# DPO (ENCARREGADO)

## Gestão dos programas de privacidade e proteção de dados

E-BOOK • AGOSTO 2021

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

# ÍNDICE

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF


Introdução 03

1 - Perspectivas para Gestão de Riscos de Privacidade e Proteção de Dados Pessoais 04

2 - Estratégias para manutenção constante do registro das operações de tratamento de dados pessoais 12

3 - Privacy by Design e Privacy by Default 16

4 - Opt-in e Opt-out: Quais são as diferenças? 23

5 - Legitimate Interest Assessment - LIA 26

6 - A importância dos direitos dos titulares 33

7 - Como gerir o direito à revogação do consentimento 38

8 - RIPD e sua importância nos programas de governança em privacidade 43

9 - Processo de Avaliação e Gestão de Terceiros 49

10 - A revisão de contratos à luz da LGPD 53

11 - Controle de Contratos 60

12 - Simulação de incidentes envolvendo dados pessoais 63

13 - Reavaliação contínua do nível de maturidade 70

14 - Plano de Treinamento e Comunicação 73

# INTRODUÇÃO

A LGPD (Lei Geral de Proteção de Dados) é uma legislação a ser seguida pelas organizações para o uso ético, seguro e responsável dos dados pessoais, que mitiga riscos de sanções e responsabilizações, gera maior competitividade, credibilidade e confiança.

Estar em conformidade com a LGPD é uma jornada contínua, que envolve não apenas um projeto de adequação à lei, mas, principalmente, a gestão eficiente do programa de privacidade e proteção de dados estabelecido. Esses esforços são necessários para assegurar que as organizações cumpram, de fato, as exigências legais.

Neste e-book, nossos advogados, em uma série de artigos, escrevem sobre os pontos de atenção que envolvem a gestão de um programa de privacidade e proteção de dados.

**Boa leitura!**

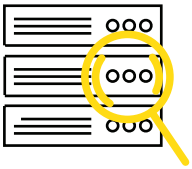
# Perspectivas para Gestão de Riscos de Privacidade e Proteção de Dados Pessoais

***Por Tiago Neves Furtado***

O risco pode ser definido como a possibilidade de perigo ou ameaça, ou como a probabilidade de prejuízo ou insucesso. Sob a perspectiva de gestão, o risco é o efeito das incertezas nos objetivos (Item 2 da Norma ABNT ISO 31000). No contexto da gestão de um programa de privacidade, o risco é a consequência de não atingir os objetivos trazidos pela Lei Geral de Proteção de Dados (LGPD).

Logo, para gerir o risco, é importante conhecer as consequências, pois são elas que trarão a ideia de impacto, ou seja, o que acontecerá caso não sejam cumpridas as regras da LGPD. Por outro lado, entender os objetivos da lei fará com que o gestor compreenda qual é a probabilidade desse risco se materializar.

Para os agentes de tratamento, as consequências estão definidas nas sanções da LGPD, no artigo 52, que são multas, advertência, publicização da infração, bloqueio ou eliminação de dados pessoais. Há também a consequência reputacional, essa, embora não esteja definida na lei, é ditada pela dinâmica social e cultural. Descumprir os objetivos da LGPD poderá prejudicar a imagem do agente de tratamento, que poderá perder clientes, parceiros e investidores.

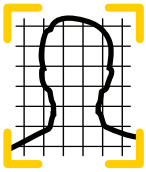


Para os titulares de dados, as consequências são outras e podem ser várias – desde um mero aborrecimento até perdas financeiras e consequências psicológicas sérias.

Por outro lado, os objetivos da LGPD estão traduzidos nos princípios, direitos dos titulares e demais obrigações da Lei. Contudo, a própria arquitetura da LGPD sugere uma avaliação constante em razão da sua abordagem de resultado.

Em verdade, a LGPD determina que essa proteção deve existir e delega a decisão do "o quê" e "como" para os agentes de tratamento, estabelecendo, ainda, que as medidas adotadas devem ser adequadas e eficazes, mas sem dizer quais parâmetros devem ser considerados para classificá-las dessa forma.

Essa perspectiva fica clara no artigo 50 da LGPD, que sugere aos agentes de tratamento a formulação de boas práticas e de governança para a garantia de que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os envolvidos no tratamento, as ações educativas, bem como os **mecanismos internos de supervisão e de mitigação de riscos** e outros aspectos do tratamento de dados pessoais.



Tratar dados pessoais é gerir risco a todo momento. É entender qual a consequência (impacto) de não se cumprir algum objetivo (probabilidade) da LGPD.

É bastante comum que se diga que o risco deve ser olhado sob a perspectiva do titular de dados, isto é, ao descumprir a Lei, a qual risco esse titular fica exposto e como fazer para mitigá-lo. Também é comum associar a análise de risco ao relatório de impacto.

Contudo, sob o aspecto de gestão, o risco deve e pode ser gerenciado sob perspectivas diferentes para alcançar esse mesmo fim, qual seja, proteger o tratamento de dados a partir do seu titular. Assim, é importante entender os riscos para o negócio (agentes) e para o titular de dados, como caminho adequado e eficaz para alcançar os objetivos da LGPD.

Podemos, então, dividir a avaliação e gestão de risco de um programa de privacidade em dois grandes blocos:

**riscos de governança, avaliados sob a perspectiva do agente de tratamento, caso ele não proteja o titular de dados de forma adequada e eficaz**

**riscos decorrentes das atividades de tratamento, nas quais o risco ao titular estará em primeiro plano**

E o que muda sob o aspecto de gestão? Em primeiro lugar, muda a identificação dos objetivos da LGPD que devem ser alcançados. Sob o aspecto de governança, busca-se entender quais são as obrigações institucionais do agente de tratamento, ou seja, quais estruturas e regras devem estar funcionando para garantir o cumprimento dos objetivos da LGPD.

Em segundo lugar, mudam as medidas de mitigação desse risco. Nos riscos de governança, as medidas são de estruturação institucional, como definição de comitê de privacidade, encarregado, políticas e procedimentos, cujos efeitos são mediatos. Já nos riscos decorrentes das operações em si, as medidas de conformidade terão efeito imediato em relação ao titular dos dados, pois mudam a forma como a atividade é desenvolvida (minimização de dados, reforço de transparência etc).

Consequentemente, com alteração de objetivos e medidas mitigadoras, mudam-se também os indicadores e a própria metodologia de avaliação de resultado. No caso dos riscos de governança, o que se mede é maturidade dos agentes de tratamento, ou seja, o comportamento e a aderência da organização às regras e às estruturas criadas. No caso dos riscos decorrentes das operações de tratamento, o que se mede é a efetividade da proteção em um contexto específico.

Para facilitar essa percepção, podemos resumir essas conclusões iniciais a partir da tabela abaixo.

| **Risco de Governança** | **Risco decorrente das atividades de tratamento** |
|---|---|
| Perspectiva: quais as consequências para o agente de tratamento? | Perspectiva: quais as consequências para o titular de dados? |
| Impacto: penalidades da LGPD e reputação. | Impacto: danos morais, fraudes, prejuízos financeiros etc. |
| Probabilidade (objetivos): quais são as obrigações institucionais do agente de tratamento, ou seja, quais estruturas e regras o agente deve ter para garantir o cumprimento dos objetivos da LGPD. Não as ter aumenta a probabilidade de materialização do risco. | Probabilidade (objetivos): o que deve ser ajustado para que a atividade de tratamento não viole os objetivos da LGPD. Não fazer isso aumenta a probabilidade de implementação do risco. |

| Risco de Governança | Risco decorrente das atividades de tratamento |
| --- | --- |
| Medidas mitigadoras: institucionais, de efeito mediato. | Medidas mitigadoras: alteram a atividade de tratamento de dados pessoais, de efeito imediato. |
| Indicadores: mede-se a maturidade do agente de tratamento para cumprimento das regras. | Indicadores: mede-se a efetividade da proteção de dados em um contexto específico. |
| Ferramentas de medição: auditoria interna e externa, acompanhamento de metas e métricas pelo DPO/Encarregado. | Ferramentas de medição: Relatórios de Impacto, Procedimento de *Privacy by Design* e/ou *Security by Design*, análise de risco mesmo após a concepção de produto ou serviço, análise do registro de atividades de mapeamento etc. |
| Objetivo: Proteger os dados pessoais e seus titulares a partir dos objetivos da LGPD. | Objetivo: Proteger os dados pessoais e seus titulares a partir dos objetivos da LGPD. |

Apenas para ilustrar a diferença prática dessa abordagem, seguem abaixo alguns exemplos de risco e medidas mitigadoras no contexto de gestão do programa de privacidade considerando essas duas perspectivas.

## Riscos de governança e medidas mitigadoras

| Parâmetro LGPD | Risco | Medida Mitigadora (exemplos não exaustivos) |
|---|---|---|
| Gestão e Governança | Risco de não obter o engajamento dos principais stakeholders internos. | Formalização da nomeação do encarregado e comitê de privacidade. |
| Manuseio de Dados pessoais | Risco de coletar, utilizar ou armazenar dados pessoais em desconformidade com a finalidade informada ao titular do dado. | Criar políticas internas que enderecem o tema consistentemente.<br>Definir indicadores para acompanhar o cumprimento da política. |
| Transparência | Risco de não apresentar o Aviso de Privacidade no momento de coleta do dado do titular. | Mapear os pontos de coleta de dados na organização. |
| Gestão do Consentimento | Risco de não tratar os dados conforme o consentimento do titular do dado. | Ausência de regras específicas para gestão e uso do consentimento. |
| Direito dos Titulares | Risco de não garantir o exercício de direitos aos titulares dos dados. | Não possui processo definido para atender às requisições feitas por titulares de dados. |

| Parâmetro LGPD | Risco | Medida Mitigadora (exemplos não exaustivos) |
|---|---|---|
| Compartilhamento | Risco de os terceiros tratarem indevidamente dados transferidos. | Existência de diligência prévia e auditorias em terceiros que tratarão dados pessoais e revisão das minutas contratuais. |
| Segurança da Informação | Risco de não serem aplicados os controles de segurança devidos, em relação aos dados pessoais. | Inexistência de processos de *security by design*. |
| Resposta a incidentes | Risco de não responder de maneira apropriada aos incidentes de violação de dados pessoais. | Formalizar um plano de resposta a incidentes. |

**Risco decorrentes da atividade de tratamento de dados pessoais e medidas mitigadoras**

| Parâmetro LGPD | Risco | Medida Mitigadora (exemplos não exaustivos) |
|---|---|---|
| Princípio da Necessidade e Adequação. | Risco de tratar dados em excesso, expondo a privacidade do titular de maneira desnecessária. | Anonimização dos dados pessoais na operação. |

| Parâmetro LGPD | Risco | Medida Mitigadora (exemplos não exaustivos) |
|---|---|---|
| Princípio da Transparência | Risco de o titular ter seu direito de conhecer o que é feito com suas informações violado. | Implementar linguagem simplificada e *Visual Law* nos avisos de privacidade. |
| Princípio da Segurança | Risco de os dados pessoais serem acessados por quem não tem esse direito. | Implementação de ferramentas de SI (como DLP, política de acesso, criptografia). |

Por fim, o mais importante é que, para garantir total aderência aos objetivos da LGPD, o monitoramento dos riscos sob as perspectivas de governança e das próprias atividades de tratamento de dados pessoais é fundamental e imprescindível. Cabe, portanto, ao DPO/Encarregado incluir nas suas funções atividades que consigam avaliar os riscos sob esses dois prismas tão distintos, por meio de abordagem, metodologia e métricas específicas.

***Tiago Neves Furtado***
Professor e advogado, gestor da equipe de Privacidade e Proteção de Dados do Opice Blum, Bruno e Vainzof Advogados Associados.

# Estratégias para manutenção constante do registro das operações de tratamento de dados pessoais

***Por Henrique Fabretti Moraes***

A construção do registro das operações de tratamento de dados pessoais, ou mapa de dados, é usualmente o primeiro passo adotado pelas organizações que buscam estar em conformidade com a Lei Geral de Proteção de Dados (LGPD)[1], uma vez que, além de ser expressamente exigido nos termos do seu artigo 37, permite uma visão ampla sobre quais são as atividades que envolvem o tratamento de dados pessoais, servindo como ponto de partida para outras ações necessárias à construção de um programa de privacidade.

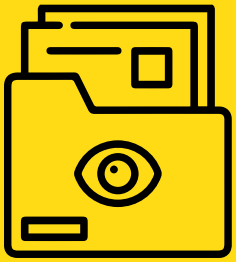
Além disso, o registro das operações de tratamento "é fundamental para guiar o encarregado em suas atividades, indicando onde estão presentes os maiores riscos, bases legais para o tratamento de dados com maior chance de questionamento pelas autoridades, compartilhamento de dados com terceiros etc."[2], funcionando como verdadeira bússola na condução das atividades de gestão do programa de privacidade.

Portanto, possuir um mapa de dados atualizado é um dos pilares mais importantes para que o programa de privacidade seja eficiente em seu propósito de assegurar a conformidade da organização com a Lei Geral de Proteção de Dados.

[1]FURTADO, Tiago Neves. Registro das Operações de Tratamento de Dados Pessoais – Data Mapping – Data Discovery: Por que é Importante e Como Executá-lo. In: OPICE BLUM, Renato; VAINZOF, Rony; MORAES, Henrique Fabretti. Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1ª Edição – São Paulo: Thomson Reuters Brasil, 2020. P. 85.

[2]VAINZOF, Rony; MORAES, Henrique Fabretti. As qualificações e os desafios do encarregado pelo tratamento de dados pessoais no setor privado. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. A Lei Geral de Proteção de Dados Pessoais: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado. 1ª Edição – São Paulo: Thomson Reuters Brasil, 2021. P. 724.

Ocorre que manter esse documento devidamente atualizado pode representar um grande desafio, uma vez que a dinâmica das organizações faz com que as atividades de tratamento sofram constantes mutações, seja no tipo dos dados ou dos titulares envolvidos na operação, na finalidade do tratamento, no tempo de armazenamento ou até com o surgimento de operações completamente novas.



Para tentar endereçar esse desafio, vamos apresentar aqui uma estratégia simples, composta de dois processos a serem utilizados concomitantemente, e que não exige grandes investimentos ou apresenta complexidade operacional.

A primeira objetiva capturar as alterações nas atividades de tratamento da organização tão logo elas aconteçam, preferencialmente integrando esse processo nas medidas de privacy by design. Vale lembrar que direcionar o negócio na adoção de medidas de conformidade com as regras de privacidade e segurança desde os primeiros passos da criação de atividades de tratamento de dados costuma ser uma atividade inerente ao time de privacidade das organizações[3] e conta com previsão expressa no artigo 46, §2º, da LGPD[4].

[3] Conforme indicando no Annual Privacy Governance Report 2020, mais de 80% dos times de privacidade possuem como uma de suas atribuições a implementação de medidas de *privacy by design* no desenvolvimento de produtos.

[4] 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Nessa linha, é possível definir um processo interno, aplicável a todos os colaboradores ou, a depender do tamanho e da intensidade com que atividades de tratamento são criadas, a áreas específicas da organização, estipulando que o responsável por essa nova operação de tratamento deve reportá-la ao encarregado.

Independentemente do meio pelo qual esse reporte é realizado, a partir da comunicação de que uma atividade está sendo criada, é possível não só aplicar os preceitos do *framework de privacy by design,* como também utilizar o mesmo processo para alimentar o mapa de dados da organização.

Para que esse processo seja efetivo, além de ampla divulgação, especialmente aos colaboradores envolvidos na criação de produtos, processos internos, práticas de negócio etc, é necessário que a definição do responsável por realizar o reporte seja clara, e que o mecanismo de reporte seja simples e intuitivo. Vale lembrar que quanto mais complexo e extenso for o relatório exigido das áreas de negócio, maior será a dificuldade de receber essas informações, portanto, para organizações que ainda estão trilhando seus primeiros passos no programa de privacidade, o ideal é exigir um mínimo de informações, deixando com o encarregado a tarefa de complementar os dados que forem necessários.

O segundo processo que pode ser implementado, complementar ao anterior, é a revisão completa do mapa de dados, possibilitando a identificação de atividades que, por algum lapso, não tenham sido reportadas anteriormente.

Considerando o elevado gasto de tempo e engajamento necessários para realizar uma revisão de todo o mapa de dados da organização, é possível dividir essa atividade em algumas etapas, iniciando a revisão por áreas específicas da organização, de acordo com o grau de criticidade que suas atividades de tratamento representam.

Para tanto, pode-se olhar para o mapa de dados já existente e classificar a criticidade dessas áreas, utilizando critérios como volume de operações de tratamento, natureza dos titulares impactados, tipos de dado tratados, bases legais utilizadas, compartilhamento ou não de dados com terceiros, entre outras características, e, a partir dessa avaliação, priorizar aquelas que denotam maior risco, seja do ponto de vista do titular, seja da própria organização.

Assim, não é necessário engajar todas as áreas da organização de uma vez e é possível definir periodicidade de revisão menor para áreas mais críticas e maior para as de menor criticidade – por exemplo, a cada seis meses para áreas mais críticas e dezoito meses para as demais.

Independentemente do método adotado, recomenda-se que o encarregado inclua em seu planejamento de longo prazo a revisão contínua do registro das operações de tratamento de dados pessoais, assegurando uma gestão eficiente, orientada a riscos, do programa de privacidade.

***Henrique Fabretti Moraes***
Advogado e gestor da área de Privacidade e Proteção de Dados do Opice Blum, Bruno e Vainzof Advogados Associados.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

# Privacy by Design e Privacy by Default

***Por Marcella Costa e Ana Catarina de Alencar***

"*Privacy by design*" ou "privacidade desde a concepção" consiste em um conceito desenvolvido na década de 1990 pela Dra. Ann Cavoukian, Comissária de Informação e Privacidade de Ontário, no Canadá[1], para contemplar sua inquietação com os efeitos que poderiam emergir a partir da combinação entre avanço da tecnologia e utilização massiva de dados pessoais pelas empresas. Para ela, o futuro da privacidade não poderia depender apenas de leis e regulações, era preciso incorporar essa preocupação à arquitetura dos sistemas e das funcionalidades, provocando uma mudança nas práticas de negócios, na forma padrão de desenvolvimento, bem como na criação de produtos e serviços pelas empresas.

E foi com a publicação dos 7 princípios norteadores do *Privacy by Design*, em 2009[2], que Ann Cavoukian conseguiu consolidar esse conceito na doutrina e na legislação. Em 2010, na 32ª Conferência Internacional de Comissários de Privacidade e Autoridade de Proteção de Dados[3], o Privacy by Design foi reconhecido como "componente essencial da proteção fundamental da privacidade".

[1]Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf Acesso em 11/05/2021.
[2]https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf Acesso em 31/03/21.
[3]https://edps.europa.eu/sites/edp/files/publication/10-10-27_-jerusalem_resolutionon_privacybydesign_en.pdf Acesso em 31/03/21.

Atualmente, o conceito está previsto no artigo 25 do General Data Protection Regulation (GDPR) e também se encontra presente ao longo dos princípios[4] invocados pela Lei Geral de Proteção de Dados (LGPD), bem como de forma expressa em seu artigo 46, §2.[5]

Destacamos abaixo os **7 princípios** do conceito "*Privacy by Design*".

1. **Proativo e não reativo - ser preventivo e não corretivo:** empresas devem adotar uma abordagem proativa na prevenção de riscos e não na sua remediação.

2. **Privacidade como configuração padrão:** empresas devem projetar seus sistemas, serviços e produtos com proteção automática dos dados pessoais de titulares. O titular não deve ter de realizar ajustes ou tomar providências para garantir a sua privacidade na utilização dos serviços.

3. **Privacidade incorporada ao design:** empresas devem incorporar a proteção de dados pessoais ao design dos seus sistemas e soluções desde a sua formulação mais inicial. Logo, o conceito de privacidade deve constituir uma parte essencial dos serviços e produtos oferecidos.

[4] Neste sentido, podem ser citados os princípios previstos no artigo 6º da LGPD, em especial, o princípio da finalidade (I), da adequação (II), da necessidade (III), da transparência (VI), da segurança (VII), da prevenção (VIII), entre outros.

[5] "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". (grifos nossos).

**4** **Funcionalidade total - soma positiva e não soma igual a zero:** empresas devem evitar "trocas" inadequadas para cumprir com as normas de privacidade. Em outras palavras, deve-se evitar a crença de que é necessário abrir mão da segurança, por exemplo, para coletar mais dados pessoais e atingir os objetivos comerciais do negócio. A equação da privacidade deve ser sempre marcada por um jogo de "ganha-ganha" ("*win-win game*") e não por um jogo de soma zero.

**5** **Segurança de ponta a ponta - proteção durante todo o ciclo de vida:** empresas devem implementar medidas de segurança suficientes, desde a formulação do produto ou serviço até o final do ciclo de vida dos dados pessoais.

**6** **Visibilidade e transparência:** empresas devem se certificar de que suas práticas comerciais e sistemas operam de acordo com os princípios aplicáveis e sejam verificáveis de forma independente. Além disso, é preciso garantir visibilidade e transparência sobre as finalidades para as quais os dados pessoais dos titulares são processados.

**7** **Respeito pela privacidade do usuário - serviço centrado no usuário:** empresas devem considerar os interesses dos titulares em primeiro lugar no oferecimento de seus produtos ou serviços, garantindo salvaguardas aos seus direitos e liberdades fundamentais.[6]

---

[6] Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd8. Acesso em 11/05/2021.

Feita essa breve introdução, podemos afirmar que o "*Privacy by Design*" representa uma mudança no modo de garantir a privacidade e a proteção de direitos e liberdades dos indivíduos, já que é pensado e incorporado às práticas de negócio antecipadamente, ou seja, desde o momento inicial quando são concebidos os processos produtivos, procedimentos e mecanismos internos do processamento de dados pessoais por Controladores, Operadores e terceiros. Mas, para que isso se concretize na prática, a proteção da privacidade e dos dados pessoais precisa se tornar um valor para a empresa e suas lideranças, a ser disseminado por meio das estruturas de governança e de medidas traçadas nos programas de *compliance*.

Não bastam políticas com vocabulário rebuscado, essa preocupação deve se tornar premissa básica na fase de formulação dos sistemas, projetos, serviços ou produtos da empresa, abarcando o desenvolvimento de sistemas, processos, estratégias e salvaguardas que (i) impliquem em aumento da proteção jurídica e da segurança da informação para os dados pessoais; (ii) possibilitem ao indivíduo um maior controle sobre seus dados e, consequentemente, (iii) propiciem um ambiente de negócios mais seguro, ético e sustentável.

Por conseguinte, além de uma prática consagrada internacionalmente, o "*Privacy by Design*" representa um reforço importante para os Encarregados ou DPOs (*Data Protection Officers*) na busca pela implementação do valor da privacidade nas ferramentas de *compliance*, de modo a efetivamente contribuir para o atendimento dos requisitos da lei, dos direitos dos titulares e para a garantia da proteção dos dados pessoais.

Assim, é papel do DPO direcionar ações orientadas por esse conceito na própria estrutura de governança da empresa, envolvendo todas as partes interessadas. Desse modo, a incorporação de estratégias de privacidade no negócio poderá ser atingida mais facilmente, tendo em vista que representará um componente essencial da própria estrutura de governança interna.

Como exemplos das ações direcionadas pelo DPO na incorporação do "*Privacy by Design*" na estrutura interna, podemos citar, principalmente:

I a determinação de políticas claras e auditáveis;
II a revisão das finalidades e formas de processamento dos dados nas atividades de tratamento;
III a avaliação dos riscos aos direitos dos titulares de dados;
IV a adoção do critério de minimização dos dados pessoais e ações de transparência, bem como a revisão e o monitoramento contínuo das estratégias de "*Privacy by Design*".

Adicionalmente, importante destacar que deverá ser levado em conta, além dos 7 princípios que integram esse conceito, as variáveis do próprio negócio em avaliação, uma vez que não há fórmula única, tais como:

I modelo de negócios;

II setor produtivo;

III porte da empresa;

IV existência de controles de governança;

V nível de engajamento dos atores envolvidos; e

VI cultura da empresa.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

Nessa perspectiva, algumas reflexões sobre as premissas do negócio também devem ser realizadas, incluindo os seguintes aspectos:

**I** a proteção de dados pessoais é considerada como parte integrante do negócio, dos serviços, produtos ou práticas comerciais da empresa?

**II** a proteção de dados é tida como um componente essencial da funcionalidade dos sistemas e das soluções da empresa?

**III** riscos e potenciais incidentes são antecipados pela empresa antes que ocorram?

**IV** são tomadas medidas efetivas para prevenir danos aos direitos de titulares?[7]

Por fim, fundamental que a adoção do "*Privacy by Design*" seja acompanhada de uma segunda abordagem denominada "*Privacy by Default*" ou "privacidade por padrão", a qual decorre da primeira e consiste na ideia de que empresas garantam:

**I** o processamento de dados pessoais apenas na medida do estritamente necessário para atingir uma finalidade específica; e

**II** a proteção da privacidade de forma automática no momento da coleta de dados pessoais por algum sistema de tecnologia ou prática de negócio, sem que seja necessária qualquer manifestação da vontade ou intervenção do indivíduo.

[7] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Essa perspectiva complementar tem como base os princípios da minimização e da finalidade, previstos no GDPR e na própria LGPD. Logo, proteger os dados pessoais "por padrão" significa que o agente de tratamento configura e especifica quais dados pessoais serão processados antes do início do tratamento, objetivando garantir de forma automática o mais alto nível de proteção da privacidade e conferindo visibilidade adequada ao titular. Assim, o "*Privacy by Design*" e o "*Privacy by Default*" são perspectivas relacionadas e devem ser implementados sobre os aspectos mais críticos e relevantes das atividades de tratamento.

Em suma, com a metodologia implementada e operante na estrutura do negócio, além de cumprir a legislação e mitigar os riscos verificados, a empresa se posiciona de forma competitiva e ética no mercado. Nesta linha, o zelo pelas melhores práticas em privacidade deve ser também um modelo de atuação organizacional da empresa, fortalecendo a confiança de seus consumidores a partir de serviços que são formulados para sua proteção desde a concepção inicial.

***Marcella Costa***

Gestora da área Startup.OBA no Opice Blum, Bruno e Vainzof Advogados Associados. Graduada pelo Instituto Presbiteriano Mackenzie, cursou Master in Law – LLM em Direito Societário, no Insper, Programação de Smart Contracts em Blockchain, na PUC/SP e Estratégias Societárias, Planejamento Tributário e Sucessório, na FGV. Pós-graduanda em Direito Digital na Escopa Paulista de Direito – EPD, certificada em Privacy and Data Protection Essentials pela Exin ICT e autora de capítulo no livro "Data Protection Officer: Teoria e Prática de Acordo com a LGPD e o GDPR" e na Revista Criptomoedas e Blockchain Descomplicadas para Advogados. Membro do Comitê de Startups da FECOMERCIO e da Comissão de Startups da OAB/SP.

***Ana Catarina de Alencar***

Advogada na área Startup.OBA no Opice Blum, Bruno e Vainzof Advogados Associados. Mestre em Teoria do Direito e Filosofia do Direito pela Universidade Federal de Santa Catarina (UFSC). Especialista em Direito Digital e Compliance. Colunista nas áreas de Direito, Inovação e Inteligência Artificial. Professora no curso de graduação em Direito da Unisociesc/Anima. Membra do Conselho Editorial da Revista da OAB/Joinville.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

# Opt-in e Opt-out: Quais são as diferenças?

***Por Renato Opice Blum e Guilherme Guimarães Vieira***

Nos últimos anos, os países europeus divergiram a respeito do opt-in e do opt-out, ou seja, houve discussão se o titular dos dados pessoais deveria consentir de maneira prévia e expressa, aceitando, por exemplo, cada cookie a ser instalado para a coleta dos seus dados de navegação (opt-in) ou se essa seria uma escolha a posteriori e que poderia ser extraída implicitamente por meio das configurações dos browsers (opt-out).

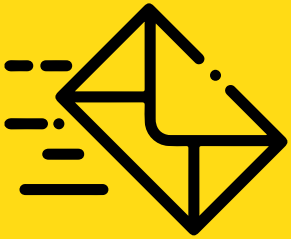
A possibilidade de uma empresa oferecer aos seus clientes o descadastramento no sistema operacional e no banco de dados chama-se "opt-out". O termo em inglês sugere a "saída" consciente e requerida pelo cliente por meio de um canal de comunicação com a empresa. Dessa forma, essa prática respeita a vontade do cliente, garantindo uma boa imagem corporativa.

Nota-se que o mercado está cada vez mais conectado com os clientes em diversas frentes, e, por isso, em algumas oportunidades, torna-se excessivo o número de comunicações promocionais, de lançamentos de produtos, de feedbacks de serviços e produtos, o que resulta em uma desproporcional relação informativa.

Por meio do opt-out, a empresa oferece a possibilidade do descadastramento no e-mail marketing, por exemplo, permitindo que seu público desautorize o envio de novos conteúdos e materiais a partir daquele momento de saída.

De forma geral, o objetivo das empresas com as comunicações é identificar as preferências dos usuários, bem como seus hábitos de consumo. Nesse processo, portanto, os mecanismos de opt-out são primordiais para o bom relacionamento com o cliente, objetivando manter uma relação de longo prazo. Nada adianta inclusive contar com um campo de opt-out se este trouxer dificuldades para o cliente. Por esse motivo, o link deve ser de fácil visibilidade, permitindo que a experiência seja simples e prática.

Usualmente, os pontos mais fáceis de visualização pelo público são início do e-mail e assinatura. E tem mais: é importante manter organizada a relação dos clientes que não querem mais o relacionamento informacional. Para isso, é suficiente uma planilha com as datas dos pedidos de retirada (opt-out).



Há, ainda, mecanismos de opt-out que devem ser incorporados ao site das empresas com a intenção de promover o ágil, seguro e confiável descadastramento do usuário. O mais eficiente deles é feito por meio da utilização de link, que também pode direcionar o cliente para a página de cadastro, onde ele vai atualizar suas informações ou retirar seu contato.

Além disso, os métodos off-line, como SMS, telefone celular e telefone fixo com atendente, podem ser empregados, porém não são os melhores. Isso porque, por causa da descentralização própria desses métodos, há mais chances de dispersão das informações internamente na empresa, o que traz desvantagens e aborrecimentos posteriores para os clientes.

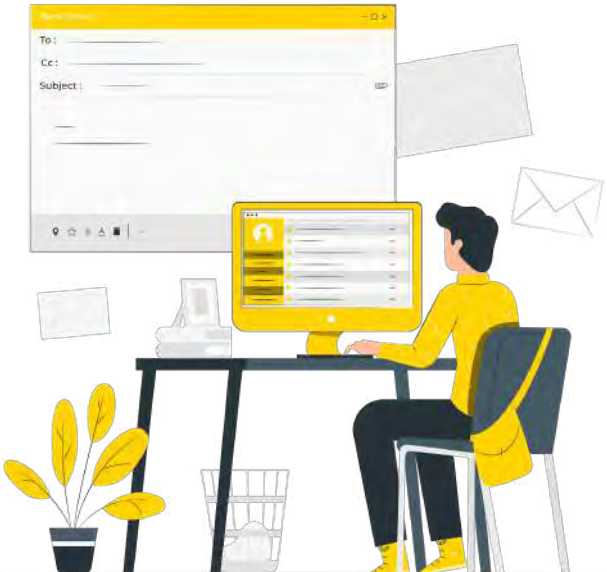
A prática de opt-out está prevista no Cdigo de Autorregulamentação para a Prática de E-mail Marketing (CAPEM) nos capítulos II e III que lidam com a definição do termo. É de suma importância igualmente que as empresas respeitem as diretrizes legais previstas na Lei Geral de Proteção de Dados Pessoais (LGPD).


***Renato Opice Blum***

Advogado e economista; chairman e sócio-fundador do Opice Blum, Bruno e Vainzof Advogados Associados; patrono regente do curso de pós-graduação em Direito Digital e Proteção de Dados da EBRADI; coordenador de cursos sobre Direito Digital e Proteção de Dados da FAAP, EPD e Insper; diretor da Itechlaw; membro do Conselho da EuroPrivacy; juiz do Inclusive Innovation Challenge do MIT; presidente da Associação Brasileira de Proteção de Dados (ABPDados); e vice-presidente da Comissão Especial de Direito e Inovação da OAB/SP.

***Guilherme Guimarães Vieira***

Estagiário da área de privacidade e proteção de dados do Opice Blum, Bruno e Vainzof Advogados Associados.


OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

# Legitimate Interest Assessment – LIA

***Por Helena Rodrigues Vaz Pedrosa***

A LGPD não tem por objetivo proibir o tratamento de dados pessoais, estando entre seus fundamentos, inclusive, o desenvolvimento econômico e tecnológico e a inovação, buscando apenas estabelecer regras mais claras para o uso destas informações a ponto de resguardar a privacidade e a proteção de dados de pessoas naturais, Titulares de Dados.

Deste modo, a fim de que as atividades de tratamento de dados pessoais possam ser consideradas legítimas, a legislação estabelece algumas hipóteses legais permissivas para o tratamento de dados pessoais (as chamadas Bases Legais), dentre as quais inclui-se o Legítimo Interesse, o qual pode ser utilizado nas hipóteses em que o tratamento for necessário para "atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

O Legítimo Interesse é uma das bases legais mais flexíveis para tratar dados pessoais, uma vez que não está focado em um propósito específico, oferecendo maior espaço para utilização em diferentes circunstâncias, tendo em vista que muitos interesses podem ser considerados legítimos. Por tal motivo, inclusive, ele não poderá ser utilizado caso a atividade envolva dados pessoais sensíveis.

Em seu art. 10, a LGPD estabelece que a adoção desta base legal deverá ser considerada para finalidades legítimas, verificadas no caso concreto e que poderão envolver o apoio e promoção de atividades do Controlador e a proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas suas legítimas expectativas, assim como seus direitos e liberdades fundamentais.

Assim, ao realizar o tratamento sob Legítimo Interesse, a transparência aos titulares envolvidos deverá ser fortalecida, justamente para garantir que tenham a legítima expectativa em relação ao tratamento de seus dados, assim como somente os dados pessoais estritamente necessários para alcançar a finalidade pretendida deverão ser tratados.

Nesse sentido, apesar de não estar prevista expressamente na legislação brasileira, a elaboração do chamado *Legitimate Interest Assessment* (LIA) é uma ferramenta importante para que o Controlador possa avaliar e documentar a legalidade do tratamento, bem como avaliar se o Legítimo Interesse é a base legal mais adequada para fundamentar a atividade.

O objetivo deste documento é, portanto, demonstrar, de acordo com a atividade concreta, o racional utilizado pelo Controlador que permitiu que tal atividade fosse fundamentada no Legítimo Interesse e o processo que o levou à tomada de decisão, haja vista sua ampla possibilidade de utilização e necessidade de atendimento aos requisitos trazidos pela legislação.

Não existem regras estabelecidas sobre como o LIA deve ser elaborado. Entretanto, a fim de se avaliar se os requisitos do Legítimo Interesse previstos na legislação estão presentes no caso concreto, e em linha com as orientações das autoridades de proteção de dados da União Europeia, esse *assessment* poderá ser realizado em três etapas:

### Teste de Propósito ou finalidade

**busca averiguar se a finalidade é lícita e qual é o interesse legítimo em questão[1]**

### Teste da Necessidade

**busca averiguar se o tratamento a ser realizado de fato é necessário para o alcance do interesse em questão[2]**

### Teste de Balanceamento

**busca avaliar se há um balanceamento entre o Legítimo Interesse e os direitos e liberdades fundamentais do titular de dados[3]**

---

[1] Lei Federal n. 13.709/2018, Art. 10, caput:" *O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: [...]*".

[2] Lei Federal n. 13.709/2018, Art. 10, § 1º: "*Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.*"

[3] Lei Federal n. 13.709/2018, Art. 10, II: "*O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: [...]II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.*"

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Para o assessment em cada uma destas três etapas, alguns fatores poderão ser considerados, entre eles:

## Sobre a Finalidade

- o que se objetiva com o tratamento de dados em questão?
- quem se beneficiará com o tratamento e de qual forma se beneficiará?
- o tratamento de dados propiciará benefícios a uma coletividade?
- O tratamento de dados propiciará benefícios a terceiros?
- quão importantes são estes benefícios?
- qual seria o impacto caso houvesse impossibilidade de seguir com o tratamento em questão?
- o tratamento é ilegal ou antiético?

## Sobre a Necessidade

- o tratamento de dados de fato auxiliará no alcance da finalidade pretendida?
- existe uma maneira menos intrusiva para alcançar o objetivo que se visa?
- é razoável o tratamento de dados em questão?

## Sobre o Balanceamento

- qual a relação existente entre o titular e o controlador?
- o controlador possui meios para exercer transparência em face do titular de dados?
- o tratamento envolve dados de crianças e/ou adolescentes ou de indivíduo que apresente alguma vulnerabilidade?
- quais serão os impactos do tratamento sobre o titular de dados?
- há medidas de segurança a serem adotadas para mitigar eventuais impactos provenientes do tratamento?
- o titular possui expectativa quanto ao tratamento de seus dados?

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Assim, o LIA deve ser elaborado antes do início das atividades de tratamento de dados e, a fim de que o documento esteja de fato refletindo a realidade da atividade, é recomendável que, em sua elaboração, sejam envolvidas personagens-chave da operação, e que o documento permaneça sob constante revisão e atualização. O objetivo é fazer com que não fique defasado ante eventuais modificações sofridas no âmbito operacional que impactem na finalidade e nos meios do tratamento de dados.

É importante, ainda, que o LIA seja elaborado de forma a evidenciar com clareza as informações a serem tratadas e as salvaguardas a serem adotadas para mitigar eventuais riscos, considerando o impacto da atividade sobre os titulares de dados tratados e os danos que podem ser causados a eles. Ao final da elaboração do LIA, além de tornar possível ao controlador averiguar se sua operação de fato se adequa à base legal do Legítimo Interesse, ele terá melhor visibilidade sobre a vulnerabilidade da atividade em questão, podendo identificar a necessidade de elaboração de um Relatório de Impacto à Proteção de Dados (RIPD), conforme dispõe o art. 10, §3º, da LGPD.

O que se percebe, portanto, é que, na escolha do Legítimo Interesse, o controlador deverá suportar uma extensa gama de responsabilidades, ampliando sua visão em diversos sentidos, para garantir o cumprimento dos requisitos sobreditos. Os inúmeros aspectos a serem observados, por sua vez, abrem espaço para discordâncias sobre a base legal escolhida, tornando-se mais complexo demonstrar a conformidade no tratamento de dados pessoais.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

A exigência do preenchimento de diversas condições para a aplicabilidade do Legítimo Interesse não tem por desígnio inviabilizar o uso da referida base legal, cuja importância é salutar. Esses critérios objetivam, na realidade, estabelecer maior nível de proteção aos dados pessoais e a seu titular, de modo que é necessário ao controlador documentar o cumprimento de todos os requisitos em questão a fim de que possa evidenciar à ANPD, se preciso for, que é adequada a utilização do Legítimo Interesse para uma determinada atividade de tratamento de dados.

Assim, o LIA, apesar de não ser um documento exigido expressamente pela LGPD, permite apoiar a legalidade do tratamento, demonstrando que o Controlador se preocupou em justificá-la e documentá-la, em aderência aos princípios da prevenção e da responsabilização e prestação de contas previstos na LGPD.

***Helena Rodrigues Vaz Pedrosa***
Advogada da área de Privacidade e Proteção de Dados do Opice Blum, Bruno e Vainzof Advogados Associados.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

# A Importância dos Direitos dos Titulares

***Por Gabriel Nantes Gimenez***

Muitos países ocidentais, ao reconhecerem o potencial dúbio dos dados pessoais, envidaram seus esforços para regular a forma com a qual organizações fazem uso daqueles, com o intuito maior de resguardar não apenas o dado pessoal, mas também a dignidade e os direitos humanos.

Neste contexto surgiu a Lei Geral de Proteção de Dados Pessoais - LGPD, que colocou o Brasil em consonância com outros países em relação ao tratamento de dados no cenário de *Big Data*, trazendo segurança jurídica para fomentar inovação sem que se firam direitos fundamentais.

As organizações - sejam elas empresas privadas ou públicas - podem, sim, dar continuidade às atividades de tratamento de dados, essenciais para consecução de seus objetivos, mas devem sempre garantir que as pessoas exerçam, de fato, o controle sobre seus dados pessoais, garantindo a observância a um dos fundamentos legais, a chamada autodeterminação informacional.

Para consubstanciar os princípios sobre os quais está embasada, a LGPD inovou ao trazer direitos específicos relacionados à privacidade e à proteção de dados, dentro da ótica do empoderamento das pessoas.

É possível ver certo paralelismo com o Código de Defesa do Consumidor – CDC, que foi revolucionário em seu surgimento ao trazer uma sistemática para lidar com os problemas e anseios dos consumidores.

Foi neste sentido que a LGPD trouxe os direitos dos titulares de dados pessoais: direito de confirmação de tratamento, de acesso, correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD; eliminação dos dados pessoais tratados com o consentimento do titular em certas hipóteses, revogação do consentimento, entre outros.

## A quem cabe garantir esses direitos?

É importante entender o papel que uma organização desempenha nas atividades de tratamento de dados pessoais, na classificação imposta pela LGPD, que cria as figuras do **controlador** e do **operador.**

Se o controlador é o agente a quem compete as decisões referentes ao tratamento de dados pessoais, o operador é aquele que realiza o tratamento destes dados em nome do controlador, não possuindo poder decisório sobre as finalidades do tratamento. Assim, quando for controladora de dados pessoais, uma empresa tem a obrigação de atender às requisições dos titulares.

É imprescindível, porém, que haja grande cooperação entre os agentes de tratamento, de modo que atuem para garantir o efetivo cumprimento da LGPD. Não apenas a LGPD atribui a responsabilidade por garantir o exercício dos direitos aos controladores, mas também quando o titular de dados pessoais se tratar de consumidor, a responsabilidade é solidária entre fornecedores, estabelecida no Código de Defesa do Consumidor (**Lei nº 8.078/1990**), cuja aplicabilidade foi mantida pela LGPD. Neste caso, sobre ambos, pode recair a obrigação de responder por descumprimento das obrigações de privacidade.

Para a consecução dos direitos instituídos pela LGPD, os agentes de tratamento devem possuir muito mais do que apenas uma política externa de privacidade em seu *website*. Em verdade, os riscos a uma empresa que não é **diligente em responder a um titular** se adicionam às eventuais multas impostas por autoridades; o risco reputacional ganha fôlego quando um titular se sente lesado pela negligência de uma empresa e vocaliza tal inconformidade por meio das redes sociais, nas quais reclamações viralizam em velocidade exponencial.

Nos programas de privacidade das organizações, devem existir estruturas de governança e ferramentas internas que criem um arcabouço operacional. E o bom funcionamento deste programa orbita no papel do chamado DPO, o Encarregado por dados pessoais na organização, que garantirá a equalização entre políticas internas e riscos à organização e funcionará como ponto de contato entre os mais diversos atores das relações de privacidade:

- **Organização;**
- **Titular; e**
- **Autoridade.**

Será o DPO o responsável por organizar os fluxos de resposta às requisições dos titulares – como receber, quem deve responder, quais os padrões de resposta, formato de comunicação –, que funcionarão como árvores de decisão que explicitem todo o caminho que uma requisição tomará desde o momento em que chegou. É exatamente essa sistemática que garantirá respostas adequadas e no tempo legal - ainda que a LGPD somente estabeleça prazo para solicitações de **confirmação de existência** e de **acesso**, quando a resposta deve ser imediata se em formato simplificado ou em 15 dias se em formato completo.

Canais de comunicação, por meio dos quais titulares farão contato, devem ser destinados não apenas aos clientes da empresa, como também aos demais titulares de dados (colaboradores, por exemplo). Por essa razão, além de gratuitos, os canais devem ser especializados, com atendentes treinados, sob supervisão do DPO e da equipe de privacidade, para receber solicitações referentes à LGPD.

As informações deverão ser fornecidas de forma concisa (e limitada ao que foi solicitado), transparente e inteligível, sempre considerando o caráter multifacetado dos titulares de dados, cujos perfis podem variar em termos de localização, idade, conhecimento, escolaridade etc. Neste sentido, por exemplo, é do titular dos dados pessoais a prerrogativa de decidir o formato desejado da comunicação, seja por meio eletrônico ou impresso.

A própria manutenção de todo o histórico de uma solicitação - quando e por quem a solicitação foi feita, por meio de qual canal, quem respondeu e em qual prazo – é uma ferramenta do DPO para resguardar a organização de quaisquer reclamações ou fiscalizações futuras.

Uma postura ativa na análise recorrente das solicitações, aliás, permite que a organização entenda padrões e condutas de seus clientes ou colaboradores, o que pode ajudá-la a atualizar procedimentos internos e a embutir a privacidade desde o princípio em suas atividades – o que é especialmente valioso para empresas cujos produtos evoluem a partir da experiência do consumidor.

A LGPD é reflexo das atuais questões impostas pelo progresso tecnológico, que trouxe riscos à privacidade na sociedade informacional. Sendo uma lei principiológica que carece de regulamentação, a LGPD depende ainda de sua autoridade encarregada de implementá-la, a Autoridade Nacional de Proteção de Dados - ANPD.

Neste cenário, quem ganha protagonismo são os agentes de tratamento que, além de agirem de forma diligente, podem aplicar as melhores práticas do mercado para se tornarem referências no atendimento às requisições das pessoas. Por meio de programas de privacidade encabeçados por DPOs que enxergam além das restrições, as organizações podem extrair vantagens competitivas das obrigações que uma lei tão importante já impõe.

***Gabriel Nantes Gimenez***
Advogado do Opice Blum, Bruno e Vainzof Advogados Associados. Possui MBA .pela HEC-Paris, Pós-graduação em Direito Empresarial pela ESA-OAB SP e Graduação em Direito pela Universidade de São Paulo - USP.

# Como gerir o direito à revogação do consentimento

***Por Maria Beatriz Previtali***

Muito se fala sobre a dificuldade de coletar o consentimento de maneira adequada. Mas gerenciá-lo e permitir que o titular o revogue é tão importante e desafiador quanto.

Ao contrário da maioria das bases legais de tratamento de dados pessoais e dados sensíveis da Lei Geral de Proteção de Dados Pessoais (LGPD), o consentimento tem características bem peculiares, inclusive um ciclo de vida próprio. Pode-se dizer que é a única base legal que permite que o tratamento de dados seja encerrado "prematuramente", mediante uma simples manifestação do titular de dados: quando o "não" chega ao controlador, aquela atividade deve ser encerrada.

Na prática, sabemos que isso não se resolve com um simples "let it go" ou apertando um botão — mas tampouco precisa ser tão complicado quanto muitos pensam. Por isso, neste artigo, abordaremos brevemente sobre o que a revogação do consentimento de fato significa e como operacionalizá-la de maneira eficiente e em conformidade com a LGPD.

Objetivamente falando, a revogação do consentimento por determinado titular significa que, a partir daquele momento, o controlador (isto é, aquele que tem o poder de decisão sobre o tratamento dos dados)[1] não poderá mais tratar os dados específicos com a finalidade para a qual o consentimento foi colhido.

[1] A LGPD define o controlador de dados como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI).

Isso não afeta a atividade de tratamento realizada até então: todo o tratamento até aquele ponto é ratificado, mas deve ser interrompido.[2] Na prática, o agente de tratamento deve deixar aquele(s) dado(s) inerte(s), ou seja, sem qualquer utilização mesmo para outras finalidades semelhantes.

É possível também que a revogação do consentimento venha acompanhada da solicitação de eliminação desses dados. Neste caso, todas as informações relacionadas àquele(s) dado(s) deverão ser eliminadas ou, no mínimo, anonimizadas, a fim de que essas informações sejam completamente desassociadas do titular de dados, exceto nas hipóteses expressamente previstas na LGPD, concentradas, principalmente, no artigo 16, dentre as quais está a necessidade de manutenção dos dados para cumprimento de obrigação legal ou regulatória pelo controlador.

Caso o gerenciamento dos citados direitos seja realizado por um prestador de serviços contratado como operador de dados (isto é, que tratará os dados em nome do contratante, o controlador), o contratante deverá disponibilizar instruções sobre como agir quando receber essa solicitação do titular de dados (geralmente, via contrato ou procedimentos estabelecidos entre as partes).

De qualquer modo, tanto para a revogação do consentimento quanto para a eliminação dos dados tratados com o consentimento, o controlador precisa disponibilizar para os titulares de dados meios facilitados e gratuitos para o exercício de tais direitos. Vale notar que a LGPD não regula quais são esses meios, mas apenas como eles devem ser.

[2] Conforme previsto na primeira parte do § 5º do art. 8º da Lei: "O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado (...)".

Por isso, o controlador é livre para adotar a solução que for mais adequada para o contexto em que ocorre aquele tratamento de dados.

**Por exemplo:** se o consentimento é utilizado como base legal para enviar e-mails publicitários, um *opt-out*, como o famoso "clique aqui se não deseja mais receber nossas mensagens", pode ser um mecanismo válido. Outros meios também interessantes incluem sistemas que permitem que o próprio titular gerencie suas preferências e autorizações por meio de uma área logada ou semelhante ou, ainda, solicitações feitas diretamente ao canal de atendimento ao titular.

Independentemente do formato adotado, o mais importante é que essa solução seja eficiente, isto é, capaz de cessar o tratamento dos dados assim que receber a informação sobre a revogação do consentimento.

Assim, no exemplo do *opt-out* do e-mail, de nada adianta se descadastrar no local indicado se os e-mails de publicidade continuam a ser enviados, contrariando a manifestação de vontade daquele titular de dados. Ou se o titular entra em contato com o canal de atendimento para revogar seu consentimento para um determinado fim, mas é exposto a procedimentos intermináveis e burocráticos apenas para processar o seu "não". Ou, pior ainda, se o titular de dados deseja revogar seu consentimento num contexto em que o consentimento não era a base legal utilizada, mas sem ter essa informação.

Além disso, é fundamental que a empresa esteja atenta às novidades regulatórias — que serão várias nos próximos anos: as sanções da LGPD estão prestes a entrar em vigor, em agosto de 2021,[3] e a Autoridade Nacional de Proteção de Dados (ANPD) também publicará regulações sobre o exercício de direitos dos titulares em breve, no primeiro semestre de 2022.[4] É, em resumo, um cenário ainda em constante evolução.

Por isso, antes de buscar as soluções disponíveis no mercado, é altamente recomendado que a empresa alinhe entendimentos com o seu Encarregado de Proteção de Dados, também conhecido como DPO (*Data Protection Officer*). Assim, será possível localizar quais atividades de tratamento utilizam o consentimento como base legal e qual a melhor maneira de gerenciar esse consentimento, a fim de permitir ao titular de dados que exercite todos os seus direitos também de maneira eficiente.

Por fim, mas não menos importante, lembramos que, embora essas mudanças trazidas pela LGPD sejam frequentemente divulgadas como grandes avanços para os titulares de dados (o que de fato são), não podemos esquecer que as empresas que lidam com o tratamento de dados pessoais, em alguma medida, também são altamente beneficiadas.

---

[3] Lei Federal n. 13.709/2018, Art. 10, caput:" *O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: [...]*".

[4] Lei Federal n. 13.709/2018, Art. 10, § 1º: "*Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.*"

Com regras mais claras sobre como, quando e por quanto tempo tratar os dados pessoais de seus clientes, colaboradores e outros indivíduos, os agentes de tratamento de dados poderão verificar quais informações necessitam ou valem a pena ser mantidas, reduzindo as chances de tratamento de dados desnecessários e da exposição a riscos de segurança da informação. No fim, uma revogação de consentimento eficiente e facilitada se presta exatamente a essas finalidades, porém conforme a autonomia e vontade do titular de dados.

***Maria Beatriz Previtali***
Advogada da Equipe Consultiva de Privacidade e Proteção de Dados do Opice Blum, Bruno e Vainzof Advogados Associados, pós-graduanda em Direito Digital pelo ITS-Rio e coordenadora do Núcleo de Proteção de Dados da Faculdade de Direito da USP, grupo de estudos supervisionado pelo Professor Carlos Portugal Gouvêa.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

# RIPD e sua importância nos programas de governança em privacidade

***Por Helena Dominguez Paes Landim***

A avaliação de riscos é parte essencial de um Programa de Governança voltado à conformidade com determinada legislação e, no caso da Lei n. 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), não poderia ser diferente. Fundamentada tanto no respeito à privacidade dos titulares de dados pessoais e na autodeterminação informativa quanto no desenvolvimento econômico e tecnológico e na inovação, a LGPD desperta a necessidade de ponderação e análise cautelosa dos Controladores de dados sobre suas atividades de tratamento de dados pessoais, a fim de que esses fundamentos possam convergir de maneira harmônica e equilibrada.

É nesse contexto, portanto, que o Relatório de Impacto à Proteção de Dados (RIPD), definido como a documentação do Controlador que analisa projetos envolvendo o tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais (Art. 5º, XVII, da LGPD), se mostra como uma ferramenta estratégica para o *assessment* da atividade de tratamento e identificação dos seus riscos, bem como para o apontamento das medidas e mecanismos de mitigação aplicáveis ao caso.

Assim, no âmbito de um Programa de Governança em Privacidade, a elaboração deste documento, por ser considerado um instrumento de avaliação e gestão de riscos, corrobora com o atendimento ao princípio da prevenção, previsto no Art. 6º, VIII, da LGPD, uma vez que ele irá apresentar salvaguardas para evitar possíveis violações da legislação que possam acarretar em danos aos titulares, bem como sinalizar as medidas para mitigação dos referidos riscos.

Ao mesmo tempo, o RIPD torna-se uma evidência da diligência do Controlador no cumprimento da LGPD, em respeito ao princípio da responsabilização e prestação de contas, conforme dispõe o Art. 6º, X, desta lei. Isso porque farão parte do seu conteúdo a descrição dos tipos de dados pessoais envolvidos e todo seu ciclo de tratamento dentro de uma atividade, desde o momento em que são coletados até o seu efetivo descarte.

Assim, a atividade de tratamento poderá ser constantemente monitorada por meio desta documentação, podendo, inclusive, ser atualizada de forma periódica, ao passo que as medidas mitigadoras de riscos forem adotadas e especialmente na hipótese de haver qualquer mudança relevante na operação. Assim, essa documentação permitirá que o Controlador demonstre a observância e o cumprimento das normas de proteção de dados pessoais no tocante à atividade avaliada.

Além de ser um documento que permite identificar a conformidade da atividade em relação ao cumprimento dos comandos legais, a LGPD estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) poderá demandar do Controlador a elaboração de um RIPD referente a qualquer atividade de tratamento de dados pessoais, observados os segredos comercial e industrial, em especial quando a atividade estiver fundamentada no Legítimo Interesse do Controlador (Art. 10, §3º da LGPD) ou quando envolver o tratamento de dados pessoais sensíveis (Art. 38, da LGPD).

Deste modo, para além dos casos previstos em lei acima mencionados, recomenda-se, com base em orientações da autoridade britânica de proteção de dados pessoais[1], que se elabore um RIPD quando a atividade envolver:

- soluções tecnológicas ou organizacionais inovadoras;
- rastreamento da localização ou comportamento online ou offline de titulares;
- dados relativos a pessoas vulneráveis (por exemplo, crianças e adolescentes);
- tratamento de dados pessoais em grande escala;
- combinação, comparação ou cruzamento de dados de múltiplas fontes; tomada de decisão automatizada para tomar decisões significativas sobre os titulares, tais como sobre acesso de alguém a um serviço, oportunidade ou benefício; e
- definição de perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade para tomada de decisão (como categorização, pontuação, bem como definição de perfis em larga escala).

[1]Conforme dispõe o ICO – Information Commissioner's Office, em guia sobre conformidade com o GDPR em tópico dedicado ao tema sobre Relatório de Impacto à Proteção de Dados Pessoais, situado enquanto documentação de accountabity e governança.
Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> Acesso em: 24/05/2021.

Assim, quando o Controlador estiver diante de determinada atividade de tratamento de dados pessoais que puder implicar elevado risco aos direitos e às liberdades das pessoas naturais, recomenda-se a elaboração do RIPD para cada uma destas atividades, a partir de uma análise de criticidade e prioridade dentro do Programa de Governança em Privacidade da organização.

Nessa mesma sequência de avaliação, com base em orientações da doutrina europeia[2] sobre o tema, a organização poderá definir sobre a elaboração de um RIPD para uma única atividade ou se abrangerá um conjunto de atividades semelhantes, desde que verse sobre temas conectados em termos de natureza, escopo, contexto, finalidade e riscos.

Para tanto, o Controlador poderá contar com a colaboração de todas as partes envolvidas com o tratamento de dados pessoais, inclusive com a do Encarregado e do Operador, quando assim for necessário. No tocante à elaboração desta documentação, a tarefa poderá ser atribuída a qualquer pessoa com conhecimento técnico sobre a atividade e potenciais riscos à proteção de dados pessoais envolvidos na operação.

[2]Conforme dispõe o ICO – Information Commissioner's Office, em guia sobre conformidade com o GDPR em tópico dedicado ao tema sobre Relatório de Impacto à Proteção de Dados Pessoais, situado enquanto documentação de accountabity e governança.
Disponível em:
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> Acesso em: 24/05/2021.

Nesse sentido, considerando o objetivo do RIPD, destaca-se que a análise do risco deverá ser desenvolvida sob a perspectiva do titular. Ou seja, a priori, não é o principal objetivo deste documento contemplar aqueles riscos que afetam diretamente o Controlador, por exemplo, sob o aspecto financeiro, jurídico ou reputacional da organização, em que pese possam representar consequências decorrentes da assunção de riscos aos titulares com a continuidade de determinada atividade.

Assim, deverão ser observados aqueles prejuízos e danos que poderão ser percebidos pelo titular e como determinada atividade poderá impactar sua vida negativamente, resultando em algum tipo de dano patrimonial, moral, individual ou coletivo. A partir desta lógica, o Controlador poderá aplicar uma metodologia para mensurar o risco, considerando, por exemplo, a probabilidade e o possível impacto que seria percebido pelo Titular, na hipótese de verificação e concretização deste.

Diante da profundidade de análise sobre determinada atividade que seja submetida à elaboração de um RIPD, esta conduta indica um alto nível de diligência do Controlador, que poderá contribuir para a percepção da ANPD acerca de seu comprometimento no cumprimento da LGPD e no respeito à privacidade e proteção de dados daqueles titulares que têm seus dados pessoais tratados pela organização.

Apesar de a LGPD prever que o RIPD poderá ser solicitado pela ANPD em determinadas hipóteses, não há uma previsão expressa na lei quanto à necessidade de que esse documento seja elaborado previamente à requisição da Autoridade.

Entretanto, em atenção:

I ao cumprimento dos princípios da prevenção, responsabilização e prestação de contas;

II à necessidade de análises sob a perspectiva de privacidade desde a fase de concepção de novos processos, produtos ou serviços;

III à necessidade de adoção pelos agentes de tratamento de regras de boas práticas e de governança que estabeleçam os mecanismos internos de supervisão e de mitigação de riscos (art. 50, LGPD), é altamente recomendável que o RIPD seja elaborado de forma antecipada e preventiva pelo Controlador.

Neste mesmo sentido, a LGPD dispõe ainda que o Programa de Governança em Privacidade deverá, no mínimo, ser implementado com o estabelecimento de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade (art. 50, I, d) da LGPD.

Em conclusão, o RIPD representa uma documentação útil, necessária e, ainda, estratégica, para que os Controladores possam realizar a avaliação e gestão de riscos de privacidade em suas organizações, contribuindo positivamente para a conformidade com a LGPD e sucesso do Programa de Governança em Privacidade, promovendo, por consequência, um relacionamento de maior confiança, segurança e sustentabilidade com todos os seus stakeholders, na medida em que a privacidade e a proteção de dados de todos aqueles que confiam seus dados à organização sejam respeitadas.

***Helena Dominguez Paes Landim***

Adovogada no Opice Blum, Bruno e Vainzof Advogados Associados. Expecialista em Privacy and Data Protection Lawyer e Certified EXIN PDPE (Privacy and Data Protection Essentials).

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

# Processo de Avaliação e Gestão de Terceiros

***Por Marcos Gomes da Silva Bruno***

Em qualquer segmento empresarial, a terceirização de alguns processos necessários para a execução das atividades comerciais é uma realidade inafastável e que deve ser objeto de atenção dos empreendedores.

Quando essa terceirização envolve algum tipo de tratamento de dados pessoais em nome da contratante, teremos, via de regra, o contratante na figura de controlador dos dados pessoais, e o terceiro, contratado, na figura de operador dos dados pessoais.

Nesta situação, o artigo 42 da Lei 13.709/18 (Lei Geral de Proteção de Dados) estabelece a possibilidade de responsabilidade solidária do contratante por ações de seu contratado que eventualmente causem qualquer tipo de dano aos titulares de dados pessoais, o que, por si só, já seria suficiente para se preocupar com a avaliação e gestão desses terceiros.

Porém, para além da questão regulatória e dos dados pessoais, é fato que as empresas confiam aos fornecedores não só a proteção dos dados de seus consumidores, mas sua reputação, suas finanças e até mesmo sua disponibilidade de negócio.

Nessa esteira, um incidente envolvendo um terceiro é praticamente equivalente a um incidente na empresa, e, é por isso, que o empresário precisa conhecer esses terceiros e os riscos ao redor das atividades por eles desempenhadas.

Mais do que um simples questionário com perguntas e respostas, como tende a ser a avaliação de terceiros em boa parte das empresas, o gerenciamento de terceiros é uma tarefa árdua, que requer transparência, documentação precisa e colaboração efetiva.

Com efeito, podemos resumir a gestão de terceiros em três pilares, quais sejam:

- programa de gestão de terceiros;
- avaliação de risco de terceiros; e
- monitoramento e resposta de vulnerabilidades.

No **Programa de Gestão de Terceiros**, a recomendação é prever:

1. A governança do programa em si, ou seja, a criação de políticas e procedimento internos que descrevam o funcionamento do programa;

2. As ações de treinamento e conscientização, informando os colaboradores internos sobre os termos das políticas e procedimentos relacionados ao Programa de Gestão de Terceiros, de modo que haja amplo conhecimento dessas condições;

3. Um processo que objetive garantir que a equipe responsável pela gestão de terceiros se envolva em todos os estágios do relacionamento com novos terceiros, desde a negociação até o eventual encerramento do contrato, depois da contratação;

4 Uma base de dados central de perfil de risco dos terceiros envolvidos na operação da empresa, com fácil acesso aos resultados de avaliações, inconsistências em aberto e inconsistências gerenciadas, entre outros itens relevantes; e

5 Disposições contratuais efetivas, para garantir os níveis requeridos de segurança dos terceiros, além dos direitos de auditoria.

Já na **Avaliação de Riscos de Terceiro**, a recomendação é prever:

1 Processo para avaliação dos riscos inerentes ao terceiro e à atividade terceirizada, permitindo mapear os ativos em risco, o risco potencial e o potencial de dano de um eventual incidente, para cada terceiro;

2 Monitoramento contínuo do terceiro por meio de "informações de superfície", acessíveis publicamente, permitindo medir, objetivamente, como os terceiros implementam e operam seus controles de segurança;

3 Gestão contínua da periodicidade das avaliações do terceiro, baseada na conjunção entre os riscos inerentes e os riscos de superfície, estabelecendo agendas dinâmicas de reavaliação dos terceiros, de acordo com sua performance e o nível do risco inerente;

4 Avaliação do terceiro lastreada em contrato, com acesso privilegiado a informações e nível de profundidade calibrado de acordo com os riscos inerentes daquele terceiro;

5 Gestão de risco, envolvendo-se com os terceiros para endereçar inconsistências que necessitam de correção, como forma de assegurar um nível satisfatório de risco.

Por fim, no que diz respeito ao **Monitoramento e Resposta de Vulnerabilidades**, recomendamos:

1. Pesquisa e monitoramento de eventuais condições de risco, de modo a rapidamente detectar e agir em eventos de segurança envolvendo o terceiro;

2. Procedimento objetivo de triagem da criticidade de vulnerabilidades em sistemas de terceiros, garantindo uma resposta assertiva, em caso de incidente;

3. Mapeamento dos fornecedores dos terceiros a serviço da empresa, para entender os pontos de concentração de risco do terceiro; e

4. Mapeamento da localização física dos sistemas do terceiro, conhecendo riscos geográficos, que podem envolver limitações regulatórias, tensões políticas e econômicas, ou, até mesmo, risco de desastres naturais.

Portanto, como mencionado no início deste artigo, o Processo de Avaliação e Gestão de Terceiros é tarefa complexa, mas essencial para garantir a segurança da organização na contratação de parceiros, sobretudo aqueles com quem há compartilhamento de dados pessoais, figurando como essencial a qualquer empresa que queira atingir um nível otimizado de gestão de riscos.

***Marcos Gomes da Silva Bruno***
Sócio do Opice Blum, Bruno e Vainzof Advogados Associados.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

# A revisão de contratos à luz da LGPD

***Por Maria Eduarda Annarumma Guedes, Gabriel Nantes Gimenez, Gabriela Bueno e Ana Rita Bibá Gomes de Almeida***

Quando a Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) entrou em vigor, muito se discutiu a respeito de como as organizações deveriam implementar medidas internas tendo em vista a privacidade e a proteção de dados. No entanto, a prática das empresas mostrou que um dos principais desafios trazidos pela LGPD ocorre justamente para equalizar as relações externas, nas negociações entre empresas por meio do complexo documento que emaranha intenções: um contrato.

Para fins da LGPD, todos aqueles que tratam dados pessoais são chamados de Agentes de Tratamento de Dados Pessoais, a quem a Lei atribui uma série de obrigações, a depender de sua categoria: de um lado, os Controladores; de outro, os Operadores. É o Controlador a pessoa natural – comumente referida como "física" - ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Já o Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Essa classificação deriva, de maneira simplista, do grau de autonomia que cada um exerce sobre o tratamento dos dados pessoais, impactando no regime de responsabilidade desses Agentes de Tratamento.

É por essa razão que as obrigações que recaem sobre o Operador são em menor número, e ele responderá pelos danos causados em decorrência do tratamento, solidariamente ao Controlador, apenas em duas hipóteses:

**Quando descumprir as obrigações decorrentes da legislação de proteção de dados**

**Quando não tiver seguido as instruções lícitas do Controlador**

Entretanto, não há na LGPD muitas previsões específicas sobre a obrigatoriedade legal da celebração de contratos entre tais agentes - salvo algumas exceções. Tampouco trata a Lei de todos os temas com os detalhes proporcionais à complexidade das novações que floresceram com essa primeira legislação sobre privacidade, ainda que tais lacunas da Lei venham sendo preenchidas com os melhores esforços, por meio das manifestações da Autoridade Nacional de Proteção de Dados (ANPD).

Nesse cenário de incertezas, há, contudo, subsídios que a LGPD nos traz, ao estabelecer seus princípios legais[1], pontos basilares que fornecem os limites para uma atuação em conformidade com o intuito da Lei.

Desses princípios, extraímos a utilidade - diríamos necessidade – de celebração de contrato ou revisão dos contratos já celebrados, para estabelecer como as atividades de tratamento deverão ocorrer na relação contratual entre as partes envolvidas, em especial para garantia de princípios como o da segurança, prevenção e responsabilização e prestação de contas.

[1] Art. 6º, LGPD.

Em síntese, os princípios citados determinam a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de tratamentos inadequados, prevenir a ocorrência de danos em virtude desse tratamento e, ainda, demonstrar a adoção de medidas eficazes e capazes de comprovar a observância desses comandos.

Nesse contexto pluridimensional, a relação contratual deve nascer – ou, quando já posta, ser alterada ou aditada – para não apenas estar em consonância com a Lei, mas complementá-la naquilo que é de discricionariedade dos agentes privados. Em outras palavras, cria-se um procedimento, pelos Agentes de Tratamento, de definição de regras de forma antecipada, em linha, inclusive, com o princípio de responsabilização e prestação de contas elencado na LGPD.

É uma oportunidade de as partes ali estabelecerem as respectivas obrigações no âmbito das atividades de tratamento de dados pessoais, bem como diretrizes que possam preencher as lacunas da lei, prevendo as consequências para as hipóteses de inadimplemento por qualquer das partes.

É fato que, inevitavelmente, os contratos trazem em seu bojo dados pessoais, independentemente do seu objeto, a exemplo dos dados de representantes legais em contratos celebrados entre pessoas jurídicas ou, a depender do seu objeto, a previsão do compartilhamento de um número relevante de dados pessoais como requisito inafastável à própria execução de seu escopo. Dessa forma, um contrato terá o intuito maior de determinar o ciclo de vida para o manejo de quaisquer dados pessoais envolvidos na relação entre as partes, estabelecendo-se, dessa forma, regras desde a coleta até sua retenção e exclusão.

Tendo em vista o acima exposto sobre a hierarquia em relação ao poder decisório dos Agentes de Tratamento, **o primeiro passo** para a revisão de um contrato à luz da LGPD é a **identificação dos papéis exercidos pelas partes, enquanto Agentes de Tratamento em relação a cada atividade**.

A mencionada identificação será relevante, entre outros aspectos, para determinar o nível de responsabilidade de cada um deles no caso de danos (patrimoniais ou morais, individuais ou coletivos) que decorram de violações à lei, o que se torna essencial para a delimitação cuidadosa das obrigações e incumbências de cada uma das partes. Nessa linha, importante mencionar o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, publicado pela ANPD, em 28 de maio de 2021, que busca estabelecer diretrizes não vinculantes aos Agentes de Tratamento e explicar quem pode exercer a função do Controlador e do Operador, até que haja regulamentação, de fato, pela Autoridade nesse sentido.

É importante consignar, contudo, que tais figuras não são estáticas, ou seja, dificilmente um agente de tratamento será apenas Controlador ou Operador, de modo que a atribuição desse papel dependerá da análise fática e contextual da atividade em que são tratados os dados. Vale mencionar que, embora não seja possível alterar o papel dos Agentes de Tratamento contratualmente, é possível distribuir os riscos do contrato por meios de cláusulas de responsabilização e penalidades.

O **passo seguinte**, por sua vez, é **aferir o nível do risco envolvido nas atividades de tratamento dos dados pessoais necessárias à execução do objeto da contratação, em relação às normas de privacidade**, a partir do qual as partes poderão definir a estratégia adequada e adotar cláusulas compatíveis e proporcionais a tal risco. Em outras palavras, é importante que se defina a relevância do tratamento de dados para a operação.

Portanto, os agentes devem proteger seus interesses na medida do possível e dentro do que se entende como economicamente viável para aquele momento. Essa verdade é especialmente relevante para a área de proteção de dados, que intrinsecamente trabalha com assunção de riscos.

Torna-se importante que, no momento da negociação contratual para inserção de novas cláusulas de proteção de dados ou revisão das relações já existentes, os Agentes de Tratamento estejam preparados também para dar alternativas de negociação e flexibilizar, dentro do possível, a redação – mas não o cumprimento da legislação - caso a parte contrária não esteja de acordo com as disposições propostas.

Assim, ao analisar um contrato e a fim de calibrar os riscos inerentes à relação entre os agentes, é necessário entender quais **categorias, natureza e criticidade do fluxo dos dados pessoais** estão envolvidas na execução das atividades daquele contrato, como:

- quais as finalidades de cada uma das operações
- qual o volume e quais os tipos de dado tratados
- se há dados de menores, especialmente de crianças e vulneráveis
- se há dados ou registros criminais
- se alguma atividade da operação fará uso de tecnologias inovadoras e disruptivas
- se haverá por alguma razão o monitoramento de comportamento ou hábitos
- transferência internacional
- compartilhamento com algum terceiro
- se é um contrato de curto ou longo prazo

Superado também o entendimento quanto ao fluxo dos dados pessoais, à mensuração dos riscos envolvidos nas atividades, bem como às delimitações de responsabilidades das partes envolvidas, **cláusulas-padrão poderão ser utilizadas como ponto de partida para a personalização do cenário existente e criação de um clausulado mais robusto** e que mais se encaixe à realidade dos Agentes de Tratamento em questão.

**Dessa maneira, tais contratos, de forma exemplificativa, podem prever cláusulas que incluam:**

- Limitação de finalidade dos dados;
- Obrigação de alocação de multa por descumprimento da LGPD;
- Previsão de auditorias recorrentes;
- Definição do grau de colaboração e assistência entre as partes, contendo o prazo e a forma de comunicação e notificação entre elas tanto no caso de atendimento a direitos dos titulares quanto a prazos de incidentes de segurança da informação envolvendo dados pessoais oriundos da relação firmada;
- Aspectos referentes ao armazenamento e à destruição dos dados pessoais até o término do objeto do contrato, considerando obrigações legais que requerem a referida manutenção.

Por fim, considerando a própria natureza do contrato, focada em evitar lacunas e confusões sobre quais regras aplicar em caso de conflito entre partes contratantes, é preciso ter especial atenção para a sobreposição de normas que constam em cláusula ou anexo de privacidade e em outras cláusulas do contrato.

É recomendável, nesse sentido, a análise do documento e **verificação da adequação das demais** cláusulas constantes no contrato para que não haja conflito entre os dispositivos ali mencionados, inclusive os comerciais, especialmente em relação à limitação de responsabilidade entre os agentes e aspectos da confidencialidade e aplicação de eventuais multas.

Enquanto documento autônomo, que sobrevive ao tempo e aos seus autores, um contrato assinado pode não mostrar, de imediato, todo o esforço das organizações em elaborá-lo, equalizando tanto expectativas quanto limitações. Nesse sentido, a elaboração de um instrumento contratual é mais do que uma atividade meramente formal por parte dos Agentes de Tratamento.

Na realidade, diante de tudo o que foi exposto acima, resta claro que a elaboração de um instrumento contratual, abarcando aspectos inerentes ao tratamento de dados pessoais entre Agentes de Tratamento, ultrapassa a finalidade basilar de condução da relação jurídica e negocial estabelecida entre partes, englobando perspectiva de demonstração de boas práticas e diligências, tanto com parceiros externos quanto com a ANPD.

O estabelecimento de regras em contratos é, em verdade, uma oportunidade para que as organizações possam regular pontos que trarão maior previsibilidade e segurança jurídica para um negócio e, em especial, para as formas de lidar com problemas futuros, traduzindo-se em uma análise estratégica da mensuração e alocação de riscos pelo próprio agente de tratamento.

---

Artigo elaborado em coautoria por ***Maria Eduarda Annarumma Guedes***, ***Gabriel Nantes Gimenez***, ***Gabriela Bueno*** e ***Ana Rita Bibá Gomes de Almeida***, advogados do Opice Blum, Bruno e Vainzof Advogados Associados.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

# Controle de Contratos

***Por Caio César Carvalho Lima***

Como observamos em outros textos desta cartilha, com a eficácia da LGPD (Lei Geral de Proteção de Dados), novas regras para o tratamento de dados pessoais foram estabelecidas. Com isso, toda operação que tenha por objetivo a oferta ou o fornecimento de bens ou serviços e que envolva o tratamento de dados pessoais no Brasil está sujeita a essa legislação.

Em decorrência disso, é muito importante que os agentes de tratamento de dados pessoais (controladores ou operadores) sigam determinadas regras e certos procedimentos para que os contratos nas organizações estejam em conformidade com a LGPD. Abaixo são trazidos os 5 passos mais relevantes para alcançar isso:

## 1 • Análise dos tipos de contratos e dos dados tratados

Para que seja feita a adequação dos contratos, há necessidade de analisar individualmente os tipos de instrumentos celebrados pela empresa, a fim de determinar as obrigações e responsabilidades de cada uma das partes, de acordo com a LGPD, bem como os pontos principais da atividade de tratamento regulada. É importante entender principalmente:

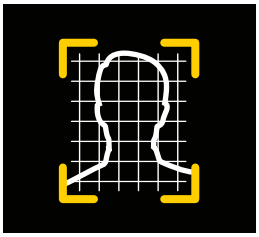
- O tipo de dado tratado (se inclui dados sensíveis, pseudonimizados, de crianças e adolescentes ou outros grupos vulneráveis);
- O volume dos dados (quanto maior o volume, maiores os riscos aos titulares);
- Posição do agente de tratamento (controlador ou operador); e
- Se há transferência internacional.

## 2 • Definição das cláusulas contratuais

Após essa análise, é o momento de definir as cláusulas mais indicadas ao caso concreto, a fim de mitigar os riscos jurídicos previsíveis, relacionados à privacidade e à proteção de dados.

Nesse ponto, importante observar que o ideal é que as companhias possuam quatro modelos de cláusula para cada um dos tipos de dados que tratarem:

**Dados pessoais sensíveis**



**Dados pessoais**

**Dados pseudonimizados**

**Dados anonimizados**

Dessa forma, haverá o equilíbrio na proteção contratual dos dados, de acordo com o risco e a criticidade que representarem às companhias.

## 3 • Análise de especificidades

É importante, ainda, observar questões particulares que podem ser relevantes, a depender de cada situação que se esteja protegendo:

- Cláusula de limitação de responsabilidade;
- Compartilhamento de dados com terceiros;
- Resposta a incidentes de segurança da informação;
- Auditoria; e
- Atendimento aos direitos dos titulares.

## 4 • Validação interna

Após finalização do texto, caso haja necessidade, criar tratativas com as áreas internas da empresa para verificação e validação das disposições contratuais elaboradas.

## 5 • Envio à contraparte

Após finalização do texto, envio dos aditivos às contrapartes e participação nas negociações que forem necessárias, a fim de que se consiga chegar à assinatura do instrumento. É importante, naturalmente, garantir a efetiva assinatura do instrumento, a fim de que possa produzir os efeitos jurídicos esperados.

Há caminhos a serem percorridos para que a organização controle adequadamente seus contratos à luz da LGPD. Agindo dessa forma, riscos serão mitigados e, na eventualidade de algum evento adverso, a companhia estará protegida para responder da melhor forma possível.

E, para que se consiga alcançar esse controle na prática, o Encarregado pelo Tratamento de Dados (também conhecido como DPO – Data Protection Officer) da companhia deve ser devidamente comunicado acerca de cada novo produto ou serviço que vier a ser contratado ou oferecido e que trate dados pessoais.

***Caio César Carvalho Lima***
Advogado e sócio do Opice Blum, Bruno e Vainzof Advogados Associados.

# Simulação de incidentes envolvendo dados pessoais

***Por Rony Vainzof***

Agentes de tratamento devem identificar e responder a potenciais incidentes envolvendo dados pessoais de forma rápida e eficaz, em que pese a identificação desses eventos nem sempre ser simples. Não são raros os casos em que os sistemas permaneceram invadidos e sob ameaça durante meses, antes de constatados e combatidos os ataques.[1]

Confirmado o incidente, é preciso entender com maior nível de detalhamento sua extensão, com atuação multissetorial da organização, de acordo com seu plano de resposta já previamente definido, o qual deve incluir, entre outras medidas:[2]

- Formação do comitê de crise;
- Preservação das evidências;
- Identificação da causa-raiz;
- Contenção da vulnerabilidade;
- Identificação se houve ou não exposição de dados;
- Elaboração do score de gravidade do incidente;
- Avaliação sobre eventual comunicação aos titulares dos dados, às autoridades e/ou parceiros de negócios;
- Plano de comunicação; e
- Relatório forense.

[1]De acordo com pesquisa divulgada pela IBM, o tempo médio global para identificação e contenção de incidente é de cerca de 280 dias; olhando apenas para o Brasil, esse número sobe para 380 dias. Fonte: IBM Security – Cost of a Data Breach Report 2020. Disponível em: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/. Acessado em 12.06.2021.

[2]Para mais informações, confira a cartilha "Como Identificar e Reagir a Incidentes de Segurança da Informação", Opice Blum, Bruno e Vainzof Advogados Associados. Março de 2021. Disponível em: https://opiceblum.com.br/wp-content/uploads/2021/02/Cartilha-Como-identificar-e-reagir-a-incidentes-de-seguranca.pdf. Acessado em 12.06.2021.

Porém, para que a organização esteja ainda mais bem preparada para agir, é fundamental a realização de simulações periódicas, de forma a compreender o seu grau de maturidade para lidar, de maneira efetiva, com eventuais incidentes de segurança e seus respectivos desdobramentos.

Para se ter uma ideia da importância da simulação, a preparação para a resposta a incidentes foi o fator que mais reduziu o prejuízo médio das empresas que sofreram algum tipo de violação de segurança em 2020: a redução de custos médios com equipes de resposta a incidentes e treinamentos/simulações foi de US$ 2 milhões (aproximadamente R$ 10 milhões), em comparação com empresas que não possuíam profissionais bem preparados e treinados[3].

Outro objetivo da simulação é preparar a alta gestão e os profissionais do comitê de crise das organizações para atuar de maneira preventiva, e em todas as fases relevantes após um incidente, para que saibam o que fazer e quando fazer, criando "memória muscular" dos tempos e movimentos de suas ações e obrigações, o que deve abordar aspectos técnicos/operacionais e jurídicos.

Usualmente, de acordo com o comitê de crise estabelecido por cada organização, devem participar das simulações profissionais de nível estratégico e tático que atuarão nos eventos, como, além do Encarregado (DPO), os dos departamentos Jurídico, Segurança da Informação, Compliance, TI, RH e Relações Públicas.

[3] IBM Security – Cost of a Data Breach Report 2020. Disponível em: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/. Acessado em 12.06.2021.

As simulações devem ser periódicas e acompanhar a evolução dos tipos de incidentes, de vulnerabilidades e de ataques cibernéticos existentes, tais como:

- simulação de acesso não autorizado;
- perda/roubo de equipamentos;
- exfiltração de dados ou informações (pessoais ou corporativas);
- extorsão (como ransomware); e
- interrupção de serviços, apenas para citar alguns exemplos.

Previamente às simulações, a organização deve avaliar qual departamento é o responsável pela investigação; quais outros departamentos devem estar envolvidos; quem compõe a equipe principal e a estendida de resposta a incidentes; quais documentos ou evidências existentes para guiá-los; quais políticas internas precisam ser consideradas; se há necessidade de especialistas externos.

**Assim, as simulações envolverão:**

- Análise da documentação interna existente (incluindo plano de resposta a incidentes, se houver), de forma a personalizar a simulação às normas internas da organização, bem como avaliar sua real eficácia e adequação legal em face a um incidente;

- Roteiro do exercício a ser aplicado, definição das áreas e dos profissionais que serão envolvidos, orientações sobre a execução do procedimento e demais esclarecimentos. Em suma, o passo a passo do procedimento;

- **Identificação e orientação dos pontos focais de contato ou facilitadores:** as pessoas que fiscalizarão todo o processo;

- **Material necessário à realização do exercício:** template de lista de presença e identificação de colaboradores envolvidos; template de orientações para a condução e realização do exercício; template de planilha de feedback sobre o exercício; e regras de engajamento do exercício;

- **Cronograma:**

  - Apresentação inicial teórica para dar visibilidade ao tema e ressaltar a importância do exercício a ser aplicado;

  - Esclarecimentos de dúvidas sobre o procedimento (informações sobre como a simulação será efetivamente implementada e quais recursos técnicos e normativos serão usados, bem como variáveis a serem introduzidas);

  - Acompanhamento por especialistas durante a realização do exercício/da simulação para discussão das situações envolvendo os principais aspectos operacionais e jurídicos em um incidente de segurança de dados, tais como:

- **A** indicação de procedimentos de identificação e coleta de evidências;

  **B** identificação do tipo de violação de dados que está sendo simulado;

  **C** condução de entrevistas com colaboradores envolvidos no incidente;

  **D** notificação e prestação de contas à ANPD ou outras autoridades;

  **E** notificação ao titular de dados pessoais ou a terceiros e resposta a questionamentos;

  **F** comunicação com a imprensa e o mercado.

- Documentação das discussões, dos processos existentes, dos esforços de mitigação que são testados e das perguntas que surgem;

- Apresentação de Relatório Final de Simulação de Incidente de Segurança – RSIS contendo ao menos:

  **A** a descrição detalhada de todo o processo de simulação;

  **B** eventuais falhas identificadas;

  **C** sugestão de medidas de correção jurídicas a serem adotadas para a conformidade plena à LGPD ou outras normas aplicáveis;

  **D** formulário de risco cibernético, demonstrando as principais fragilidades e necessidades internas.

Após as simulações, a organização deverá ser capaz de[4]:

- Classificar ameaças cibernéticas, com relação ao risco corporativo que propõem, de acordo com a combinação de ativos de negócio;
- Diferenciar entre ameaças cyber de TI e ameaças cyber de negócio;
- Criar uma estratégia de mitigação de riscos corporativos com base no panorama de ameaças daquele território onde a empresa opera;
- Defender e contrastar visões sobre como o risco cibernético deve ser mitigado dentro da corporação, no nível executivo e linguagem de negócio;
- Adotar as medidas de preservação de evidências do evento e de procedimentos realizados de forma a manter a sua validade jurídica como meio de prova;
- Identificar o tipo de violação de dados e as medidas jurídicas correspondentes a serem adotadas em cada caso (como notificação a autoridades competentes, comunicados ao mercado, adoção de medidas judiciais, dentre outras).

[4]Conteúdo elaborado em conjunto com a empresa Ventura Academy.

Assim, as simulações ajudam as organizações a enfrentar e responder aos diferentes cenários de risco e ameaças, sendo um instrumental relevante para incentivar a discussão e a colaboração.

Mais do que isso, as simulações de incidentes também contribuem para a diminuição do prejuízo quando da ocorrência desses maléficos eventos, assim como para a demonstração de evidências de suas diligências preventivas, em conformidade com os princípios da LGPD de responsabilização e prestação de contas e prevenção, respectivamente.

***Rony Vainzof***
Advogado, professor e árbitro especializado em Direito Digital e Proteção de Dados. Sócio do Opice Blum, Bruno e Vainzof Advogados Associados. Coordenador e professor do MBA em Direito Eletrônico da Escola Paulista de Direito e do Curso de Extensão em Proteção de Dados da FIA. Mestre em Soluções Alternativas de Controvérsias Empresariais pela Escola Paulista de Direito. Diretor do Departamento de Defesa e Segurança e responsável pelo Grupo de Trabalho de Defesa Cibernética da Federação das Indústrias do Estado de São Paulo (FIESP).

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

# Reavaliação contínua do nível de maturidade

***Por Marcos Gomes da Silva Bruno***

Por essência, entre outras questões, a conformidade com a privacidade e proteção de dados pessoais corresponde ao atingimento, pela empresa, de um nível de maturidade minimamente satisfatório com a proteção desses ativos tão valiosos e relevantes, ao estabelecer uma estrutura de governança ao redor de um novo risco, representado pelos dados pessoais.

Em paralelo a isso, um dos princípios da Lei 13.709/18 (Lei Geral de Proteção de Dados) é o da prestação de contas, definido no artigo 6º, inciso X, da Lei como a "demonstração (...) da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas".

Portanto, além da avaliação do nível de maturidade ser importante para garantir aos gestores de privacidade da companhia que suas práticas de privacidade e proteção de dados estão em nível adequado à legislação e ao mercado, também pode servir como importante instrumento de prestação de contas às autoridades, o que torna seu papel ainda mais relevante à organização.

No entanto, assim como esse nível de maturidade pode se elevar pela otimização constante do programa de privacidade da companhia, ele também pode se degradar frente à alteração do estado da técnica, ou até mesmo em decorrência da inobservância do risco da privacidade em novas iniciativas da empresa.

Justamente por isso, é recomendável que o nível de maturidade da empresa em relação à governança de dados pessoais seja reavaliado de forma contínua, o que se torna uma importante atribuição do Encarregado pelo Tratamento de Dados Pessoais.

Não há tempo certo ou errado para a periodicidade da reavaliação, até porque se trata de boa prática, e não de uma exigência regulatória. Idealmente, a periodicidade do processo de reavaliação pode variar, de acordo com o negócio principal da companhia e a velocidade com que a inovação permeia aquele ambiente.

A partir desse princípio, evidente que uma empresa cujo negócio principal envolve o tratamento de dados pessoais, e que tem a inovação muito presente, deverá realizar esse processo de reavaliação em menor intervalo de tempo, ao passo que uma empresa cujo negócio principal não está diretamente relacionado ao tratamento de dados pessoais, e se move mais lentamente no que tange à atualização e inovação tecnológica, pode fazer essa reavaliação em um intervalo maior.

No tocante à estrutura do processo de reavaliação do nível de maturidade da companhia, é importante que ele seja construído de acordo com os ativos de dados pessoais gerenciados pela empresa, sua posição enquanto agente de tratamento de dados, com as melhores práticas do mercado e a observância do aspecto regulatório.

Aprofundando um pouco a questão do aspecto regulatório, para a finalidade da reavaliação aqui proposta, é importante que a empresa tenha mapeadas todas as Leis às quais se subordina e que tenha provisões específicas de privacidade e proteção de dados, de modo a observar todo o espectro regulatório aplicável, e não apenas a Lei Geral de Proteção de Dados. A partir desse conjunto de Leis e Normas aplicáveis, é recomendável que a empresa crie uma estrutura de avaliação baseada em pilares, que cubram a totalidade dessas legislações.

Seguindo esses passos, a empresa terá uma estrutura de avaliação objetiva, auditável, documentável e que facilmente poderá ser aplicada no intervalo apropriado, a ser definido pelo Encarregado pelo Tratamento de Dados Pessoais, conforme os critérios acima, o que vai assegurar a manutenção do nível de conformidade da empresa com a proteção da privacidade e proteção de dados, bem como garantir a prestação de contas às autoridades, se necessário.

***Marcos Gomes da Silva Bruno***
Sócio do Opice Blum, Bruno e Vainzof Advogados Associados.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

# Plano de Treinamento e Comunicação

***Por Gisele Karassawa e Ana Catarina de Alencar***

Muitos são os relatos de incidentes de segurança e golpes aplicados em empresas devido a falhas humanas. Colaboradores sem treinamento e capacitação podem fazer de suas empresas vítimas de hackers e vazamentos não intencionais.

Por isso, de nada adiantará a empresa cumprir todas as etapas de um programa de conformidade à Lei Geral de Proteção de Dados (LGPD)[1] se o seu quadro interno de colaboradores manipula dados pessoais de forma inadequada. Uma compreensão satisfatória das principais diretrizes da LGPD é um requisito essencial e poderá afetar o trabalho da organização como um todo.

Em pesquisa realizada pela Cisco em 2019[2], foram identificados índices relevantes do impacto positivo nos negócios das empresas que se adequaram à General Data Protection Regulation - GDPR[3], tais como 42% de ganho em agilidade e inovação por possuir maior controle sobre os dados, 41% de aumento de vantagem competitiva em relação a outras empresas, 41% de alcance de maior eficiência operacional, por ter os dados organizados e catalogados, 39% de redução de perdas relacionadas a incidentes de segurança com dados pessoais.

---

[1]Lei Federal nº 13.709/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12.05.2021.

[2]Cisco´s Data Privacy Benchmark Study, 219. Disponível em https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf

[3]Regulation (EU) 2016/679 (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 12.05.2021.

Assim como ocorre no contexto do GDPR, a LGPD não traz regras específicas sobre como deve ser o Plano de Treinamento e Comunicação dos agentes de tratamento. Entretanto, o treinamento dos colaboradores e iniciativas de comunicação interna, incluindo campanhas e ações educativas, são medidas fundamentais para um accountability eficaz junto à Autoridade Nacional de Proteção de Dados.

Conforme disciplina o artigo 6º, "x"[4], da LGPD, os agentes de tratamento deverão prestar contas de sua conformidade mediante demonstração de medidas eficazes no cumprimento da lei. Além disso, conforme dispõe o artigo 50 do referido diploma legal, os agentes de tratamento poderão formular regras de boas práticas, incluindo "ações educativas e mecanismos internos de supervisão"[5].

Assim, ainda que não exista menção expressa à obrigatoriedade da realização de treinamentos e ações de comunicação interna sobre a matéria, com base em uma interpretação sistemática da LGPD, conclui-se que o Plano de Treinamento e Comunicação é uma das ações essenciais para a demonstração de conformidade e *accountability* eficazes.

[4]"Art. 6º, X - responsabilização e prestação de contas: demonstração, 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".

[5]"Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais".

Como a LGPD não especifica os parâmetros mínimos do Plano em questão, ficará a critério do Encarregado de Proteção de Dados (DPO) determinar o conteúdo, formato, público-alvo e demais detalhes do treinamento e ações educativas, segundo as necessidades e os riscos do negócio.

Importante destacar que a cultura de proteção de dados não se constrói de maneira imediata e depende de um forte alicerce que deve começar a ser construído pela liderança da instituição, proporcionando as ações educativas apropriadas e reforçando a importância destas ao time.

Um treinamento geral para colaboradores deve nivelar o conhecimento sobre a Lei Geral de Proteção de Dados na empresa, a fim de que todos, independentemente da posição ocupada, possam conhecer as nuances principais da LGPD.[6] Por isso, essa capacitação deve incluir alguns itens essenciais como:

- **uma explicação sobre objetivos da LGPD**
- **uma descrição dos seus princípios básicos e como se aplicam à realidade da empresa**
- **uma explicação abrangente sobre a Política de Privacidade da empresa e outros documentos aplicáveis**
- **informações sobre canais de comunicação para dúvidas e/ou reporte de incidentes**

[6] Disponível em: https://ico.org.uk/for-organisations/accountability-framework/training-and-awareness/. Acesso em: 12.05.2021.

Além disso, é recomendável que os treinamentos de proteção de dados incluam aspectos básicos de segurança da informação, de maneira que a equipe possa identificar eventuais ameaças em suas rotinas de trabalho. É importante, por exemplo, que colaboradores dos mais diversos setores saibam:

I reconhecer um ataque de *phishing*;
II seguir as políticas de senhas; e
III não conceder acesso não autorizado a terceiros etc.

Em síntese, os treinamentos gerais devem ser simples e objetivos, contando com a disponibilização dos materiais utilizados para consulta pelos colaboradores e *surveys* para uma avaliação geral de compreensão do conteúdo. Ao final de um treinamento, colaboradores devem ter compreendido como a empresa utiliza dados pessoais e por quais motivos, quais os riscos envolvidos e quais as medidas adotadas pela empresa para mitigá-los.

É necessário destacar que o Encarregado de Proteção de Dados (DPO) possui uma função estratégica na criação de uma cultura de privacidade na organização. Essa figura, estabelecida pela LGPD, é responsável por estruturar iniciativas de conscientização sobre o tema, fornecendo treinamento adequado às equipes de acordo com os riscos verificados dentro de cada área e/ou posição específica. Nesta linha, é possível, por exemplo, que departamentos como marketing, tecnologia da informação e recursos humanos exijam capacitações específicas com base no tipo de dado pessoal que manuseiam e obrigações decorrentes.

Assim, além de contar com conhecimentos gerais, algumas equipes necessitam conhecer processos e procedimentos internos com maior riqueza de detalhes. É possível que esses times precisem compreender algumas regras específicas, incluindo:

I por quanto tempo devem manter os dados pessoais armazenados;
II o que devem fazer no caso de uma solicitação encaminhada por um titular de dados pessoais;
III quais ações devem ser tomadas para o gerenciamento de crises na segurança de sistemas e redes etc.

Treinamentos são o ponto de partida para permitir o entendimento da sistemática de proteção de dados que é complementada pelas diretrizes e pelos documentos de governança corporativa.

Em suma, o ponto fundamental do Plano de Treinamento e Comunicação consiste em fazer com que todos os envolvidos compreendam os princípios da LGPD, as medidas adotadas pela empresa e os riscos para o negócio, dos pontos de vista jurídico, financeiro e reputacional. Adicionalmente, é imprescindível que as medidas disciplinares eventualmente aplicáveis à conduta inadequada de colaboradores, envolvendo casos de suspensão e demissão, sejam comunicadas de forma clara e eficaz.

Neste ponto, a manutenção dos registros de treinamento, incluindo o aceite dos colaboradores nos documentos pertinentes e lista de presença, é de extrema importância para demonstrar a conformidade e punir os casos considerados graves, de acordo com as diretrizes de compliance da empresa.

Por fim, o Encarregado de Dados Pessoais deverá ter em mente que o Plano de Treinamento e Comunicação deve ser revisto periodicamente, incluindo novas iniciativas de conscientização interna e renovação dos treinamentos já ministrados. A observância de todos esses aspectos na construção do Plano de Treinamento e Comunicação é fundamental para o sucesso de qualquer programa de governança.

***Gisele Karassawa***
Gestora da área Startup.OBA no Opice Blum, Bruno e Vainzof Advogados Associados. Graduada em Direito pelo Instituto Presbiteriano Mackenzie. Graduada em Comunicação Social com ênfase em Publicidade pela Universidade Paulista. Especialista em Propriedade Intelectual, Direito do Entretenimento e Mídia pela Escola Superior de Advocacia e em Direito das Novas Tecnologias pelo Instituto Internacional de Ciências Sociais.

***Ana Catarina de Alencar***
Advogada da área Startup.OBA no Opice Blum, Bruno e Vainzof Advogados Associados. Mestre em Teoria do Direito e Filosofia do Direito pela Universidade Federal de Santa Catarina (UFSC). Especialista em Direito Digital e Compliance. Colunista nas áreas de Direito, Inovação e Inteligência Artificial. Professora no curso de graduação em Direito da Unisociesc/Anima. Membra do Conselho Editorial da Revista da OAB/Joinville.

# CRÉDITOS

**SÓCIOS**
José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio Lima
Danielle Serafino

**COORDENAÇÃO EDITORIAL**
Bruno Toranzo

**REVISÃO**
Rony Vainzof
Caio Lima
Bruno Toranzo
Yasmin Brandão

**ARTE E DIAGRAMAÇÃO**
Paola Cosentino

**ESTAGIÁRIO**
Lucas Souza Fernandes

## CONTEÚDO JURÍDICO

Ana Catarina de Alencar
Ana Rita Bibá Gomes de Almeida
Caio César Carvalho Lima
Gabriela Bueno
Gabriel Nantes Gimenez
Gisele Karassawa
Guilherme Guimarães Vieira
Helena Dominguez Paes Landim
Helena Rodrigues Vaz Pedrosa
Henrique Fabretti Moraes
Marcella Costa
Maria Beatriz Previtali
Maria Eduarda Annarumma Guedes
Marcos Gomes da Silva Bruno
Renato Opice Blum
Rony Vainzof
Tiago Neves Furtado

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF