Auditoria de Sistemas

Prof. Luiz Antonio Ferraro Mathias

Aula 09

Privacidade dos dados pessoais

A importância da proteção de dados pessoais

Os dados pessoais têm sido alvo de muitas notícias recentemente, e violações de dados vêm acontecendo em empresas de arquivos de crédito, companhias aéreas e até mesmo naquelas que deveriam saber gerenciar melhor esses dados, como por exemplo um fornecedor de proteção de dados.

A tecnologia facilitou a violação de dados e sua transferência para as mãos erradas. A privacidade de dados é importante para as informações pessoais, e mais ainda para categorias especiais de dados pessoais, incluindo:

a) CPFs

b) Histórico médico

c) Origem étnico-racial

d) Crenças religiosas ou filosóficas

e) Opiniões políticas

f) Associação a sindicatos

g) Dados biométricos usados para identificar um indivíduo

A importância da proteção de dados pessoais

h) Dados genéricos

i) Dados de saúde

j) Dados relacionados a preferências sexuais, vida sexual e/ou orientação sexual

Com dados pessoais sendo coletados em uma taxa cada vez maior, e com os saltos na tecnologia usado para alavancá-lo, não é de se estranhar que os estados, países e blocos comerciais procurem aumentar a regulamentação nessa área. Atualmente, há muito mais discussões sobre a Lei de Proteção de Dados Pessoais no Brasil.

Ciclo de vida do tratamento de dados pessoais

O tratamento de dados pessoais de pessoas naturais (físicas) é baseado em um ciclo de vida que se inicia com a coleta do dado e que determina a "vida" (existência) do dado pessoal durante um período, de acordo com certos critérios de eliminação.

Para orientar a prática do tratamento, o controlador divide o ciclo de vida do tratamento dos dados pessoais em 5 (cinco) fases: coleta, retenção, processamento, compartilhamento e eliminação.

Fases do ciclo de vida do tratamento de dados pessoais

O ciclo de vida do tratamento do dado pessoal tem início com a coleta deste e se encerra com a eliminação ou descarte. Cada fase do ciclo de vida tem correspondência com operações de tratamento claramente definidas.

a) A fase “coleta” refere-se à coleta, produção, recepção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.);

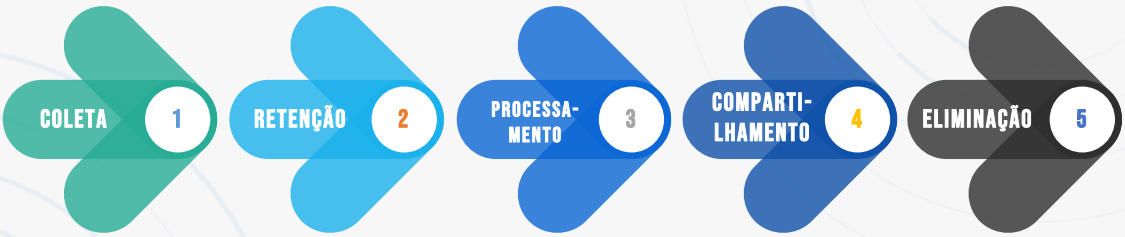
b) A “retenção” corresponde ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.);

c) O “processamento” é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador;

d) O “compartilhamento”, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhamento de dados pessoais;

e) A “eliminação” é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, bem como eliminação de documentos eletrônicos ou em papel em que constam dados pessoais. Esta fase também contempla o descarte dos ativos organizacionais (documentos, equipamentos etc.) nos casos necessários ao negócio da instituição.

Fases do ciclo de vida do tratamento de dados pessoais



Fases do ciclo de vida do tratamento de dados pessoais

As fases do ciclo de vida do tratamento de dados pessoais encontram correlação com as operações de tratamento previstas na LGPD:

Fases do ciclo de tratamento	Operações de tratamento
Coleta	Coleta, produção, recepção, acesso.
Retenção	Arquivamento, armazenamento e acesso
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração, modificação e acesso.
Compartilhamento	Transmissão, distribuição, comunicação, transferência, difusão e acesso.
Eliminação	Acesso e eliminação.

A Lei Geral de Proteção de Dados (LGPD)

A Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios, prevalecendo, portanto, sobre quaisquer outras leis municipais ou estaduais.

A (LGPD), sancionada em 14/08/2018, entrou em vigor em 18/09/2020 após inúmeras discussões normativas nos Poderes Executivo e Legislativo. As infrações e sanções administrativas, de acordo com a Lei 14.010/2020, só passam a valer a partir de 01/08/2021. Esta Lei representa o primeiro regulamento geral sobre proteção de dados pessoais no Brasil, onde o tema era tratado apenas por leis específicas, como o Código Brasileiro de Defesa do Consumidor (Lei 8.078/1990) e a Lei Brasileira da Internet (Lei 12.965/2014).

A LGPD oferece aos indivíduos maior controle sobre seus dados pessoais, garantindo maior transparência sobre a utilização dos dados e exige maior segurança e controles de proteção de dados.

A Lei Geral de Proteção de Dados (LGPD)

Diferentemente das leis de privacidade em algumas jurisdições, a LGPD é aplicável às organizações de todos os tamanhos e em todos os setores e foi inspirada no GDPR (*General Data Protection Regulation*) ou Regulamento Geral de Proteção de Dados europeu, que é geralmente visto internacionalmente como um modelo em questões de privacidade, portanto, há de se esperar que as interpretações e desenvolvimentos no GDPR influenciem diretamente a obrigatoriedade da LGPD no decorrer do tempo.

A LGPD foi construída com base em determinadas premissas e tendo como fundamentos:

I. o respeito à privacidade (direito à reserva de informações pessoais);

II. a autodeterminação informativa (o cidadão é soberano sobre suas próprias informações pessoais e deve ser o protagonista de quaisquer temas relacionados ao tratamento de seus dados);

III. a liberdade de expressão, de informação, de comunicação e de opinião (previstos na CF 88);

IV. a inviolabilidade da intimidade, da honra e da imagem (preservação de direitos do cidadão);

V. o desenvolvimento econômico e tecnológico e a inovação (não prejudicam as atividades das empresas que realizam tratamento de dados);

A Lei Geral de Proteção de Dados (LGPD)

VI. a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por 2 (dois) “agentes de tratamento”: o Controlador e o Operador:

• O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito da organização, o controlador é representado pelo corpo diretivo da instituição, imbuído de adotar as decisões acerca do tratamento de tais dados.

• O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. No contexto da organização, os operadores são os colaboradores, ou mesmo, parceiros de negócio (fornecedores), pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

A Lei Geral de Proteção de Dados (LGPD)

Considera-se “tratamento de dados” pessoais, qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Essas operações de tratamento são destacadas a seguir:

1. COLETA - recolhimento de dados com finalidade específica;
2. PRODUÇÃO - criação de bens e de serviços a partir do tratamento de dados;
3. RECEPÇÃO - ato de receber os dados ao final da transmissão;
4. CLASSIFICAÇÃO - maneira de ordenar os dados conforme algum critério estabelecido;
5. UTILIZAÇÃO - ato ou efeito do aproveitamento dos dados;
6. ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
7. REPRODUÇÃO - cópia de dado preexistente obtido por meio de qualquer processo;

A Lei Geral de Proteção de Dados (LGPD)

8. TRANSMISSÃO - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;
9. DISTRIBUIÇÃO - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
10. PROCESSAMENTO - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;
11. ARQUIVAMENTO - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a sua vigência;
12. ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;
13. ELIMINAÇÃO - ato ou efeito de excluir ou destruir dado do repositório;
14. AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;
15. CONTROLE - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
16. MODIFICAÇÃO - ato ou efeito de alteração do dado;
17. COMUNICAÇÃO - transmitir informações pertinentes a políticas de ação sobre os dados;
18. TRANSFERÊNCIA - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
19. DIFUSÃO - ato ou efeito de divulgação, propagação, multiplicação dos dados;
20. EXTRAÇÃO - ato de copiar ou retirar dados do repositório em que se encontrava.

A Lei Geral de Proteção de Dados (LGPD)

Há de se observar que as disposições da LGPD não são aplicadas ao tratamento de dados pessoais nas seguintes situações:

I. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II. Realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os artigos 7º e 11 da LGPD);

III. Realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou;

IV. Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

A Lei Geral de Proteção de Dados (LGPD)

A LGPD previu expressamente, 10 (dez) hipóteses de tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais. Estas hipóteses são:

I. Mediante o fornecimento de consentimento pelo titular;

II. Para o cumprimento de obrigação legal ou regulatória pelo controlador;

III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD;

IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

A Lei Geral de Proteção de Dados (LGPD)

VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O tratamento de dados pessoais, pelo controlador, considerará as hipóteses de tratamento descritas acima, bem como observará a boa-fé e os demais princípios estabelecidos no ordenamento jurídico:

a) Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. O tratamento posterior somente será possível se for compatível com esses propósitos e finalidades. No caso da organização, a finalidade relaciona-se com a execução de suas atividades cotidianas vinculadas com a sua atividade fim, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória;

A Lei Geral de Proteção de Dados (LGPD)

b) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

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

f) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

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

h) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

A Lei Geral de Proteção de Dados (LGPD)

i) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

j) 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.

A LGPD traz regramento específico para o tratamento de dados pessoais sensíveis, que são definidos como "*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*.".

São dados cujo tratamento pode ensejar a discriminação do seu titular, e por isso, são sujeitos a proteção mais rígida. O tratamento mediante consentimento exige que se registre a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento.

Relatório de impacto á Proteção de Dados (RIPD)

A Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

A LGPD estabelece que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

O RIPD deverá conter, no mínimo: a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Término do tratamento de dados

Conforme estabelece a LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses: (i) exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade; (ii) fim do período de tratamento; (iii) revogação do consentimento ou a pedido do titular; (iv) determinação da autoridade nacional em face de violação de dispositivo legal.

Segurança da informação

Os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais. A proteção dos dados pessoais será alcançada por meio de medidas de segurança, técnicas e administrativas, que deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução, algo previsto no conceito fundamental para a proteção da privacidade dos dados pessoais denominado Privacidade desde a Concepção (do inglês *Privacy by Design*).

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo.