizes da LGPD ao contratualizar sobre propriedade intelectual e direito autoral. Em primeiro lugar, é importante ter em mente que a lei não se aplica a finalidades artísticas. Logo, se no âmbito de uma criação artística, como um documentário ou peça de teatro, houver a utilização de dados pessoais, a LGPD não será aplicável. Mas, para que seja assim, é preciso que a finalidade seja estritamente artística, se a finalidade for desviada – como com publicidade, chamamento para curso, ou outras ações de engajamento – a lei será aplicada normalmente.

Já os dados pessoais tratados para atribuir a autoria de uma obra a seu autor, que é também titular de dados, está justificado pela necessidade de cumprir com a obrigação legal regulatória do art. 7°, II. Apesar de não ser obrigatória a coleta de consentimento, é boa prática de transparência indicar as bases legais utilizadas para tratamento dos dados e divulgação do nome do autor, dando a possibilidade de publicação anônima ou da utilização de pseudônimo, conforme direito moral do autor disposto no art. 24 da Lei de Direitos Autorais.

5.7 Transferência internacional de dados pessoais

Eventualmente as OSCs ou os Negócios de Impacto são financiados ou têm como parceiros em seus projetos OSCs, organizações internacionais e/ou empresas sediadas no exterior. Pode acontecer também de a representação de uma OSC internacional no Brasil vir a transferir dados para a matriz, baseada fora do país. São algumas das situações que já vivenciamos na prática.

A LGPD traz algumas hipóteses de justificação das transferências internacionais de dados. Contudo, em sua maioria, as justificativas dependem ainda da chancela da Autoridade Nacional de Proteção de Dados, que não se manifestou sobre o assunto.

Assim, mais seguro por hora é a interpretação de que as transferências são necessárias para cumprimento dos contratos e serviços prestados pelas organizações (art. 33, IX c/c art. 7º, V, da LGPD) quando sua sede está em outro país e, portanto, as nuvens de armazenamento.

Outra possibilidade, quando em parceria com o Poder Público, seria a afirmação de que as transferências são necessárias para as políticas públicas nas quais elas estão envolvidas (art. 33, VII, da LGPD). Conforme comentado no tópico 3.5. deste Guia, isso também é um ponto importante de estar previsto no acordo estabelecido com o poder público, pois somente a administração pública pode fazer uso desse tipo de justificativa.

No caso de pesquisas, por exemplo, nas quais há acordo com instituições de outros países, pode-se sustentar que há um acordo internacional ou global se houver acordos específicos dispondo sobre o tratamento de dados na pesquisa (art. 33, VI, da LGPD).

Por fim, a última possibilidade seria coletar o consentimento específico e em destaque dos titulares para essa finalidade (art. 33, VIII).

5.8 Uso de dados em relações trabalhistas

Para captar os dados necessários para a contratação, não é indicado utilizar o consentimento dos titulares como a base legal que fundamenta o tratamento de dados. Isso porque nesse tipo de relação, a disparidade de posições é tamanha, que o empregado, o(a) titular de dados, não estaria livre para não consentir com o tratamento de seus dados pelo empregador, uma vez que o próprio emprego depende disso.

Por isso, sugere-se o uso das seguintes bases legais:

- obrigação legal regulatória – para dados que a CLT ou outra regulação setorial obriga a captar como: Nome completo, data de nascimento, CPF, gênero, grau de instrução profissional ou escolar, endereço, descrição do cargo ou função ocupada, salario variável ou contratual conforme o caso, nome e dados dos dependentes, data de admissão no emprego, natureza da atividade (rural ou urbana), modalidade de contrato, matricula do empregado, categoria do trabalhador, código da CBO, horário de trabalho, local de trabalho, onde o trabalho é executado, se o funcionário é pessoa com deficiência, reabilitado ou não, data de opção pelo FGTS, informações relativas ao monitoramento da saúde do trabalhador, e informações sobre afastamentos por acidente ou doença[8].

- necessidade dos dados para o cumprimento do contrato – para dados captados em razão dos benefícios que a CLT não prevê, mas que a OSC ou NI (controladora) queira fornecer ao seu empregado (titular);

- legítimo interesse do agente de tratamento (apenas para dados pessoais não sensíveis) – para dados pessoais que sejam utilizados, por exemplo, para análise e devolutiva em relação ao trabalho do titular, para a garantia da segurança dos espaços da organização/negócio e etc. O uso dessa justificativa deve ser acompanhado pelo fornecimento de mecanismos eficientes de transparência e da documentação do teste de legítimo interesse, previsto no artigo 10º da LGPD;

- Consentimento – para dados sensíveis dos quais a contratação não dependa, como dados para a participação de políticas de diversidade que visam promover a seleção e progressão de carreira a partir desse tipo de critério.

Nesse caso, ainda é importante dar transparência ao funcionário sobre as finalidades para as quais os seus dados estariam sendo utilizados pela organização/negócio.

8 https://www.in.gov.br/en/web/dou/-/portaria-n-1.195-de-30-de-outubro-de-2019-224742577

5.9. Alteração de Estatuto Social

Para utilizar a base legal do artigo 7, inciso IV da LGPD recomendamos que a OSC de pesquisa tenha em seu estatuto como parte de seus objetivos sociais a pesquisa básica ou aplicada, de caráter histórico, científico, tecnológico ou estatístico. Desta forma, sugerimos adequar o estatuto para que nele exista a pesquisa como um dos objetivos e, assim, o uso desta justificativa seja adequado.

Para formalizar o Comitê de Proteção de Dados de maneira mais perene e transparente, pode ser interessante incluir como órgão oficial da sua governança no estatuto social da organização ou no contrato social do negócio de impacto. Isso gera também um processo formativo imediato dos(as) associados(as) ou sócios(as) que precisam entender os conceitos da lei e a responsabilidade que estão assumindo para decidir sobre a composição e atribuições.

5.10. Guarda de documentos

As atividades de tratamento de dados pessoais precisam de uma finalidade clara para existir, isso quer dizer que, quando o objetivo que motivou a coleta dos dados chega ao fim, estes devem ser eliminados ou anonimizados, é o que dizem os artigos 15º e 16º da LGPD:

Contudo, podem existir motivos legais para a manutenção dos dados, como, por exemplo, o dever de guarda de documentos, nos projetos realizados através das parcerias com a Administração Pública, reguladas pelo Marco Regulatório das Organizações da Sociedade Civil, que estabelece o prazo 10 anos após a entrega de prestação de contas final do projeto (art. 68º, parágrafo único, da Lei 13.019/2014).

Outro exemplo é a manutenção dos dados devido à possibilidade de exercício legal de direitos no âmbito de uma ação judicial, situação em que a manutenção dos dados deverá ocorrer pelo prazo de prescrição da ação que pode ser movida.

De toda forma, o que precisa ficar evidente, é a necessidade de ter uma finalidade para a manutenção dos dados e uma base legal (estabelecida no art. 7º ou 11º) que suporte o armazenamento, que não deixa de ser um tipo de tratamento de dados.

06

AGENDA REGULATÓRIA DA ANPD E A POSSIBILIDADE DE INCIDÊNCIA

Ainda há muitos temas em aberto que precisam de maior maturação regulatório-legislativa sobre proteção de dados pessoais, seja pela ANPD, seja pelo próprio Congresso Nacional.

No início de 2021, a ANPD divulgou em sua página a agenda regulatória que guiará seus trabalhos durante o biênio de 2021 e 2022, por meio da Portaria nº 11/2021. Nessa comunicação, encontram-se as ações regulatórias definidas como prioridade de atuação da ANPD nos próximos dois anos, o que proporciona a possibilidade de que organizações e negócios de impacto também se apropriem dos temas para estar presentes e contribuir com os espaços de debate sobre eles. Nesse sentido, a agenda regulatória da ANPD 2021/2022 envolve os seguintes assuntos:

SUMÁRIO

Proteção de dados pessoais e da privacidade para pequenas e médias empresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos

O tema da calibragem da aplicação da lei às possibilidades dos agentes de tratamento de pequeno porte já foi objeto de uma audiência pública, realizada nos dias 14 e 15 de setembro de 2021. Além disso a ANPD recebeu as contribuições escritas da sociedade civil até o dia 14 de outubro de 2021. O SBSA advogados contribuiu com a ANPD participando da audiência e por meio de texto escrito disponível em seu site para consulta pública.

Os direitos dos titulares de dados pessoais e como eles podem ser exercidos perante a ANPD e os agentes de tratamentos de dados;

O estabelecimento de normativos para aplicação das sanções administrativas que podem ser aplicadas pela ANPD e como isso deve ocorrer

Nesse caso, já foi emitida a norma específica que regulamenta o processo de fiscalização e aplicação de sanções por força dessa lei e ele pode ser conferido clicando aqui. O escritório SBSA participou da audiência pública e contribuiu para a consulta aberta pela ANPD por meio de texto em formato de nota técnica disponível no site para consulta pública.

Como comunicar incidentes de segurança e especificação do prazo para notificação

Já foi realizada uma primeira tomada de subsídios, abrindo a possibilidade para contribuição da sociedade civil para a construção de uma norma aderente às práticas de proteção de dados existentes no Brasil, a qual será objeto de debate por meio de audiência pública e consulta pública. Aqui você confere a contribuição do Data Privacy Brasil, que traz ponderações importantes sobre o tema e que pode servir para estruturar um bom Plano de Resposta à Incidente de Segurança.

A elaboração de relatório de impacto à proteção de dados pessoais

O Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) é um importante instrumento para prever e buscar medidas de mitigação de riscos que determinadas atividades de tratamento de dados podem trazer para os titulares de dados. Autoridades europeias têm lançado modelos de relatório para facilitar a produção deste registro e, aqui no

SUMÁRIO

Brasil, a ANPD promoveu três reuniões técnicas, nos dias 21, 23 e 25 de junho de 2021 para discutir o RIPDP. Ainda estão por vir uma audiência pública e uma consulta pública sobre a minuta de regulamentação, que será produzida pela ANPD a partir dos subsídios captados por ela no início do ano.

O(a) encarregado(a) de proteção de dados pessoais

A autoridade pretende regular, principalmente, quem deverá ou não indicar uma pessoa ou grupo de pessoas para endereçar as atribuições deste cargo. Esse tema já foi debatido na consulta pública da norma que visa regulamentar a aplicação da ANPD para agentes de pequeno porte e deve continuar sendo debatido até a consolidação de uma posição da autoridade sobre o tema. Recentemente o SBSA Advogados publicou um artigo falando sobre as possibilidades de arranjos para apontamento do o(a) encarregado(a) de proteção de dados pessoais pelas organizações da sociedade civil.

Transferência internacional de dados pessoais

A autoridade apontou a necessidade de se debruçar sobre o tema dos artigos 33 a 35 da LGPD, que indicam as possibilidades nas quais a transferência internacional de dados pode ocorrer de forma legítima. O tema é de suma importância para organizações e empresas que possuem sede ou que recebem financiamento de atores estrangeiros, os quais podem exigir a transferência internacional de dados a título de prestação de contas. Espera-se que a ANPD defina as diretrizes para a interpretação do que significa transferência internacional de dados e o conteúdo do que deve estar previsto em clausulas padrão contratuais, que podem servir para regular as salvaguardas que devem ser aplicadas nessa transferência.

Orientações sobre a aplicação das bases legais de tratamento de dados nos casos concreto

É expectativa da sociedade que haja posicionamento mais claro sobre os limites e condições para fundamentação do tratamento de pessoais utilizando-se as bases legais do Legítimo Interesse do agente de tratamento e da Proteção ao Crédito. Para além destes temas, no âmbito das atividades das Organizações Da Sociedade Civil, será importante buscar junto à ANPD e/ou o próprio Poder Judiciário o reconhecimento da possibilidade de tratamento de dados com fundamento na base legal de implementação de políticas públicas, sempre que estes tratamentos forem necessários para o desenvolvimento das atividades previstas nos Planos de Trabalho firmados por meio de parcerias e contratos junto à administração pública.

Como é possível ver, a ANPD está engajada na construção de interpretações sobre a LGPD em parceria com os agentes de tratamento de dados, o que demonstra a sua disponibilidade de calibrar a aplicação da lei por meio da permeabilidade às contribuições dos diferentes setores da sociedade sobre o assunto.

Assim, é importante que as Organizações da Sociedade Civil e os Negócios de Impacto, como agentes de tratamento, se mobilizem para participar dos momentos nos quais é aberto espaço para contribuição nos diversos temas elevados na agenda de atuação da ANPD para os próximos anos. Normalmente, a ANPD abre um espaço para contribuição escrita, na plataforma Participa + Brasil e, também, espaço para a manifestação oral, por meio de audiência pública sobre o tema que será regulado por ela.

Há ainda o Conselho Nacional de Proteção de Dados (CNPD), que se trata de um órgão consultivo da ANPD, composto por 23 membros da sociedade civil, representantes de diferentes setores da sociedade, e do poder público, e que tem como atribuições (nos termos do artigo 58, da LGPD):

> - Propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
>
> - Elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
>
> - Sugerir ações a serem realizadas pela ANPD; elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e
> - Disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

Esse órgão se reunirá três vezes ao ano ou quando for convocado pelo seu presidente. As organizações da sociedade civil com atuação comprovada em proteção de dados pessoais contam com 6 representantes (3 membros titulares e 3 suplentes): Rodrigo Badaró Almeida de Castro, Fabro Boaz Steibel, Bruno Ricardo Bioni, Maria Lumena Balaben Sampaio, Michele Nogueira Lima e Davis Souza Alves.

Vale destacar, conforme o artigo 50º da LGPD, o papel fundamental das associações, que poderão formular regras de boas práticas e governança para o seu próprio campo, de forma a auxiliar na calibragem da aplicação da lei às suas especificidades. Por exemplo, em 2017, a ICO, Autoridade Nacional de Proteção de Dados do Reino Unido, reconheceu publicamente a validade da interpretação do órgão independente que regula a captação de recursos por organizações sem fins lucrativos no Reino Unido (FR – Fundraising regulator),estabelecida no seu guia de captação de recursos em conformidade com a GDPR (*General Data Protection Regulation)*.

A Plataforma MROSC também seguirá antenada com o tema sob o ponto de vista regulatório do campo da sociedade civil organizada.

Esperamos que a Autoridade Nacional de Proteção de Dados siga as melhores práticas internacionais nas diversas áreas, incluindo o campo das Organizações da Sociedade Civil e dos Negócios de Impacto.

07

LINKS ÚTEIS

Lei Geral de Proteção de Dados

LGPD e terceiro setor: oportunidade de regulamentação mais adequada

LGPD e compliance: o encarregado de dados e o canal de denúncias nas organizações da sociedade civil

Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

Autoridade Nacional de Proteção de Dados

Marco Regulatório das Organizações da Sociedade Civil

Plataforma MROSC

Mapa das Organizações da Sociedade Civil

Proteção de dados de crianças e adolescentes

Justificativas de tratamento dos dados para além do consentimento

Operador e controlador

Guia da ANPD sobre segurança da informação para agentes de pequeno porte

A tutela coletiva na proteção de dados pessoais

Manual prático de implementação OSC

Manual prático de implementação MEI

Guia de boas práticas – Governo Federal

Civil Society Organizations and General Data Protection Regulation Compliance

PARA SE INFORMAR:

https://www.observatorioprivacidade.com.br/memorias/
https://www.internetlab.org.br/pt/
https://codingrights.medium.com/
https://irisbh.com.br/

GLOSSÁRIO

AGENTES DE TRATAMENTO DE DADOS: Termo que abrange os conceitos de controlador e operador de dados, sendo que o primeiro possui poder de decisão sobre as finalidades do tratamento de dados dos titulares, o segundo é aquele que realiza o tratamento de dados a partir das diretrizes do controlador, como prestadores de serviços e pessoas jurídicas que executam funções auxiliares.

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.

AUTORIDADE NACIONAL: É o órgão da administração pública federal, integrante da Presidência da República. Suas tarefas essenciais são fiscalizar e regular a aplicação da LGPD. A ideia é que esse órgão faça a ponte entre a sociedade e o governo, prestando um serviço aos cidadãos. A "ANPD" também terá um papel de orientar e apoiar governo e empresas em relação às situações em que o tratamento de dados é ou não permitido.

BANCO DE DADOS: Conjunto estruturado de dados pessoais, anonimizados ou pseudonimizados, localizado em um ou em vários locais, em suporte eletrônico ou físico.

BLOQUEIO: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

CAMPANHA DE ENGAJAMENTO CIVIL: Engajamento cívico ou participação cívica é o incentivo da população em geral para se envolver no processo político e as questões que a afetam.

COMPARTILHAMENTO DE DADOS: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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.

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

CONTEÚDO: Qualquer informação, dados, comunicações, software, fotos, vídeos, gráficos, música, sons e outros materiais e serviços que podem ser visualizados pelos usuários na plataforma. Isso inclui mensagens, conversas, bate-papo e outros conteúdos originais.

CONTROLADOR DE DADOS: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

COOKIES: São arquivos enviados pelo servidor e enviados para o computador do usuário, com a finalidade de identificar o computador ou celular e obter dados de acesso, permitindo, desta forma, personalizar o uso da plataforma de acordo com o comportamento do usuário.

DADOS MANIFESTAMENTE PÚBLICOS: as informações que podem ser utilizadas livremente, respeitados requisitos da legislação de proteção de dados, porque estão disponíveis nos portais de autoridades governamentais como a Receita Federal e os diversos Tribunais de Justiça.

DADOS PESSOAIS: informação relacionada a pessoa natural identificada ou identificável.

DADOS PESSOAIS ANONIMIZADOS: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

DADOS PESSOAIS SENSÍVEIS: 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.

ELIMINAÇÃO: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

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).

FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com esses propósitos.

INCIDENTE DE SEGURANÇA: O incidente pode ser compreendido como uma violação de segurança que provoca, de modo incidental e ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tratamento.

IP (Internet Protocol): É um conjunto de números que identifica o computador ou celular do usuário na Internet.

LEGÍTIMO INTERESSE: trata-se da justificativa mais flexível para o tratamento, e processamento, regular e legal de dados. O legítimo interesse do controlador de dados tem fundamento nas finalidades para as quais os dados são coletados, considerando as situações concretas em que isso será feito.

OPERADOR DE DADOS: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

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

TRATAMENTO DE DADOS: 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.”