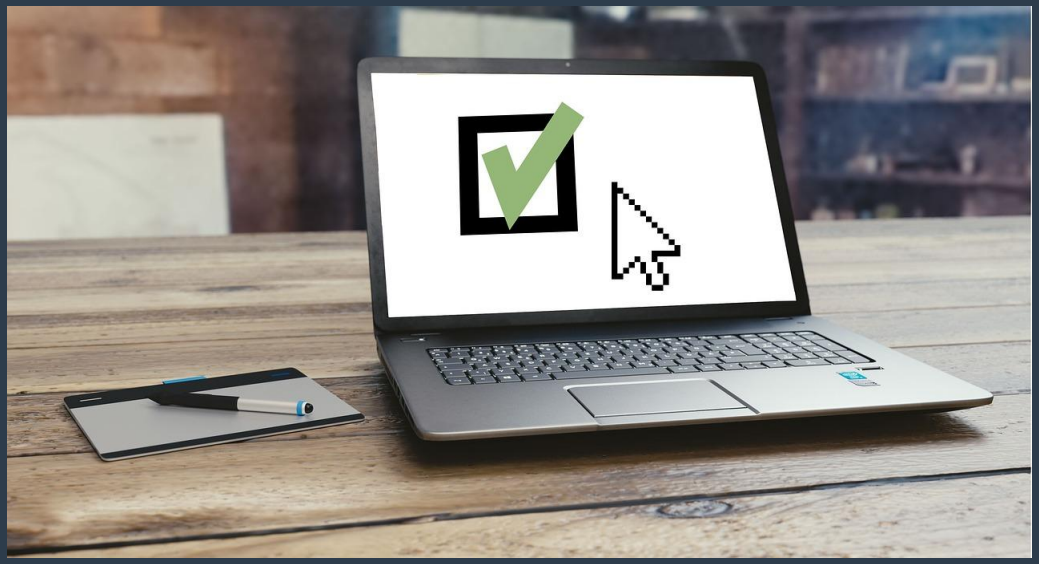


Políticas de Privacidade

Um guia prático para a construção de uma política de privacidade conforme a Lei Geral de Proteção de Dados
Conceitos & Checklist

By LGPD Academic

Índice

Organização

- **Adriana Tocchet Wagatsuma**

https://www.linkedin.com/in/adriana-tocchet-wagatsuma/

- **Angela Maria Rosso**

https://www.linkedin.com/in/angela-maria-rosso/

- **Remilina Yun**

https://www.linkedin.com/in/remiyun/

O trabalho Políticas de Privacidade - Um guia prático para a construção de uma política de privacidade conforme a Lei Geral de Proteção de Dados - Conceitos & Checklist de
Adriana Tocchet Wagatsuma; Angela Maria Rosso; Carolina Braga; Clarisse De La Cerda; Henriete Fejes; Ingrid Ferreira; Karyne F. Barbosa; Remilina Yun (Remi); Vanessa Pareja Lerner está licenciado com uma

Licença Creative Commons - Atribuição 4.0 Internacional.
Crédito das imagens: www.pixabay.com

Introdução

Em meados de 2018, navegando pelo LinkedIn, encontrei a publicação de um advogado carioca que não conhecia - Dirceu Santa Rosa.

O advogado simpaticamente convidava os mais diversos profissionais a participarem de um grupo, via WhatsApp, que ele estava criando para fomentar os estudos e discussões sobre a lei europeia de proteção de dados, a GDPR (General Data Protection Regulation), que havia acabado de entrar efetivamente em vigor na Europa. Imediatamente me interessei.

Os eventos de GDPR multiplicavam-se em São Paulo e as questões de privacidade e proteção de dados faziam cada vez mais parte do meu dia-a-dia. As discussões eram interessantíssimas. O grupo reunia profissionais de diversos perfis e graus de experiências: advogados, profissionais de tecnologia da informação, *compliance*, auditoria, acadêmicos; iniciantes e especialistas no tema. Representantes da iniciativa privada e da iniciativa pública também. O grupo acompanhou a promulgação da Lei Geral de Proteção de Dados - 13.709/18 (LGPD), os vetos presidenciais e, logo depois, a publicação da Medida Provisória 869/18, que criava, enfim, a Autoridade Nacional de Proteção de Dados (ANPD) brasileira.

Os grupos aumentaram e logo surgiu um para discutir a nossa lei local e, por iniciativa da Remilina Yun (Remi), participante ativa das discussões, nasceu um grupo acadêmico, do qual todas as autoras deste *e-book* fazem parte.

O propósito era fatiar a lei e criar projetos que a discutissem a partir de um enfoque prático, criando literatura sobre a matéria.

Nosso subgrupo optou por tratar sobre as políticas de privacidade — aqueles textos imensos e indecifráveis que estão lá, em qualquer *website* ou aplicativo.

As políticas de privacidade sempre foram alvo de críticas, sejam pelo tamanho, pela falta de clareza, por não serem funcionais. Não é raro ouvirmos expressões como **"não li e concordo"**.

A intenção era criar um material bastante didático, de abordagem simples e objetiva, tanto é assim que a primeira ideia foi de desenvolvermos um checklist e glossário que auxiliassem na elaboração das políticas, observando-se todos os novos requisitos da LGPD, algo inédito no Brasil, já que agora não bastarão para as políticas estarem nos *websites*. As políticas de privacidade agora deverão ser plenamente efetivas e, para isto, antes de ser um documento jurídico, terão um caráter eminentemente informativo.

Assim, os antigos padrões deverão ser revistos! As políticas terão que ser reinventadas. A linguagem, o tamanho, o formato, o que solicitam, de que forma fazem isso… A política deverá empregar linguagem simples, de fácil compreensão. Utilizar o idioma natal da localidade em que os serviços ou produtos serão ofertados.

O usuário que navega — titular dos dados pessoais — deverá, ao lê-la, ter esclarecidas todas as suas dúvidas sobre a coleta, utilização, armazenamento e descarte dos seus dados. E, caso ainda restem perguntas, a que canal ou canais deverá recorrer.

Enfim, o caminho para a adequação é longo.

Esperamos que o nosso guia possa ser útil na jornada de implementação da LGPD e na construção da cultura; *awareness* da proteção de dados e confiança digital. E que cada leitor possa exercer seu importante papel para que estes temas sejam cada vez mais acessíveis e que estejam ao alcance de todos. Que a educação digital torne-se uma pauta da sociedade brasileira.

Desta forma, esta obra está licenciada e poderá ser reproduzida, com fins particulares e comerciais, desde que sua fonte e autoria sejam citadas.

Aproveitamos para registrar aqui o nosso muito obrigada ao Dirceu, que com sua iniciativa fomentou tantas outras e criou laços que vão muito além dos debates da LGPD.

Boa leitura!

Adriana Tocchet Wagatsuma

Sobre as Autoras

Adriana Tocchet Wagatsuma

- Advogada corporativa generalista, com mais de 20 anos de experiência no setor automobilístico;
- Especialista em Direitos difusos e coletivos, pela PUC-SP;
- Cursos especializantes no Data Privacy e na ESA em Direito Digital, Proteção e Privacidade de Dados;
- Supervisora de Assuntos Legais e Compliance na Ford Motor Company Brasil Ltda.;
- Bacharel em Direito pela Faculdade de Direito de São Bernardo do Campo-SP.

Angela Maria Rosso

- Cientista da Computação especialista em privacidade e proteção de dados;
- Consultora em adequação à LGPD e Políticas de Segurança da Informação ISO 27001;
- Administradora de Redes (Serpro);
- Pesquisadora do DUN@ - Grupo de Estudo e Pesquisa em Tecnologia, Direito e Inclusão;
- Pós Graduada em Direito Digital;
- Bacharel em Ciências da Computação (UNIOESTE);
- Bacharelanda em Direito (FAG).

Sobre as Autoras

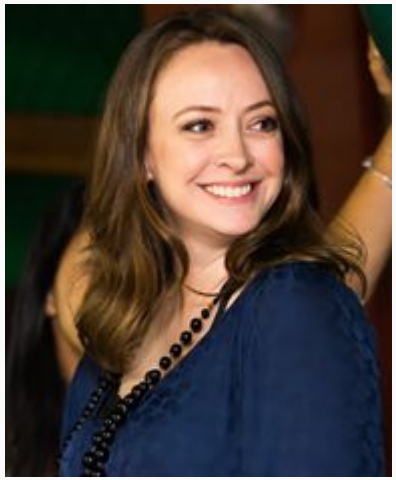
Carolina Braga

- Consultora de tecnologia da MJV;
- Advogada;
- Palestrante;
- Pós-graduada em Direito Digital e *Compliance* pela Faculdade Damásio;
- Mestranda em Princípios Fundamentais e Novos Direitos pela UNESA;
- Associada da AB2L;
- Pesquisadora em Direito e Tecnologia no Droit (PUC-Rio).

Clarisse De La Cerda

- Advogada especialista em Contratos de Transferência de Tecnologia;
- Bacharel em Direito pela Universidade do Estado do Rio de Janeiro;
- Mestre em Propriedade Intelectual e Atividades Empresariais pela Universidade do Estado do Rio de Janeiro;
- LLM em Lei, Ciência e Tecnologia pela Universidade de Stanford (CA);
- Bolsista da Fundação Carlos Chagas Filho de Amparo à Pesquisa do Rio de Janeiro em Dissertação sobre Patenteamento de Sequências Genéticas.

Sobre as Autoras



Henriete Fejes

- Gerente do time de Tecnologia no escritório PK Advogados;
- 15 anos de experiência em Contratos, Negociações Complexas, Propriedade Intelectual, Mídia e Entretenimento, Direito Digital, Tecnologia e Inovação; bitcoin, blockchain, proteção de dados, direito autoral, entre outros;
- Graduada em Direito pela Universidade Presbiteriana Mackenzie (2004) e Pós Graduada em Direito Civil pela mesma universidade (2008), atualmente cursando o MBA executivo de Gestão Empresarial na FIA-USP.

Ingrid Ferreira

- Atuação nas áreas de direito empresarial, com foco em regulatório e entretenimento;
- Especialista em Propriedade Intelectual pela Fundação Getúlio Vargas;
- Especialista em Direito e Tecnologia da Informação pela Universidade de São Paulo;
- Cursos especializantes no Data Privacy e na IAPP em Proteção de Dados;
- Atualmente à frente do departamento jurídico da Viacom Networks no Brasil.

Sobre as Autoras

Karyne F. Barbosa

- Advogada desde 2014;
- Pós-graduanda em Direito do Trabalho (UNIRN);
- Estudando com afinco o universo do Direito Digital e Tecnologias.

Remilina Yun (Remi)

- Consultora Auditoria Investigativa - Suzano Papel & Celulose;
- Especialista em Gestão de Riscos e *Compliance*;
- Profissional com experiência em Auditoria Interna e Investigações de Fraudes;
- Experiência em implementação e gestão de Canal de Denúncias;
- Tutora da Trilha Fraudador Cibernética pelo Instituto de Pesquisa do Risco Comportamental (IPRC);
- Gestão de Projetos pela Universidade de Ohio – LAIOB;
- MBA Gestão de Risco e *Compliance* pela Trevisan;
- Bacharel em Direito pela Universidade Presbiteriana Mackenzie.

Sobre as Autoras

Vanessa Pareja Lerner

- Sócia do Dias Carneiro Advogados;
- Atuante no mercado de tecnologia, videogames/ eSports e mídia & entretenimento;
- Assessoria em contratos comerciais em geral, atuando de forma especializada com proteção de dados, propriedade intelectual e na estruturação de negócios na área de tecnologia;
- Formada em Direito pela PUC/SP;
- Especialização em Propriedade Intelectual pela GV Law e LLM em Direito, Ciência e Tecnologia da Stanford University.;

Capítulo 1

Reflexos da LGPD e da GDPR nas Políticas de Privacidade

Por Adriana Tocchet Wagatsuma

Reflexos da LGPD e do GDPR nas Políticas de Privacidade

As novas regulamentações sobre proteção de dados pessoais são uma tendência global e todas elas, da lei brasileira à californiana, têm grande inspiração na lei europeia: a *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados ou GDPR).

A Europa, muito embora contasse com diretivas que regulassem fortemente esta questão, saiu na frente e imprimiu ao globo um padrão mundial; rígido, de fato, mas necessário.

A GDPR veio como uma reação do bloco europeu aos casos de espionagem feitos pelo governo dos Estados Unidos, revelado por Edward Snowden.

O Brasil, em que se discutia há anos e que, inclusive, já havia reagido com o Marco Civil da Internet, viu-se acuado economicamente e optou, enfim, por regulamentar a matéria. Legislações e princípios esparsos foram compilados e organizados em forma de lei geral; a LGPD, que passará a produzir, em agosto de 2020, seus efeitos.

Em linhas gerais, os marcos regulatórios são construídos com base em princípios que devem nortear todo o processo que envolve a utilização de dados pessoais; desde a solicitação de tais dados até o seu descarte. O princípio central é o da *Accountability* ou, em livre tradução, responsabilidade com ética. Ao seu redor, orbitam os princípios da transparência, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança (prevenção) e não discriminação.

Ademais, ambas as regulamentações possuem efeitos extraterritoriais e atingem organizações que estejam fisicamente fora de seus países, obrigando-as a protegerem os dados pessoais obtidos a partir da oferta de produtos ou serviços na União Europeia ou no Brasil, na forma prevista em suas leis locais. Outrossim, bancos de dados coletados em solo europeu ou brasileiro somente poderão ser transferidos — desde que autorizados por seus titulares — para países que possuam legislação local similar ou superior à GDPR ou LGPD, ou que estejam certificados para tanto. Ou seja, aos titulares deverá ser assegurado que o país de destino possua adequado nível de proteção de dados; com requerimentos legais que sejam compatíveis ou superem seu país de origem.

Ambas as regulamentações possuem efeitos extraterritoriais e atingem organizações que estejam fisicamente fora de seus países

Observando-se os princípios da finalidade e adequação, os dados coletados deverão se restringir ao mínimo necessário para o funcionamento ou aprimoramento dos produtos ou serviços ou da própria sociedade. A coleta deverá guardar proporcionalidade ao fim pretendido. Os dados solicitados deverão ter estreita relação com o serviço ou produto ofertado e sua utilização deverá referir-se a estes, seja para sua execução, para aprimoramento dos negócios, segurança destes, personalização dos serviços ou produtos, marketing, publicidade ou que, de alguma forma, contribuam para a sociedade em si. Esta medida visa a obstaculizar a coleta desenfreada de dados que, por muitas vezes, não guardavam qualquer relação com o produto ou serviço contratados.

Os dados coletados deverão se restringir ao mínimo necessário para o funcionamento ou aprimoramento dos produtos ou serviços ou da própria sociedade

Adicionalmente, o titular deverá consentir inequivocamente para que a coleta e utilização dos dados ocorra. Note que há mais de nove formas de validação que podem ser buscadas pelo controlador de dados. O direito ao esquecimento (que não se confunde com o direito à exclusão dos dados, também assegurado pelas novas leis) é obrigatório, tornando desnecessário recorrer ao Judiciário para fazer valer este direito. Informações a respeito de crianças ganham proteção especial, evitando a exposição excessiva dos menores nas redes. Dados sensíveis, aqueles que, pela sua própria natureza, podem sujeitar o seu titular a práticas discriminatórias, tais como dados sobre a origem racial ou étnica, a convicção religiosa, a opinião política, dado referente à saúde ou à vida sexual; ou permitir a sua identificação de forma inequívoca e persistente, tais como dado genético ou biométrico, também ganham proteção adicional. Os chamados *Data Breach* também deverão ser informados e remediados em prazo razoável, sob pena de multas vultosas -- na Europa, multas de 10 a 20 milhões de Euros ou de 2 a 4% do faturamento anual global, o que for maior. No Brasil, multa de até 2% do faturamento, limitado a R$ 50 milhões por infração. Além disso, outra inovação é a possibilidade de portabilidade dos dados, sendo possível ao titular solicitar que seus dados -- resguardados segredos industriais e de negócio -- sejam encaminhados para outros controladores.

Os impactos do GDPR e da LGPD estão sendo sentidos em muitos aspectos, sejam nas relações de consumo, de trabalho, com entes públicos e privados e tantas outras. Aqui, pretendemos abordar os efeitos nas políticas de privacidade.

As políticas de privacidade sempre foram alvo de críticas, sejam pelo tamanho, pela falta de clareza ou por não serem funcionais. Não é raro ouvirmos expressões como “não li e concordo”, em referência aos usuais *opt-in* de aplicativos ou sites de internet.

As novas leis de proteção de dados visam justamente a mudar este cenário. Sob a égide destas novas regulamentações, as políticas de privacidade não bastarão informar, mas terão que ser efetivas.

E, para isto, os antigos padrões terão que ser revistos e as políticas terão que ser reinventadas.

A política deverá informar indubitavelmente quem é o controlador dos dados (aquele a quem competem as decisões relativas ao tratamento dos dados pessoais) e quem é o operador dos dados (quem realiza o tratamento dos dados pessoais em nome do controlador), bem como quem é o encarregado, no Brasil, ou *data protection officer* (DPO), na Europa, indicado pelo controlador, que atuará como um canal de comunicação entre o controlador, os titulares e a ANPD.

Deverá esclarecer também o papel que cada um destes agentes exerce no processo de coleta, processamento e utilização dos dados.

Sempre que houver uma mudança significativa, os usuários que já forneceram seus dados deverão ser informados e uma nova concordância com os termos da política deverá ser solicitada (*opt-in*). Caso o usuário não concorde com os novos termos, deverá ser oportunizada, na mesma comunicação, a realização do *opt-out*.

Todo compartilhamento de dados pessoais deverá ser informado e autorizado pelo seu titular. Caso um terceiro, a partir de um compartilhamento inicial de iniciativa do próprio titular, venha a conhecer ou utilizar os dados pessoais, seu titular deverá autorizar previamente tal compartilhamento, o mesmo vale para transferência. Independentemente do propósito que tal compartilhamento persiga (cumprimento do contratado, melhoria de produtos, definição do perfil de consumo etc.), ele deve estar autorizado e ser claramente comunicado sobre esta questão.

Deverá haver ainda meios disponíveis para que o titular de dados, solicite exclusão ou correção de seus dados armazenados – este mecanismo, já previsto anteriormente no Código Defesa do Consumidor, assegura ao titular o direito de: (i) saber os dados que a instituição armazena sobre ele; (ii) solicitar a correção dos referidos dados (caso a informação armazenada seja errônea ou incompleta); (iii) fácil identificação para os meios disponíveis para que o titular solicite a exclusão de seus dados pessoais do banco de dados da organização.

Aos titulares de dados, deverá ser oportunizada a possibilidade de ver, corrigir e excluir as informações armazenadas sobre ele, além de consentir de forma granular. Ademais, deverá ser esclarecido sobre as consequências de não consentir (haverá privação parcial / total dos serviços?).

A fim de buscar a adequada efetividade, os controladores poderão servir-se de todos os meios disponíveis, valendo-se de vídeos ilustrativos, *storyboards* que demonstrem o propósito da coleta de dados, entre outros aspectos. Poderão utilizar-se de versões simplificadas das políticas (*pocket version*), que, adicionadas à versão completa do documento, darão o integral cumprimento do pretendido.

Importante não perder de vista que, uma vez obtido o consentimento ou de posse dos dados, deverá ser instaurado todo um procedimento para adequado processamento destes dados com completo rastreamento destas informações para viabilizar correção, exclusão por retirada de consentimento ou exclusão findo o contrato. Sobre este último, cada instituição controladora de dados deverá definir qual é o momento de fazê-lo, observando-se todas as peculiaridades que ensejam seus produtos ou serviços.

Uma nova era para a proteção de dados pessoais foi instaurada e caberá a cada controlador adequar-se a fim evitar a aplicação das multas, bem como proteger sua marca. Incidentes envolvendo o vazamento de dados poderão trazer grandes consequências aos responsáveis pelos dados. Caberá também à sociedade adaptar-se a uma nova cultura de dados, que, se construída de forma responsável e ética, lhes trará grande benefício.

Capítulo 2

Finalidade do Tratamento dos Dados Pessoais - o Princípio a ser Considerado

Por Clarisse De La Cerda

Finalidade Aplicada à Coleta de Dados

O primeiro princípio a ser observado na coleta de dados pessoais é o da finalidade. A finalidade deve nortear tal coleta, restringindo-a e impondo limites.

Fazem parte dos pilares das boas práticas das políticas de privacidade a imposição de limites à coleta de dados, para que sejam de acordo com os usos antecipados, e a restrição do uso conforme os propósitos especificados da coleta.

No entanto, dados pessoais estão sendo usados cada vez mais em formas não antecipadas quando da coleta destes. Isso porque, em razão dos avanços tecnológicos, a coleta de dados tem se tornado mais eficiente e ampla, sem qualquer limitação territorial. O fenômeno da “big data” (grandes quantidades de dados que podem ser armazenados, ligados e analisados), com o desenvolvimento de algoritmos e técnicas de análise de grandes quantidades de dados, tem levado a crescentes novos usos para dados anteriormente coletados, agregando valor.

Esses usos não antecipados, em princípio, necessitariam de novo consentimento ou outra base legal que os validassem. Por outro lado, tal obrigação pode limitar a inovação, seja por impedir a exploração, seja por diminuir a possibilidade de receita econômica com o uso de tais dados. Daí a importância de uma coleta pautada pelas boas práticas.

Por exemplo, recentemente, a concessionária ViaQuatro, que administra a Linha 4 – Amarela do Metrô da cidade de São Paulo, foi alvo de ação civil pública em razão de nova tecnologia implementada com sensores que reconhecem figuras humanas e suas emoções, coletando tais dados. Argumenta-se que o usuário não possui sequer liberdade no consentimento da coleta, que tem o propósito de aplicação em pesquisas de mercado para marketing direcionado.

Tais limitações à coleta de dados passam pela forma com que estes serão processados, sua natureza, o contexto do uso, dentre outros requisitos. A Organização para a Cooperação e Desenvolvimento Econômico (OECD), em seu guia sobre os direitos de privacidade, dispõe que tais limites possam estar relacionados com:

(i) aspectos da qualidade dos dados;
(ii) limites associados com o propósito do processamento dos dados;
(iii) marcação de dados especialmente sensíveis, de acordo com as tradições e costumes de cada país membro;
(iv) limites à atividade de coleta de dados para determinados agentes; e
(v) preocupações em conexão com direitos civis.

Assim, um dos princípios é a limitação da coleta de dados, que determina que a coleta de dados pessoais deve ter limites e tais dados deverão ser obtidos por meios legais e justos e, quando apropriado, com a ciência ou consentimento do titular dos dados.

Desta forma, é necessário informar, de plano, se o provimento dos dados é obrigatório para a fruição do serviço ou produto e quais as consequências no não fornecimento dos dados. Recomenda-se que sejam obrigatórios somente aqueles dados estritamente necessários ao fornecimento do serviço ou produto, caso se trate, por exemplo, de um serviço ou produto essencial, para que questões ligadas aos direitos de consumidor sejam minimizadas.

Note-se que, caso os dados sejam obtidos via um intermediário, isso deverá ser informado na política de privacidade.

É imperativo que seja determinado quais dados estão sendo coletados. Desta forma, de acordo com o princípio da qualidade dos dados, os dados pessoais coletados deverão ser relevantes aos propósitos para os quais serão usados, bem como precisos, completos e atualizados, na medida da extensão necessária a tais propósitos.

De acordo com o princípio da qualidade dos dados, os dados pessoais coletados deverão ser relevantes aos propósitos para os quais serão usados, bem como precisos, completos e atualizados, na medida da extensão necessária a tais propósitos

Consequentemente, a política de privacidade será tão extensa quanto a qualidade dos dados que estão sendo coletados, por que estão sendo coletados e como serão usados, nas palavras de Mike Hintze[1].

Nesse ponto, acrescenta o guia da OECD que os propósitos para os quais os dados são coletados deverão ser especificados, no máximo, até o momento da coleta de dados e o subsequente uso limitado à consecução de tais princípios ou outros que não incompatíveis com tais propósitos ou caso especificados em cada ocasião de alteração de tal propósito.

Finalmente, o princípio da limitação do uso dos dados determina que os dados não devam ser usados para outros usos que não aqueles para os quais foram colhidos, salvo com o consentimento do titular dos dados ou por determinação legal.

Ou seja, é importante que seja informado como os dados serão utilizados, se para fruição do serviço ou produto, se para melhoramento do serviço ou produto, ou mesmo para marketing direcionado.

[1]HINTZE, Mike. Privacy Statements: Purposes, Requirements, and Best Practices. P. 3.

A LGPD incorpora todos os princípios que permeiam a coleta de dados informados acima. Ainda, determinar quando começa a coleta de dados é importante, pois a LGPD, em seu art. 3º, determina ser ela aplicável quando os dados pessoais objeto do tratamento tenham sido coletados no território nacional, sendo considerados coletados em território nacional os dados pessoais cujo titular nele se encontre no momento da coleta[2].

A LGPD, ainda, determina que, nas atividades de tratamento, incluindo-se, aí, a coleta, deverão ser observados os princípios:

(i) da finalidade (art. 6º, inciso I), de forma que o tratamento dos dados deverá ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
(ii) da adequação (art. 6º, inciso II), para que o tratamento seja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
(iii) da necessidade (art. 6º, inciso III), para que o tratamento esteja limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; e
(iv) da qualidade dos dados (art. 6º, inciso V), sendo garantido aos titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

[2]Veja que a disposição não faz menção à coleta de dados de residente em território nacional ou nacional que se encontre no exterior, no momento da coleta. Ou seja, não há previsão de aplicação da lei brasileira pela coleta caso o titular dos dados seja brasileiro ou residente no território brasileiro, mas que, no momento da coleta, esteja no exterior. Contudo, trata-se apenas de aparente ausência de previsão legal, tendo em vista que, quando da definição de tratamento, no art. 5º, inciso X, a LGPD inclui nesta toda a operação realizada com dados pessoais, inclusive a coleta, e o inciso I, do art. 3º, determina a aplicação da LGPD a toda operação de tratamento realizada no território nacional.

Importante dispositivo é aquele que determina que poderão ser coletados dados pessoais de crianças, sem o consentimento específico dado por um dos pais ou responsável legal, quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção. Veja que, em nenhum caso, poderão ser repassados a terceiro sem o consentimento específico de um dos pais ou do representante legal (art. 14, §3º).

Um bom exemplo de como não cumprir as boas práticas de privacidade encontra-se na Lei Estadual 16.758/18, sancionada em junho de 2018, em São Paulo, que torna obrigatória a informação sobre cor ou identificação racial em todos os cadastros, bancos de dados e registros de informações assemelhados, públicos e privados, com o intuito de mapeamento das concentrações de pessoas para planejamento de políticas públicas para combate de indevidas segregações. Ou seja, a lei impõe a coleta de um dado pessoal sensível, que, em princípio, parece ferir os princípios da adequação e necessidade da coleta.

Capítulo 3

Consentimento como Base Legal para o Tratamento de Dados Pessoais

Vários autores

Consentimento Específico

Por Henriete Fejes

O consentimento é uma das bases legais para o tratamento de dados pessoais previstas na LGPD, assim como:

- Cumprimento de obrigação legal ou regulatória
- Execução de políticas públicas
- Realização de estudos por órgãos de pesquisa
- Execução de contratos
- Exercício regular de direitos
- Proteção da vida ou da incolumidade física do titular
- Tutela da saúde
- Legítimo interesse do controlador dos dados
- Proteção do crédito

Sendo coberto por quatro características: **LEI²**

1. **L**IVRE
2. **E**XPRESSO
3. **I**NFORMADO
4. **I**NEQUÍVOCO

O consentimento é a base legal para tratamento de dados pessoais e possui uma natureza contratual, pois, de um lado há a manifestação da vontade de uma parte em tratar os dados pessoais para determinada finalidade e, de outro lado, há alguém que concorda com este tratamento.

Além de ser uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais, também este consentimento deve se dar para uma finalidade determinada.

A sua forma está prescrita na lei: deve se dar por escrito ou por qualquer outro meio que demonstre que houve manifestação de vontade do titular. A lei não admite o consentimento tácito. Qualquer que seja o meio pelo qual o titular expressou seu consentimento, este deve ser preservado de maneira que se prove que houve inequívoca manifestação de vontade do titular dos dados.

Ou seja, independente do meio utilizado para o consentimento, o importante é que ele seja preservado, inequívoco, inteligível, comprovável perante autoridades judiciais, em caso de questionamento, e adequado aos termos do tratamento de dados proposto.

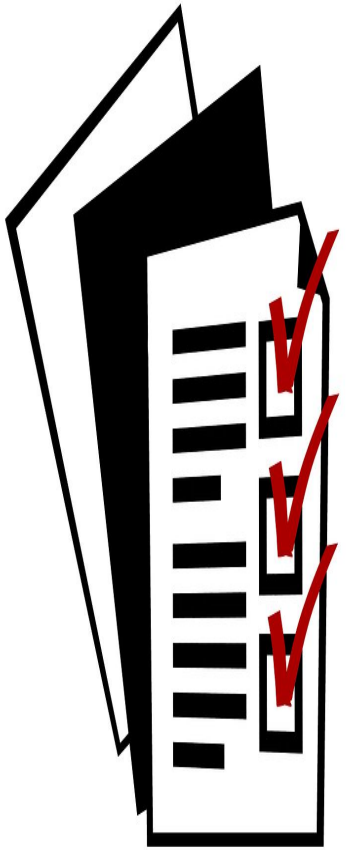
A cláusula sobre o consentimento, quando inserida em uma política ou contrato, deverá ser DESTACADA. Esse destaque poderá se dar dentro do texto do instrumento celebrado com o detentor dos dados, em negrito, itálico, caixa alta, ou em um capítulo ou seção específicos para tanto. Contudo, muitos entendem que a expressão "destacada" inserida no texto pelo legislador significa que deverá se dar em um documento avulso. Qualquer que seja a forma escolhida, o importante é que haja clareza e precisão no texto.

Caso não seja observada a forma prescrita na lei para coleta do consentimento, o negócio jurídico será nulo.

Outra característica importante do consentimento é que ele deve ser específico, determinado. A política deverá detalhar como os dados do titular serão utilizados e a finalidade da sua coleta. A utilização de expressões vagas ou finalidades genéricas não serão admitidas.

Neste mesmo sentido, se houver mudança da finalidade específica do tratamento após a coleta, ou mudança na forma, duração ou compartilhamento dos dados, e o consentimento for a base legal daquela coleta, o titular dos dados deverá ser informado para que consinta com esta alteração ou revogue seu consentimento.

Nota-se, portanto, que a redação da cláusula de consentimento de uma política de privacidade é extremamente relevante e qualquer omissão pode tornar ineficaz o consentimento obtido.



Consentimento Crianças e Adolescentes

Por Ingrid Ferreira

A proteção da criança e do adolescente é direito fundamental garantido no texto constitucional brasileiro. O artigo 227 da Constituição Federal estabelece, como dever da família, sociedade e do Estado, com absoluta prioridade, dentre outros direitos, o direito dos menores à dignidade e ao respeito, colocando-os a salvo de toda forma de "negligência, discriminação, exploração, violência, crueldade e opressão".

Na mesma linha, o Estatuto da Criança e do Adolescente (ECA) dispõe sobre a proteção integral à criança e ao adolescente, reiterando, nos artigos 4º e 5º, o direito acima deflagrado no texto da Carta Magna. Mas não apenas isto, o artigo 2º do ECA também define a faixa etária aplicada à criança, esta considerada como a pessoa até os doze anos de idade incompletos, e ao adolescente, a pessoa entre doze e dezoito anos de idade.

Portanto, a LGDP não se omitiu em tratar de forma diferenciada este grupo de vulneráveis. Antes, incluiu um tópico específico sobre o tema, frisando que o tratamento dos dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse e mediante consentimento específico, em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Além disto, a LGDP estabeleceu algumas obrigações ao controlador, como o de primar pela transparência, mantendo de maneira pública a informação sobre os tipos de dados coletados da criança e do adolescente, a forma de utilização e os procedimentos para revogar o consentimento, dentre outras responsabilidades.

O tratamento dos dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse e mediante consentimento específico, em destaque dado por pelo menos um dos pais ou pelo responsável legal

Importante ressaltar que a GDPR estabeleceu um tópico especial para proteger os dados de crianças, permitindo, todavia, que o consentimento do detentor da responsabilidade parental não seja necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança. E, da mesma forma, a LGDP também incluiu uma ressalva para a coleta de dados pessoais de crianças sem consentimento parental quando para fins de sua proteção e salvaguarda, bem como, quando necessária para contatar os pais ou o responsável legal, desde que utilizados uma única vez e sem armazenamento.

Analisando ainda a lei brasileira de proteção de dados, há algumas regras específicas a serem observadas em se tratando da coleta de dados pessoais de crianças e adolescentes. Uma delas é que a disponibilização de jogos, aplicações de internet ou outras atividades oferecidas diretamente para crianças e adolescentes não deve ter acesso e participação condicionados à coleta de seus dados pessoais, salvo quando estritamente necessário à atividade oferecida.

Note que as informações sobre o tratamento dos dados de crianças e adolescentes deverão ser fornecidas de maneira simples, clara e acessível, levando em consideração as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais da criança e do adolescente. Não basta constar apenas da política de privacidade ou termos e condições de uso dos dados coletados, mas devem ser empregados recursos audiovisuais, sempre que possível, de forma a proporcionar a informação adequada ao entendimento da criança e necessária para compreensão dos pais ou responsável legal.

Outra regra constante do nosso marco civil de proteção de dados é da obrigação do controlador em envidar esforços razoáveis para verificar se o consentimento foi dado pelo pais ou responsável legal da criança, considerando as tecnologias disponíveis.

Esta exigência legal, flexibilizada de certa forma pelo limite das tecnologias disponíveis, é também presente na GDPR e tem sido objeto de reflexão quanto ao seu cumprimento. Empresários como a Microsoft tem se valido de um processo de autenticação pelos pais ou responsável legal das contas de crianças, em conformidade com a COPPA (*Children's Online Privacy Protection Act* – Lei de Proteção à Privacidade Online das Crianças, vigente para os Estados Unidos da América). Esta lei exige o consentimento dos pais ou responsável legal quando a criança for menor de 13 (treze) anos de idade. Assim, quando o usuário informar idade menor de 13 anos no momento do cadastro da conta, os pais ou responsável legal deverá permitir formalmente a utilização da conta pelo menor em um prazo curto de tempo, sob pena da conta ser bloqueada. Um método que vem sido comumente utilizado para comprovar esta aprovação "parental" é a cobrança de uma pequena taxa não reembolsável em um cartão de crédito ou cartão de débito que tenha um número CVV.

A conformação ao disposto pelo GDPR mediante a utilização das regras do COPPA vem suscitando discussões na comunidade europeia. Isto porque, na prática, um aviso de que o site ou aplicativo não é direcionado a menores de 13 anos é apresentado, excluindo-se a necessidade de obtenção do consentimento dos pais ou responsável legal. Como alertam Macenaite e Kosta[3] o controle para saber se o acesso a tal site foi feito por uma criança menor de 13 anos é impraticável e cookies podem ser instalados no seu computador, tablet ou smartphone, e, consequentemente, coletar seus dados pessoais.

Importante notar que, diferente da GDPR, nossa lei especial não vedou o uso de dados pessoais de crianças para fins de comercialização ou criação de perfis de personalidade dos usuários, tampouco proibiu a coleta de dados pessoais de crianças para fins de oferta de bens e serviços direcionados diretamente à criança, deixando esta questão à margem dos debates existentes sobre publicidade direcionada ao público infantil, amplamente debatido em nossa sociedade civil quanto aos seus limites e legalidade.

[3]Macenaite, Milda & Kosta, Eleni. (2017). Consent for processing children's personal data in the EU: following in US footsteps?. Information & Communications Technology Law. 26. 1-52. 10.1080/13600834.2017.1321096.

Recentemente, um caso de potencial violação à proteção de dados pessoais de crianças e adolescentes foi apresentado perante a *Information Commissioner's Office* (Autoridade Europeia de Proteção de Dados ou ICO). Nele, a Amazon foi inquirida a prestar esclarecimentos com relação ao seu produto de internet das coisas conhecido como Alexa. Isto porque o produto colhe informações e dados da "vida em casa", misturando, portanto, dados de adultos com os de crianças. Segundo Veronica Barassi, que reportou o caso para a ICO, atualmente, os fornecedores de produtos e serviços não reconhecem as implicações quanto ao tema de privacidade de crianças e adolescentes.

O assunto da proteção dos dados de crianças e adolescentes tem muito debate pela frente e, para fins de cumprimento e conformidade, recomenda-se total transparência nas informações, clareza na comunicação, adoção de uma medida para evitar a coleta de dados de crianças e adolescentes, salvo mediante aprovação dos pais ou responsável legal. No entanto, a existência de uma autoridade nacional será estritamente necessária para nortear o tema e pacificar o assunto.

Retirada do Consentimento

Por Karyne F. Barbosa

A LGPD preleciona que a revogação para tratamento de dados pode ocorrer a qualquer momento, desde que seja da vontade do titular. É o que consta no artigo 8º, § 5º, abaixo transcrito:

> *"O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (...)*
> *§ 5º - 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 enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei."*

Sendo assim, a retirada de consentimento deve ser tão fácil quanto seu fornecimento, ou seja, além de ser por manifestação expressa do titular deve ser por procedimento gratuito e facilitado e, uma vez retirado o consentimento, deve a organização responsável pelo tratamento de dados, além de finalizar o processo de tratamento de dados, garantir a possibilidade de eliminação dos dados, caso requerido. É o que assegura o art. 18, VII:

> *"O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...)*
> *VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;"*

Existem hipóteses nas quais, mesmo com o consentimento para tratamento revogado, os dados serão conservados, isso ocorre em situações específicas elencadas no art. 16:

> *"Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:*
> *I - cumprimento de obrigação legal ou regulatória pelo controlador;*
> *II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;*
> *III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou*
> *IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados".*

Insta salientar que, se houver desvio de finalidade para o tratamento de dados que não sejam compatíveis ao consentimento fornecido originalmente, a LGPD garante que, após ser informado pelo controlador sobre as mudanças ocorridas, o titular pode revogar o consentimento fornecido anteriormente, caso não concorde com as alterações. É o que instrui o art. 9º, § 2º:

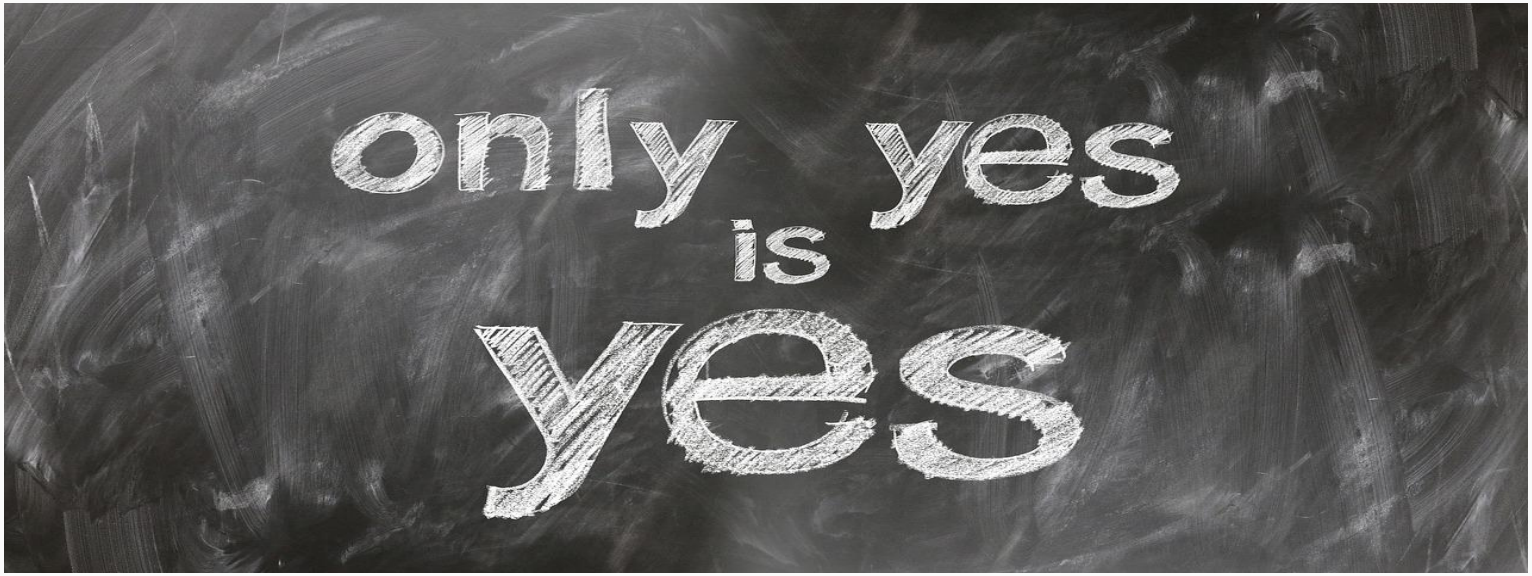
> *"Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações."*

Visto isso, é essencial saber que, para que o consentimento seja considerado livre, deve ser conferido ao usuário pleno controle sobre o tratamento de seus dados pessoais. O usuário deve poder escolher quais dados fornecer e quais dados não fornecer, bem como deve poder retirar seu consentimento a qualquer momento.

Todas essas informações precisam constar de forma clara e objetiva nas políticas de privacidade daqueles que coletam os dados para posterior tratamento de dados, sendo necessário destinar uma parte específica à revogação de consentimento, esclarecendo-se ao titular o modo pelo qual poderá solicitá-lo, sendo os meios mais práticos o acesso à conta pessoal no site, o envio de e-mail com o pedido de retirada de consentimento ou, ainda, por meio de formulários físicos, que deverão ser assinados por todas as partes interessadas, ou seja, o titular, o controlador e o encarregado de proteção de dados.

Como forma de melhor elucidar essa questão de retirada de consentimento, observe-se o seguinte exemplo prático: Um site de notícias tem um boletim informativo semanal. O cliente dá o seu consentimento para subscrever o boletim, permitindo-lhe efetuar o tratamento de todos os dados que sejam do seu interesse para criar um perfil do tipo de artigos que consulta. Passado um ano, o cliente informa que já não deseja receber o boletim informativo. Consequentemente, devem ser apagados da base de dados todos os dados pessoais relacionados a esse titular que tenham sido recolhidos no contexto da subscrição do boletim informativo, incluindo os perfis relacionados com essa pessoa, caso existam. No mais, deve-se observar as possibilidades de conservação dos dados elencados no art. 16 acima citado.

Portanto, a retirada de consentimento é um procedimento que deve ser de conhecimento do titular de dados e deve ser apresentado como uma possibilidade que pode ser requerida a qualquer tempo de maneira prática e objetiva, garantindo ao titular controle e segurança quanto à disponibilidade ou não de seus dados para tratamento.



Capítulo 3

Direitos do Titular de Dados e a Elaboração da Política de Privacidade

Vários Autores

Do Direito de Acesso

Por Carolina Braga

A parte inicial da LGPD contém os dez princípios que devem orientar o tratamento de dados, tais como o da finalidade, necessidade, transparência, segurança, não discriminação e o novo princípio da responsabilização e prestação de contas, que obriga o responsável pelo tratamento dos dados pessoais a demonstrar, de forma cabal e transparente, a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, algo que pode ser feito por meio dos *assessments*, metodologias de análise também previstas na lei.

Nos termos do art. 6º, os princípios do tratamento de dados no Brasil são, além da boa-fé objetiva, os seguintes:

1. **princípio da finalidade**, descrito como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (inciso I);

2. **princípio da adequação**, descrito como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (inciso II);

3. **princípio da necessidade**, descrito como a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (inciso III);

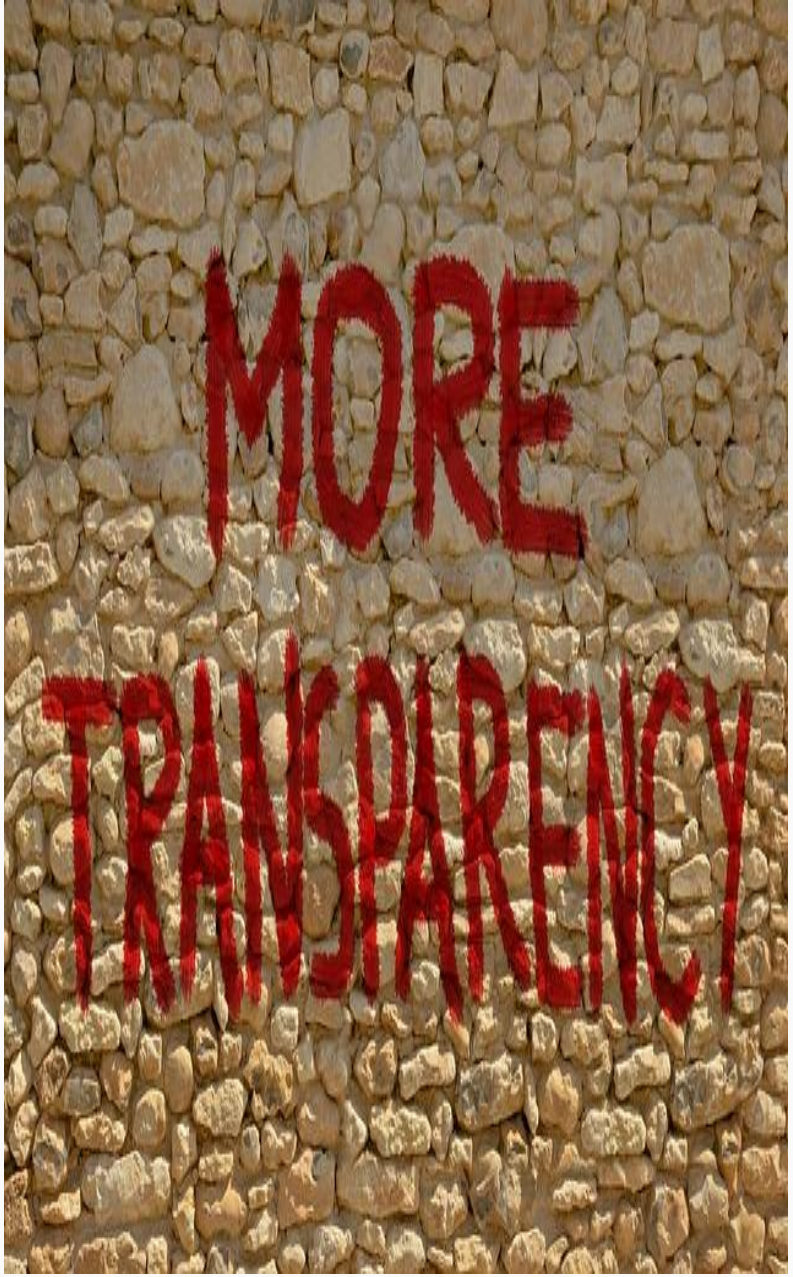
4. **princípio do livre acesso,** descrito como a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (inciso IV);

5. **princípio da qualidade dos dados**, descrito como a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (inciso V);

6. **princípio da transparência**, descrito como a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial” (inciso VI);

7. **princípio da segurança**, que exige “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (inciso VII);

8. **princípio da prevenção**, traduzido na “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais” (inciso VIII);



9. princípio da não discriminação, que consiste na "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (inciso IX); e

10. princípio da responsabilização e prestação de contas, que exige "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."

Embora a própria enunciação do princípio da transparência excetue os segredos de negócios, tal previsão não deve impedir que haja um maior controle de dados por seus usuários, em compatibilidade com os fundamentos constantes do art. 2º (livre desenvolvimento da personalidade e preservação da autonomia e da cidadania).

Da mesma forma, não se pode assegurar a eficácia de diversos princípios previstos pela lei sem maior transparência e *accountability* sobre os algoritmos, ainda que estes sejam proprietários ou sujeitos à segredo industrial.

Não se pode assegurar a eficácia de diversos princípios previstos pela lei sem maior transparência e *accountability* sobre os algoritmos

A partir do art. 7º, portanto, a LGPD já começa a tratar de vários assuntos que envolvem direitos dos titulares de dados, a seguir enumerados:

(i) Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais - Arts. 7º, I, e 8º;

(ii) Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei mesmo para os casos de dispensa de exigência de consentimento - Art. 7º, § 6º;

(iii) Direito à inversão do ônus da prova quanto ao consentimento - Art. 8º, § 2º;

(iv) Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais - Art. 8º, § 4º;

(v) Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca - Art. 9º, § 1º;

(vi) Direito de revogar o consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado - Art. 8º, § 5º;

(vii) Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados - Arts. 8º, § 6º e 9º, § 2º;

(viii) Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras, finalidade específica do tratamento, forma e duração do tratamento, observados os segredos comercial e industrial, identificação do controlador, informações de contato do controlador, informações acerca do uso compartilhado de dados pelo controlador e a finalidade, responsabilidades dos agentes que realizarão o tratamento, e direitos do titular, com menção explícita aos direitos contidos no art. 18 - Art. 9º;

(ix) Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações - Art. 8º, § 6º;

(x) Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos - Art. 9º, § 3º;

(xi) Direito de ser informado sobre a utilização dos dados pela administração pública, para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa - Art. 7º, III e IV c/c art. 7º, § 1º;

(xii) Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização - Art. 7º, § 3º;

(xiii) Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento - Art. 7º, § 5º;

(xiv) Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador - Art. 10, § 1º;

(xv) Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador - Art. 10, § 2º;

(xvi) Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa - Art. 11, II, c;

(xvii) Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para tratamento de dados sensíveis nas hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos - Art. 11, § 2º;

(xviii) Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular - Art. 11, § 4º;

(xix) Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas - Art. 13;

(xx) Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública - Art. 13, § 1º;

(xxi) Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa - Art. 13, § 2º;

(xxii) Direito ao término do tratamento quando verificado que (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento, (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou (i) por determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. - Art. 15; e

(xxiii) Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, autorizada a conservação somente nas exceções legais - Art. 16.

Os titulares dos dados pessoais tiveram seus direitos ampliados, e devem ser garantidos de forma acessível e eficaz. Dentre os direitos listados, destaca-se o de acesso aos dados, retificação, cancelamento ou exclusão, oposição ao tratamento, de informação e explicação sobre o uso dos dados.

A grande novidade é o direito à portabilidade dos dados, que permite ao titular de dados requisitar uma cópia da integralidade de seus dados, assim como requerer que estes sejam fornecidos em um formato que facilite a sua transferência para outros serviços, ainda que se trate de concorrentes.

Trata-se, na verdade, de diversos direitos que garantem ao titular de dados um certo poder em relação àqueles que coletam e tratam seus dados. Assim,, a partir da entrada em vigor da LGPD, aqueles que, até o momento, coletavam e tratavam dados com total liberdade, passarão a ter que atender a princípios e deveres mais rígidos que protegem o usuário e seus dados.

Direito à Segurança

Por Angela Maria Rosso

A LGPD traz, como um dos princípios a serem respeitados no tratamento dos dados, a segurança - art. 6º, VII que consiste em:

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

A lei obriga, portanto, que as melhores técnicas de segurança sejam adotadas em relação aos dados. De acordo com Mike Hintze, não basta afirmar “(s)eus dados estão seguros conosco”, é preciso esclarecer ao titular dos dados como essa segurança é construída ao longo de todo o ciclo de vida do dado.

Por ser um princípio basilar da proteção de dados pessoais e por considerá-lo de importância única, o legislador dedicou-se a explicar ainda, nos artigos 46, 47,48 e 49, o que se deve entender por boas práticas para a segurança dos dados. Dessa forma, entendemos que a concretização desse princípio passa também pela elaboração de uma política de privacidade que contemple detalhadamente quais os meios e métodos empregados na garantia do direito do titular.

Alguns pontos que devem ser considerados quando da elaboração da política de privacidade são os seguintes:

1 - Mencionar a base legal que obriga a organização a adotar as melhores práticas em relação à segurança dos dados pessoais em seu poder. Interessante pontuar o que isso inclui, ou seja, se os dados estão protegidos contra acessos não autorizados, por exemplo;

2 - Qual(is) setor(es) da organização é(são) o(s) responsável(is) por garantir que as melhores práticas de segurança dos dados pessoais estão sendo adotadas para assegurar a privacidade do titular dos dados;

3 - Explicitar quais medidas são tomadas para garantir que toda a organização trabalhe em função de assegurar a inviolabilidade dos dados, ou seja, explicitar as garantias de que só acessam os dados aquelas pessoas que precisam deles para fazer seu trabalho (confidencialidade) e que as senhas utilizadas por essas pessoas não são compartilhadas e que são encriptadas, por exemplo. Explicar que a equipe passa por constante treinamento como meio de garantir que as políticas de segurança adotadas pela organização sejam efetivamente aplicadas;

4 - Deixar explícito se os dados podem ser transportados em *laptops*, *pen drives,* etc., e, no caso de ser permitido, em quais situações e sob quais medidas de segurança;

5 - Deixar explícito se os sistemas que utilizam dados pessoais como insumo são/estão remotamente acessíveis aos colaboradores. Se sim, quais as medidas de segurança adotadas, como *vpn*, por exemplo.

6 - Deixar claro que todo o pessoal envolvido no tratamento dos dados pessoais conhece e é responsável pela implementação da política de privacidade;

7 - Deixar explícito quais as situações que permitem que o dado pessoal seja divulgado; e

8 - Armazenamento e auditabilidade das operações de processamento dos dados pessoais.

Ao especificar os pontos que sustentam a segurança que a organização dá aos dados pessoais, é importante que haja fidelidade entre o que está escrito - compromisso assumido com o titular dos dados - e as práticas efetivamente adotadas.

Data Breach

Por Angela Maria Rosso

A LGPD prevê, em seu artigo 48:

"O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares

§1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;
II - as informações sobre os titulares envolvidos;
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV - os riscos relacionados ao incidente;
V - os motivos da demora, no caso de a comunicação não ter sido imediata;
VI - as medidas que foram ou serão adotadas para reverter ou mitigar os efeito do prejuízo "

É de responsabilidade do controlador dos dados tomar todas as medidas de segurança necessárias para garantir a inviolabilidade das informações pessoais em seu poder. Entretanto, é mandatório que estejam previstas de forma clara, na política de privacidade da organização, qual o procedimento que será adotado em caso de incidente.

1 - Definir quem será o encarregado de dados responsável por comunicar o titular dos dados sobre a violação dos dados;

2 - Definir o prazo em que o titular dos dados será informado em caso de incidente na ausência de previsão legal;

3 - Definir qual será o meio utilizado para comunicar o titular dos dados (email, sms, ligação telefônica etc); e

4 - Explicitar quais medidas serão tomadas para minimizar os efeitos do incidente.

A comunicação com o titular dos dados em casos de incidentes deve ser clara, direta e transparente, de forma a refletir a realidade da ocorrência e os seus possíveis impactos. Além disso, deve ser disponibilizado canal de contato com pessoal preparado para responder aos eventuais questionamentos dos titulares dos dados.

Capítulo 4

Políticas de Privacidade e o Marketing Direto

Por Vanessa Pareja Lerner

Um dos tópicos polêmicos da LGPD é o impacto que a sua aplicação terá no uso de dados pessoais e sensíveis para a realização de marketing direto. Em seu conceito, marketing direto é a oferta ou promoção de produtos, serviços ou outras solicitações direcionadas a uma pessoa específica. Cada vez que você recebe um e-mail de uma loja ou uma *newsletter* de seu médico; atende uma ligação telefônica com a oferta de produtos ou recebe em casa um panfleto promocional direcionado a você, tudo isso são formas de marketing direto.

> Marketing direto é a oferta ou promoção de produtos, serviços ou outras solicitações direcionadas a uma pessoa específica

O assunto sempre teve uma importância relevante no Brasil, sendo tratado no contexto de normas gerais de proteção ao consumidor e de privacidade. No mundo atual, a forma de interação das pessoas com tecnologias diversas eleva em muito a importância do tópico. O uso intenso de equipamentos portáteis (como o celular, *tablet* e *laptop*) associado a aplicativos e tecnologias emergentes tornam as pessoas suscetíveis aos mais diversos artifícios para a coleta de dados pessoais para marketing direto. Esses podem variar desde o uso de ferramentas de geolocalização para venda de produtos e serviços, até a segmentação de usuários com base em características e definição de perfis (como situação econômica, idade, interesses, localização, entre outros) para o direcionamento de propagandas e campanhas voltadas a cada pessoa. A realidade é que nunca o marketing direto teve um potencial tão invasivo como agora.

Dessa forma, volta-se à pergunta: Como a LGPD irá afetar o marketing direto e qual a forma adequada de tratamento de dados pessoais para esse propósito? O primeiro ponto é que a LGPD não proíbe a utilização de dados pessoais ou sensíveis para marketing direto, apenas condiciona o tratamento de dados para esse propósito a situações nas quais exista uma base legal adequada e observação de outros requisitos legais.

Seguindo as bases legais que autorizam o tratamento de dados pessoais previstas no art. 7 da LGPD, o tratamento de dados pessoais para marketing direto pode ser fundamentado no consentimento livre, informado e inequívoco do titular ou no cumprimento do legítimo interesse do controlador. Dessa forma, passa-se a explorar brevemente ambas as hipóteses.

O consentimento pode autorizar tanto o uso de dados pessoais quanto de dados sensíveis para marketing direto, desde que observadas as normas aplicáveis a essa base legal. O consentimento deve ser prévio ao tratamento e, quando escrito, deve ser obtido de forma destacada de outras cláusulas contratuais, exigindo, para sua validade, um ato afirmativo do titular de dados, passível de comprovação posterior. Dessa forma, o silêncio do titular ou até mesmo o uso de caixas pré-selecionadas podem descaracterizar a existência de um ato inequívoco de consentimento.

Quando houver o tratamento de dados pessoais sensíveis, o consentimento precisa ser qualificado para atender aos requisitos do artigo 11 da LGPD, devendo ser destacado e específico. Essa categoria comporta quaisquer dados pessoais que revelem dados sensíveis (art. 11, § 1º). Logo, não se descarta que, por exemplo, uma fotografia, da qual se depreenda a religião ou raça de uma pessoa, seja considerada um dado pessoal sensível, se tratada para esse propósito.

Assim como em outras bases legais, o primeiro passo para viabilizar o tratamento de dados por meio do consentimento será determinar o propósito legítimo específico, ou seja, a finalidade que justifica cada ato de tratamento que se pretende realizar, lembrando sempre que autorizações genéricas podem gerar vícios de consentimento.

No tratamento de dados pessoais sensíveis, o consentimento precisa ser qualificado para atender aos requisitos do artigo 11 da LGPD, devendo ser **destacado e específico**

Se, para a realização de marketing direto for necessária a comunicação ou o compartilhamento de dados pessoais com outros controladores, a situação será um pouco diferente. Dados pessoais somente poderão ser compartilhados ou comunicados a terceiros se houver consentimento específico para esse propósito. Caso o controlador receba dados de terceiros para enriquecimento de sua base, o mesmo princípio se aplica, na medida em que a ausência do consentimento original para a transferência e tratamento de dados poderá viciar a base do controlador. No tocante a dados sensíveis, tal compartilhamento ou comunicação é estritamente proibida na forma art. 11, §3º da LGPD.

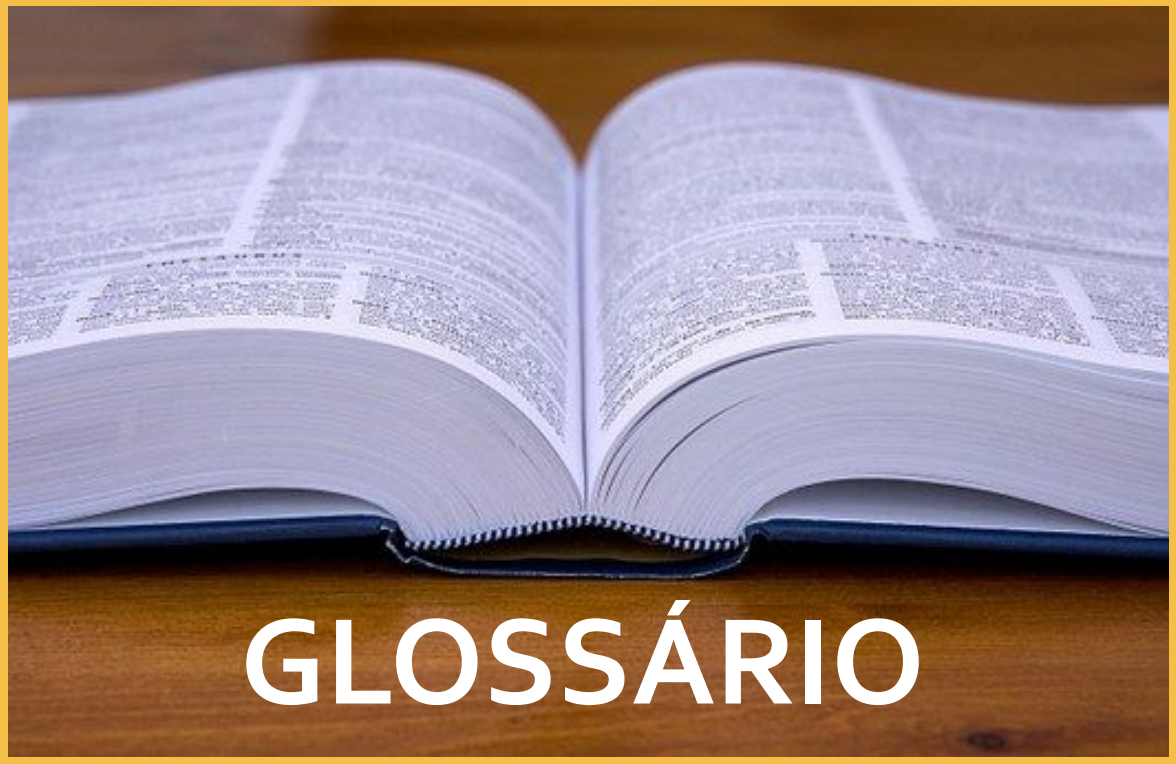
Conforme mencionado, por sua vez, o legítimo interesse do controlador também pode ser uma potencial base legal para o tratamento de dados pessoais. De fato, existe menção específica no artigo 10, I da LGPD, que, dentre as finalidades que autorizam a sua aplicação, encontra-se o "apoio e promoção de atividades do controlador". Cumpre-se apontar, no entanto, que essa base legal não poder ser suscitada para o tratamento de dados pessoas sensíveis.

Para tanto, será essencial realizar uma avaliação interna prévia ao tratamento de dados para aferir: (i) se existe uma finalidade legítima que justifique o tratamento de dados; (ii) se os dados pessoais sujeitos ao tratamento são os estritamente necessários para cumprir a finalidade específica almejada e (iii) se o tratamento de dados na sua forma proposta tem algum impacto em relação aos direitos do titular. É relevante notar que a ANPD, quando constituída, poderá solicitar ao controlador a apresentação de um relatório de impacto de proteção de dados pessoais.

O tratamento de dados com base no legítimo interesse não depende de um ato de consentimento positivo do titular, mas é necessário que o controlador insira na sua política de privacidade as finalidades específicas que justificam o tratamento de dados, bem como a identificação específica da base legal que o justificou.

Pelo exposto, a LGPD não inviabiliza a realização de marketing direto com o uso de dados pessoais e de dados pessoais sensíveis, porém terá um impacto considerável em muitas práticas atuais que se baseiam na coleta e enriquecimento de dados indiscriminada. O foco deve ser sempre garantir que o titular de dados tenha conhecimento das práticas para que possa exercer os seus direitos a qualquer momento.

Capítulo 5



Por Remi Yun e Adriana Tocchet Wagatsuma

Este glossário pretende facilitar sua compreensão quanto aos termos mais frequentes numa política de privacidade.

- **Adequação** - compatibilidade do tratamento com as finalidades informadas ao titular;

- **Anonimização** - processo em que um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, mediante utilização de meios técnicos razoáveis e disponíveis no momento do tratamento;

- **Armazenamento dos Dados -** é a retenção de informações através de uma tecnologia específica com o objetivo de guardar esses dados e mantê-los acessíveis conforme necessário. Exemplos: Cloud, Servidores, Dispositivos de Storage, etc;

- **Autoridade Nacional (ANPD)** - órgão da administração pública indireta responsável pelo cumprimento da LGPD;;

- **Bases Legais para Processamento** – trata-se de normativos jurídicos brasileiros ou não vigentes que determinam o processamento, ou seja, tratamento de dados;

- **Consentimento do Titular dos Dados Pessoais -** qualquer manifestação de vontade do titular de maneira livre, inequívoca, específica, informada e explícita por escrito ou por qualquer outro meio;

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

- **Dados Anonimizados -** dado relativo a titular que não possa ser identificado, utilizando-se meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

- **Dados Pessoais -** qualquer informação, de qualquer natureza relativa a uma pessoa singular identificada ou identificável (“Titular dos Dados”);

- **Dados Pessoais de Menores de Idade –** é o tratamento de dados pessoais de crianças e adolescentes através de consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal;

- **Dados Sensíveis -** são dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, político, ou filosófico, referente à saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Esses dados podem sujeitar seu titular a práticas discriminatórias, ou permitir a sua identificação de forma inequívoca;

- **Direito à Explicação –** o controlador de dados, durante o período que estiver utilizando, armazenando, guardando os dados pessoais do titular deverá a este sempre esclarecer ou informar o que for necessário;

- **Direito de Acesso –** a política deverá informar um canal de contato entre controlador e titular de dados. Tal canal será responsável por esclarecer as questões de privacidade, eventuais dúvidas, reclamações ou comentários que possam surgir a partir da leitura da política. É importante que os atendentes do referido canal, tenham expertise para tratar e esclarecer tais questões;

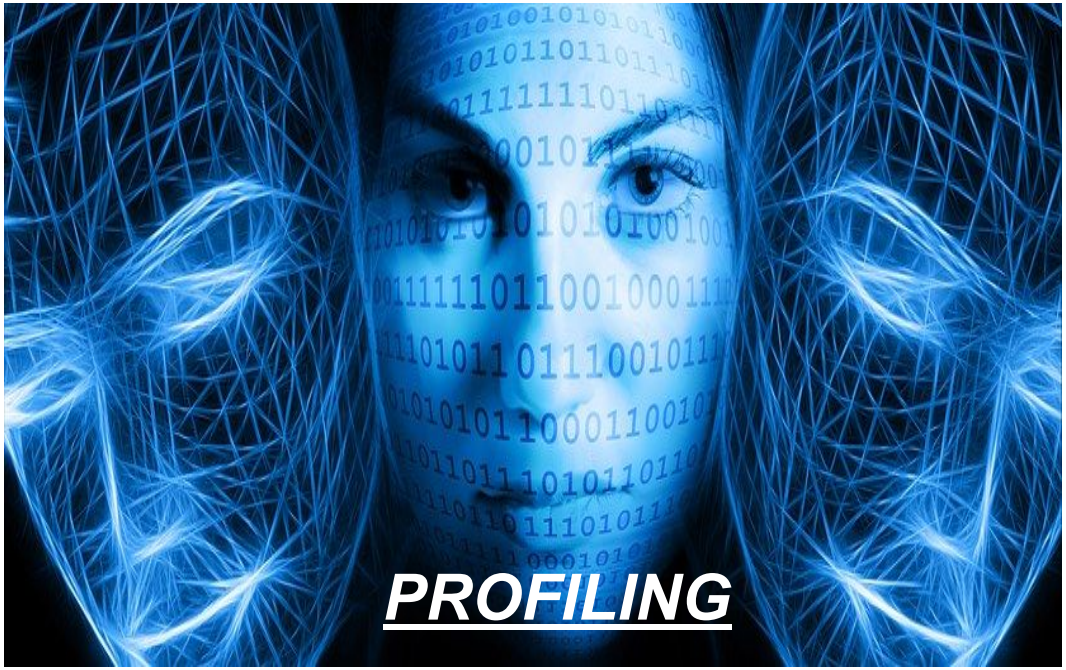
- **Encarregado de Proteção de Dados ou *Data Protection Officer* (DPO) -** pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares e a autoridade nacional, ou seja, pessoa designada pela organização que estará envolvida em todas as questões relacionadas com a proteção de dados pessoais;

- **Finalidade de Tratamento -** é o tratamento a ser feito quanto aos dados pessoais coletados com propósitos legítimos, específicos, explícitos e informados ao titular;

- **Informações de Contato –** são meios de comunicação para se reportar um incidente;

- **Legislações Vigentes e Competentes -** legislação geral, local e setorial. Ex: LGPD, Código de Defesa do Consumidor, Marco Civil da Internet, etc;

- **Legítimo Interesse –** refere-se à previsão de autorização para tratamento de dados pessoais quando necessário para atender aos interesses legítimos do responsável pelo tratamento ou terceiro;



- **Necessidade/ Minimização dos dados (*Data Minimization*)** - limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com a utilização de dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento;

- ***Profiling* -** forma automatizada de processamento de informação pessoal, com o objetivo de avaliar e tipificar indivíduos com base nos seus dados pessoais;

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

- **Pessoa Identificável** – é a pessoa que possa ser identificada direta ou indiretamente, por referência como o nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, econômica, cultural, social e outros;

- **Privacidade desde a Concepção (*Privacy by Design*) -** significa levar o risco de privacidade em conta em todo o processo de concepção de um novo produto ou serviço;

- **Privacidade por Padrão (*Privacy by Default*)** - significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por padrão (alguns autores utilizam a expressão "por defeito"), apenas será recolhida/coletada, utilizada e conservada para cada tarefa a quantidade necessária de dados pessoais;
- ***Privacy Impact Assessments* (PIA)** - permite que a organização encontre problemas nas fases iniciais de qualquer projeto, reduzindo os custos associados e danos à reputação que poderiam acompanhar uma violação das leis e regulamentos de proteção de dados;

- **Pseudonimização** – substituição de informação identificável por identificadores artificiais, cifragem, codificação de mensagens e outros;

- **Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) ou *Data Protection Impact Assessment* (DPIA) -** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

- **Retenção dos Dados –** a política deverá esclarecer qual o período de retenção dos dados e se não for possível estimá-lo, informar o critério utilizado para esta retenção e descarte;

- **Segurança dos Dados –** são medidas técnicas e administrativas aptas a proteger a segurança dos dados no seu processamento;

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

- **Tratamento de Dados Pessoais** - toda operação realizada com dados pessoais, como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração;

- **Uso de Cookies** – são pequenos arquivos que os sites colocam no disco rígido do seu computador quando você os visita pela primeira vez. Como se fosse um cartão exclusivo de identificação que guarda preferências e nomes de usuário, registrando produtos e serviços, personalizando páginas;

- **Violação de Dados Pessoais** - violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

- **Violação de Segurança (Incidentes de Segurança)** - evento com um efeito adverso real na segurança das redes e dos sistemas de informação;

Capítulo 6

Boas Práticas na Elaboração da Política de Privacidade - Checklist

Por Remi Yun e Adriana Tocchet Wagatsuma

Abaixo, seguem algumas boas práticas que podem ser utilizadas como um “checklist” para elaboração de uma política de privacidade.

1. **DISPONIBILIDADE DA POLÍTICA:**
   - ❖ Exibir a política de privacidade em uma posição clara na página inicial do site, sendo ideal um link para cada página do site
   - ❖ Desenvolver mecanismos de disponibilização offline para titulares sem acesso à internet
   - ❖ Recomenda-se que os titulares recebam as informações necessárias desde o primeiro ponto de comunicação

2. **LINGUAGEM DA POLÍTICA**
   - ❖ As políticas de privacidade devem ser claras e fáceis de entender por indivíduos que não têm conhecimento da lei de privacidade
   - ❖ Deve haver uma tradução da política para o idioma local relevante;

3. **INFORMAÇÕES IMPORTANTES E QUEM SOMOS**
   - ❖ Propósito da política de privacidade
   - ❖ Especificar o controlador
   - ❖ Detalhar os meios de contatos
   - ❖ Esclarecer sobre o dever de informar sobre mudanças/alterações no aviso de privacidade
   - ❖ Esclarecer se houver links de terceiros

4. SOBRE OS DADOS COLETADOS

- ❖ Detalhar os tipos de dados que são coletados;
  - Dados Pessoais - nome, sobrenome, estado civil, data de nascimento, etc;
  - Dados de Contatos - endereço de cobrança, entrega, e-mail e números de telefone;
  - Dados Financeiros - conta bancária e número do cartão de pagamento;
  - Dados Técnicos - endereço IP, dados de login, etc;
  - Dados de Perfil - nome de usuário e senha, preferências, comentários e respostas à pesquisa, etc;
  - Marketing e Comunicações - preferências em receber marketing e comunicação;
  - Outros;

5. COMO OS DADOS FORAM COLETADOS

- ❖ Esclarecer e especificar como os dados são coletados;

6. USO DOS DADOS

- ❖ Esclarecer que os dados pessoais serão utilizados apenas quando houver consentimento legítimo interesse ou previsão legal;
- ❖ O consentimento poderá ou não ser obtido em documento apartado da política de privacidade;
- ❖ Especificar as finalidades para as quais os dados pessoais coletados serão utilizados;
- ❖ Esclarecer sobre possíveis ações promocionais;
- ❖ Esclarecer sobre o direito de cancelamento;
- ❖ Esclarecer sobre as finalidades dos cookies e disponibilizar a política de cookies;
- ❖ Esclarecer sobre a possibilidade de mudanças de finalidade quanto ao tratamento de dados, mediante notificação e fundamento legal que o permita;

7. DIVULGAÇÕES DOS DADOS

- Esclarecer sobre a possibilidade de compartilhamento dos dados pessoais para as finalidades estabelecidas
- Esclarecer sobre a possibilidade de vender, transferir ou fundir partes dos negócios ou ativos
- Esclarecer que todos os terceiros/processadores estão em conformidade quanto à segurança dos dados pessoais, permitindo-se apenas o processamento dos dados pessoais para fins específicos e de acordo com instruções do controlador

8. TRANSFERÊNCIAS INTERNACIONAIS

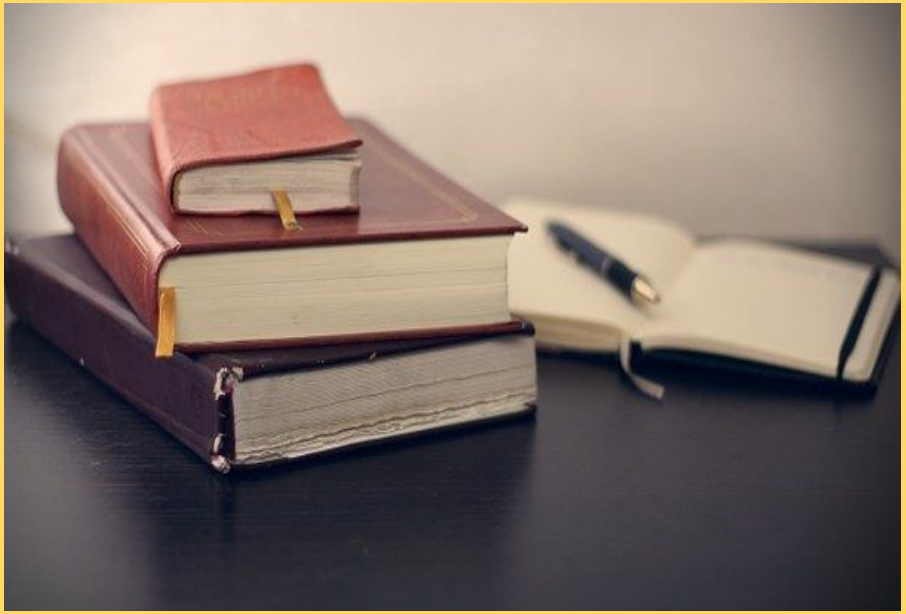
- Esclarecer sobre a possibilidade de transferência internacional de dados
- Assegurar sobre o grau de proteção e os tipos de salvaguardas adotadas
- Fornecer meios de contatos para maiores esclarecimentos

9. SEGURANÇA DOS DADOS

- Esclarecer sobre as medidas de segurança implementadas para evitar incidentes quanto aos dados pessoais
- Assegurar sobre o estabelecimento de procedimentos quanto a qualquer suspeita de violação de dados pessoais
- Assegurar a devida notificação do titular dos dados pessoais, bem como de qualquer regulador aplicável, se houver previsão legal

10. RETENÇÃO DE DADOS

- Esclarecer sobre o tempo de retenção de dados pessoais, ou seja, que os dados pessoais serão mantidos pelo tempo necessário para atender a quaisquer requisitos legais, boas práticas, etc.
- Esclarecer sobre o critério adotado para adoção do prazo de retenção
- Esclarecer sobre a possibilidade de exclusão de dados, quando requerido pelo titular
- Esclarecer sobre a possibilidade de anonimizar os dados pessoais para fins estatísticos ou de pesquisa



11. DIREITOS LEGAIS DO TITULAR

- Esclarecer sobre os direitos do titular em relação aos seus dados pessoais, tais como: acesso, correção, exclusão, restrição, transferência e retirar o consentimento
- Especificar os contatos disponíveis para exercício desse direito
- Esclarecer sobre a possibilidade ou não de eventual cobrança
- Especificar prazo para resposta quanto às solicitações

12. GLOSSÁRIO

- Definir termos e conceitos utilizados na política de privacidade

Considerações Finais

Um dos principais e mais polêmicos pontos apresentados por Hintze, autor que serviu de inspiração e de referência para este trabalho, é a extensão da política de privacidade e o seu grau de detalhamento. Esta é uma das principais queixas dos usuários, clientes e funcionários que precisam lê-la, compreendê-la e aceitá-la para usufruírem de serviços prestados ou serem contratados para um emprego. Assim como Hintze, entendemos que não é a extensão da política de privacidade que importa, mas sim o quanto esclarecedora e completa é a mensagem que ela passa ao usuário.

Ou seja, de uma forma geral, a política de privacidade deve ter as seguintes características: ser escrita em linguagem clara, direta e de fácil compreensão; deve ser completa de forma a deixar de antemão o seu leitor esclarecido acerca de todos os tipos de tratamento ao qual o seu dado pessoal será submetido, relacionando-o a alguma base legal dentre aquelas estabelecidas no artigo 7º da LGPD, de forma a legitimar o tratamento, dentre outros requisitos.

Entendemos que todas as políticas de privacidade devem respeitar requisitos comuns acerca da construção, mas que não há forma genérica ideal. Assim, a especificidade de cada modelo de negócio que trabalha com dados pessoais deve ser observada.

Cada política de privacidade nasce de um contexto único, respeitando-se a cultura da organização e do próprio negócio.

Fica, então, lançado o desafio aos profissionais em desenvolver tais políticas sob a égide das leis de proteção de dados.

Resta ainda esclarecer que a motivação para a elaboração desta obra foi a de destacar alguns aspectos de presença obrigatória nas políticas de privacidade e construir um material de consulta prático e de fácil leitura.

Por fim, esperamos que este texto, escrito por várias mãos, rico em diversidade de conhecimento, nascido da nossa paixão pela proteção de dados e da vontade de transmitir um pouco do *know-how* adquirido nas longas horas de estudos, seja útil a quem a ele tiver acesso.

Certamente, o tema não se esgota nesta obra, que nada mais é do que um guia básico que pode e deve servir como inspiração e base para que outros sigam com o trabalho e o aprofundem com outros aspectos práticos do desenvolvimento de uma política de privacidade.

Agradecemos por ter nos acompanhado até aqui!

Angela Maria Rosso