PROGRAMA DE ADEQUAÇÃO À PROTEÇÃO DE DADOS PESSOAIS

Guia Prático

Coordenação – Remilina Yun (Remi)

OBRA COLETIVA

ADRIANA TOCCHET WAGATSUMA

ADRIANO MENDES

ANA CAROLINE DA SILVA

ANGELA MARIA ROSSO

CAROLINA BRAGA

DAYANA CAROLINE COSTA

FERNANDA MAIA

GISELE KAUER

GUSTAVO C. GODINHO

GUSTAVO ROCHA

MARCILIO BRAZ JR.

MARIA ANGELA MENDES NASCIMENTO

MARIANA DE SOUZA CRUZ CAPARELLI

NÚRIA BAXAULI

PAULO LILLA

PAULO ROGÉRIO DIAS DE OLIVEIRA

RACHEL GONZAGA

RAPHAEL DUTRA CAMPOS

REMILINA YUN (REMI)

VINICIUS RAVANELLI COSSO

VIVIANE CORROCHER MALANGA

SUMÁRIO

BIBLIOGRAFIA

❖ INTRODUÇÃO

Esse e-book foi desenvolvido a partir de uma iniciativa (sem fins lucrativos) que começou em Agosto/2018, o grupo **LGPD Acadêmico**, o qual é composto por voluntários do Brasil inteiro, apaixonados pelo mundo da privacidade e com objetivo comum – aprender e compartilhar.

Por identificar uma necessidade direta da sociedade, organizações corporativas – independente do seu porte, profissionais, entre outros, por conta da Lei Geral de Proteção de Dados (Lei Nº. 13.709,de 14 de Agosto de 2018) que entrará em vigor em 16 de agosto de 2020.

O LGPD Acadêmico decidiu reunir o conhecimento e experiência prática de cada autor neste material através de uma linguagem simples, evitando-se o famoso "juridiques", recorrendo a termos técnicos somente quando absolutamente necessário e claro, acessível a todos de maneira gratuita.

Boa Leitura!

❖ POR ONDE COMEÇAR

Entendimento quanto aos principais conceitos

Vinicius Ravanelli Cosso

Informação é aquilo a que se pode dar sentido, podendo representar apenas dados ou gerar conhecimento. Não há, portanto, informação sem um observador cognitivo que possa percebê-la.

A informação não necessariamente está vinculada à atividade ou percepção humana, sendo encontrada e até processada facilmente no meio ambiente natural quando consideramos, por exemplo, a informação genética que compõe o DNA, os sonares dos morcegos, ou mesmo as diversas informações captadas pelos cães ao farejar a urina de outros cães.

Já os dados são os componentes das informações que, para os fins aqui propostos, são armazenados em suportes físicos - sulcos na pedra, desenhos, escrita em papel, livros, filmes fotográficos e outros - ou mídias digitais, nas quais os dados são representados de forma binária, mais comumente traduzida por “0” e “1”, mas que também pode estar representada em diversas outras formas, como “verdadeiro” e “falso”, “presente” e “ausente”, “ligado” e “desligado”, “positivo” e “negativo” e assim por diante, sendo as mídias mais comuns os discos rígidos, fitas magnéticas, discos óticos, e diversos tipos de chips de memória como RAM, EPROM e NAND, mas também presentes em cartões perfurados, como os usados em grande escala no censo dos Estados Unidos em 1890, com a aplicação da tecnologia desenvolvida por Herman Hollerith.

Com a evolução tecnológica e ampliação da utilização de dados para as mais diversas finalidades, por pessoas, empresas e governos, ainda mais após o desenvolvimento de uma sociedade da informação, surge a necessidade de

regulação da utilização de dados, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, nos termos da LGPD.

Entretanto, não é qualquer dado que será objeto de regulação pela LGPD, mas apenas os dados definidos pela Lei e denominados Dados Pessoais. Portanto, Dado Pessoal é toda e qualquer informação relacionada a pessoa natural identificada ou identificável. (Art. 5º, I).

Adicionalmente aos dados pessoais, a LGPD elege ainda alguns destes como dados pessoais qualificados, lhes dedicando maior proteção. São os denominados Dados Pessoais Sensíveis, definidos como tais os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (Art. 5º, II).

Para a correta aplicação da LGPD é importante delimitarmos o seu objeto, que são os Dados Pessoais, atendendo às seguintes condições:

(1) toda e qualquer informação;
(2) relacionada a pessoa natural;
(3) identificada ou identificável.

Assim, não se aplica a LGPD, nas seguintes hipóteses:

(1) Se os dados forem anônimos, ou tiverem sido anonimizados, (art. 5º, III), não sendo a pessoa natural identificada ou identificável;
(2) Se os dados não forem relacionados a pessoa natural;

Não há restrição no texto legal a dados digitais, sendo que a LGPD também será aplicada a registros em suporte analógico.

Em relação à possibilidade de identificação, somente não haverá aplicação da LGPD se a anonimização for efetiva, devendo ser impossível, de forma direta ou indireta, a identificação da pessoa natural. Caso contrário, esta seria, então, identificável.

Destacamos que, para definição de incidência ou não da LGPD tomando-se por referência a pessoa às quais os dados se referem, não basta separar os dados da base em pessoas jurídicas e pessoas físicas, pois se os dados que constam como de titularidade de pessoa jurídica permitirem a identificação de informações sobre uma pessoa física, identificada ou identificável, haverá a aplicação da LGPD.

Damos o exemplo de um cadastro baseado em CNPJ, referente a um Empreendedor Individual (EI) ou Microempreendedor Individual (MEI), em que os dados são diretamente relacionados a uma pessoa natural.

Além de definir o seu objeto, a LGPD define a quem se aplicam as normas de proteção de dados pessoais (art. 3º):

(1) Se aplica à pessoa natural ou jurídica, de direito público ou privado;
(2) Sobre qualquer operação de tratamento de dados pessoais;

Independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- A operação de tratamento seja realizada no Brasil;
- A atividade de tratamento seja direcionada a indivíduos no Brasil;
- A coleta dos dados tenha ocorrido no Brasil, de brasileiro ou estrangeiro de passagem pelo nosso território;

São exceções à aplicação da LGPD o tratamento de dados pessoais que:

- For realizado pela pessoa natural para fins particulares e não comerciais;
- Realizado para fins jornalísticos, artísticos ou acadêmicos;

- Realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou investigação de crimes; e
- Sobre dados oriundos de outro país, que proteja os direitos de privacidade de maneira semelhante ao Brasil, desde que não haja participação de agentes brasileiros.

Conscientização da organização

Adriana Tocchet Wagatsuma

A conscientização da organização é um passo muito - se não o mais - importante na jornada de implementação da nova lei. A construção da cultura de privacidade, o *awareness* da proteção de dados e confiança digital, é essencial para o bom desenvolvimento, sustentabilidade do programa e a criação de conceitos essenciais como o *privacy by design*.

E para construí-la, os conceitos da nova lei deverão ser difundidos e disseminados em toda estrutura das organizações. Todos os níveis de colaboradores, da copeira mais júnior até o C-level da Companhia, exercerão um importante papel para que os requisitos legais sejam cada vez mais observados nas pautas diárias, estando presentes desde um simples cadastro na entrada no edifício até um complexo projeto de engenharia, por exemplo.
Cada colaborador deverá estar ciente sobre o papel que irá exercer; o impacto da nova lei em sua atividade diária. Daí a importância de construir-se um ambiente capaz de engajar e orientar os colaboradores em relação à importância e as vantagens advindas da observância dos requisitos da LGPD.

Neste sentido, treinamentos periódicos sobre a lei são necessários para que se abram canais de discussão e esclarecimentos. É muito importante que os empregados saibam a quem ou a que canais recorrer em caso de dúvidas (e, com certeza, elas surgirão).
Outro ponto a ser sopesado, é que as organizações dificilmente contratarão um grande número de profissionais com *expertise* de proteção de dados e

privacidade. O natural e o caminho mais comum a ser trilhado é o de treinar e qualificar os empregados que já estão em seu *staff*.

A organização deve fazer um diagnóstico em torno de suas informações e, em seguida, um prognóstico acerca de quais práticas devem ser mantidas ou modificadas para assegurar a sua conformidade regulatória.

Com a entrada da LGPD, o profissional deverá ser capaz de identificar o que muda em suas atividades diárias, identificando os dados pessoais utilizados em seus processos, bem como o que deverá ser feito diferente, inclusive, uma eventual necessidade de eliminação.

Checar seus arquivos, inclusive, os documentos físicos (e não só sistemas e arquivos eletrônicos) e reavaliá-los, questionando-se, primeiramente, se os dados não deveriam ser eliminados, quiçá nunca deveriam ter sido coletados. Atualmente, muitos dados são coletados sem qualquer finalidade, observando-se exclusivamente a lógica de coletar o maior número de informações possível sem qualquer propósito. Informações sem utilização além de não possuírem qualquer valor, ainda atraem para a empresa ou cadeia que os coletaram a responsabilidade de por eles responderem em caso de eventual *data breach*.

A LGPD não proíbe a utilização de dados pessoais na concepção de produtos ou serviços, apenas disciplina para que o titular possa ter pleno controle sobre a forma que os seus dados são utilizados; permitindo ou não sua utilização. A coleta, antes de tudo, deve ser norteada observando-se a boa fé e os princípios elencados no artigo 6º da LGPD, destacando-se a finalidade, a transparência e necessidade.

Ademais, para engajar e comprometer a organização, nos parece que o melhor caminho é mostra-lhes que a lei não vem para inibir ou proibir negócios, mas sim para criar oportunidades e fortalecimento dos negócios.

É certo que as multas reguladas assustam -- a lei disciplina que cada infração poderá chegar a até R$ 50.000.000,00 -- todavia, há uma perda intangível advinda de *data breachs,* que pode, afetar a imagem e a da marca da empresa, danos reputacionais irreparáveis, além da perda de credibilidade, principalmente quando a segurança digital é um dos diferenciais do produto ou serviço.

Além disso, estar *complaint* passará a ser uma vantagem competitiva ou a sobrevivência do próprio negócio. A autoridade, recém legislada, não terá estrutura organizacional para fiscalizar todas as empresas que tratam dados. Todavia, de maneira a viabilizar a sustentabilidade e a observância dos requisitos legais, criou mecanismo na própria lei que coloca o próprio sistema a fiscalizar-se. Assim, ao responsabilizar solidariamente toda a cadeia envolvida no tratamento de dados - controlador (es) e operador (es) - impõe ao Controlador diligente a obrigação de envolver-se somente com operadores que observam e cumprem os ditames legais.

Neste sentido, colaciono abaixo artigo de autoria de Bruno Bioni que coaduna com este entendimento:

> *Duas das principais ferramentas de adequação à nova lei seguem essa lógica: mapeamento de dados e relatórios de impacto à proteção de dados. Respectivamente, a organização deve fazer um diagnóstico em torno de suas informações e, em seguida, um prognóstico acerca de quais práticas devem ser mantidas ou modificadas para assegurar a sua conformidade regulatória.*
>
> *Se realizado de forma adequada, é um exercício que trará novas ideias, sobretudo em torno de dados subutilizados com o potencial de informar novas ações tanto no poder público, quanto no setor privado.*
>
> *O processo de conformidade não deve ser internalizado como um custo, muito menos enquanto uma papelada para formalmente fazer um "check-list" das*

obrigações legais. Ao contrário, deve ser compreendido como um investimento capaz de otimizar e tornar mais eficiente as atividades dos atores regulados.

Esse cenário exige que o Sênior Management promova cada vez mais um ambiente nas organizações que prime pela transparência e *accountability*, criando e disseminando uma cultura de privacidade e de proteção de dados, enfatizando como o sucesso da companhia e sustentabilidade dos negócios, numa economia 4.0, depende da observância e entendimento destes requisitos legais.

Criação de um Comitê Multidisciplinar

Adriana Tocchet Wagatsuma & Raphael Dutra Campos

A multidisciplinaridade do assunto fica evidente desde a primeira leitura da Lei 13.708/18. A lei geral de proteção de dados pessoais (LGPD) aborda aspectos que não estão restritos a um conhecimento técnico específico. Ao lê-la resta claro que para implementá-la efetivamente será necessário um esforço conjunto de diferentes profissionais com *know- how* diferentes, que se complementarão.

O viés de segurança da informação é óbvio e, em razão também deste fato, Tecnologia da Informação, desempenhará um papel importante no projeto. O Departamento Jurídico, Controles Internos, Governança e *Compliance* são áreas que terão papel fundamental no projeto.

As áreas de Marketing, que são as áreas com maior interesse na coleta e utilização dos dados, também deverão ser envolvidas de forma que esclareçam o ciclo de vida dos dados coletados e sua utilização, que em alguns casos é vital para o desenvolvimento do negócio.

Um programa de privacidade e proteção de dados pessoais é extremamente complexo e demanda esforços conjuntos de diversas partes interessadas. Por conta dessa alta complexidade, é recomendável que as organizações estruturem

um Comitê Multidisciplinar que irá atuar e cooperar com o desenvolvimento do Programa de Proteção de Dados Pessoais.

Esse comitê deve, portanto, compreender e acompanhar as mudanças regulatórias e setoriais, além de observar possíveis fontes de ameaças externas e internas, de modo a garantir a conformidade nas práticas de negócios existentes ou emergentes.

O Comitê Multidisciplinar também responsável por conscientizar e responder perguntas das diversas partes interessadas e, além disso, liderar o tema dentro da organização. Ele é fundamental para o sucesso do programa, pois deverá buscar um alinhamento estratégico com as metas do próprio negócio da organização.

O alinhamento deve ocorrer tanto no campo regulatório - mitigando possíveis riscos de infrações, multas, supervisões e ações legais, como também no campo da conscientização de clientes, funcionários, investidores e fornecedores sobre a importância da privacidade e da proteção dos dados pessoais.

Assim, ao final da análise, o alinhamento do Programa de Proteção de Dados Pessoais com as metas de negócio da organização desencadeará - de fato - uma vantagem estratégica para a organização, por meio de uma visão regulatória adequada e uma coerente conscientização dos objetivos que serão alcançados por meio da conformidade.

Do encarregado de proteção de dados

Adriano Mendes & Maria Angela Mendes Nascimento

Para alguns setores e conforme regulamentado pela Autoridade Nacional de Proteção de Dados - ANPD, o encarregado de proteção de dados, figura também conhecida como Data Protection Officer – DPO.

Este profissional será a pessoa responsável na empresa por acompanhar todas as demandas que dizem respeito à proteção de dados pessoais, bem como ser o ponto de contato e facilitar a comunicação entra e Empresa, titulares de dados pessoais e com a Autoridade Nacional de Proteção de Dados.

Dentro das melhores práticas e seguindo conceitos emprestados da GDPR europeia, sugere-se que o DPO tenha conhecimento e perfil multidisciplinar, podendo opinar sobre questões técnicas e jurídicas que envolvam a lei e seus desdobramentos dentro da organização, reportando-se preferencialmente à alta direção e com imparcialidade na função, quando possa haver conflito de interesses entre áreas e orçamentos afetados pelos investimentos em Proteção de Dados.

Embora a nomeação de uma pessoa para o cargo de DPO precise sempre recair sobre uma pessoa física, este não precisa ser um empregado contratado pela empresa, podendo ser uma pessoa física que acumule funções dentro da Organização ou mesmo um prestador de serviços identificado, contratado através de outra empresa ou instituição.

Dentre as principais funções do DPO, estão:

- Informar e orientar controlador, operador, seus profissionais e contratados sobre as obrigações e boas práticas a serem seguidas, de acordo com a Lei Geral de Proteção de Dados – LGPD;
- Monitorar o cumprimento da LGPD nas atividades de tratamento de dados da empresa, reunindo informações sobre procedimentos que executam

tratamento de dados, propondo e organizando práticas que assegurem a adequação à LGPD, bem como reportando eventuais incidentes no tratamento de dados;

- Realizar a comunicação entre empresa e a ANPD, o que compreende cooperar durante fiscalizações, cumprir diligências e adotar providências, podendo ainda realizar consultas perante esta autoridade sobre o adequado tratamento de dados; e
- Realizar a comunicação entre empresa e titular de dados, de forma a receber solicitações e reclamações, esclarecer dúvidas e permitir o exercício de seus direitos.

Este profissional deve ser envolvido e participar das decisões sobre as questões relacionadas à proteção de dados pessoais tratadas, tanto pela própria empresa, como no compartilhamento destes com fornecedores e terceiros.

Pelas funções, nota-se, portanto, que o cargo exige certa autonomia e independência, de maneira que o DPO exerça suas atribuições e emita opiniões conforme suas concepções e conhecimentos técnicos, sem qualquer direcionamento, instrução ou orientação de terceiros ou da alta direção. Tais características são essenciais para uma adequada aplicação da LGPD na empresa, isenta de inclinações que possam prejudicar o correto tratamento de dados.

Salienta-se, contudo, que o encarregado não possui poderes decisórios. Ele orienta, indica e recomenda, porém a decisão quanto à adoção ou não de suas instruções cabe à empresa.

Exceto em casos bem específicos e quando houver comprovado dolo, a responsabilidade decorrente de qualquer infração à LGPD será da empresa. Por este motivo, a empresa não deverá subestimar ou negligenciar as funções e perfil do DPO, sob pena de posteriormente arcar com as multas e sanções previstas na Lei.

A ANPD poderá também estabelecer hipóteses em que o Controlador e o Operador estarão dispensados da indicação do encarregado interno, tendo em consideração a natureza e o porte da empresa ou ainda o volume de operação de tratamento de dados.

De qualquer forma, recomenda-se que todos os operadores sigam as obrigações e boas práticas de acordo com a LGPD, haja vista que a sanção decorrente de infração à Lei poderá também ser aplicada ao operador.

A ANPD regulamentará ainda a possibilidade de um grupo econômico indicar um único encarregado para as empresas do grupo. Contudo, a disponibilidade do encarregado não poderá ser afetada, devendo ser mantido fácil acesso a este profissional.

Por fim, deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no site do controlador, a identidade e as informações de contato do DPO. Esta regra tem por finalidade garantir aos titulares de dados e à ANPD acesso fácil e direto ao encarregado, tendo em vista sua atribuição para atuar como canal de comunicação entre empresa, titulares de dados e a ANPD.

Mapeamento de dados

Dayana Caroline Costa

Uma das principais fases do processo de adequação de uma organização às regras da LGPD refere-se ao mapeamento dos dados pessoais. Essa é a etapa de traçar um raio-x da empresa, identificar quais dados pessoais que são coletados, quais as áreas da empresa que realizam o tratamento, onde e por quanto tempo esses dados ficam armazenados, com quem são compartilhados, qual a finalidade do tratamento, enfim, é a fase em que é elaborado um inventário completo dos dados pessoais tratados pela empresa, seja em meio digital ou físico.

Trata-se de uma etapa de verdadeiro autoconhecimento da organização. É a partir do mapeamento que as organizações conseguem mensurar o volume e sensibilidade dos dados que tratam e a complexidade de seus processos. É com base no mapeamento que a organização terá seu primeiro diagnóstico de adequação à LGPD.

Essa fase, geralmente, é uma das etapas mais demoradas do diagnóstico para implementação do programa de adequação, mas deve ser desempenhada com meticulosidade e muita atenção, pois o seu resultado é determinante para os próximos passos e direcionará todo o processo de implementação.

Para se iniciar o mapeamento dos dados pessoais de uma empresa, primeiramente o comitê de privacidade deverá estudar o organograma da companhia, identificar as principais áreas que podem, de alguma forma, ter algum tipo de dado pessoal e criar um cronograma de entrevistas que abranja todas as áreas impactadas, sendo certo que as mais críticas deverão ser tratadas com maior cautela.

Mapeamentos eficazes e completos geralmente abarcam praticamente todos os departamentos de uma empresa, pois sempre há, de alguma forma, algum dado pessoal transitando pelas áreas das organizações. No entanto, existem departamentos que já são reconhecidamente mais problemáticos e que tratam grande volume de dados pessoais, incluindo dados pessoais sensíveis como as áreas de Recursos Humanos, Marketing, TI, Análise de dados, entre outras.

Importante se atentar que até mesmo departamentos que, em um primeiro momento, não aparentam tratar dados pessoais, em uma investigação detalhada podem revelar o tratamento até mesmo de dados sensíveis.

Para realizar o mapeamento de cada setor da empresa, deve-se identificar quais as pessoas-chave de cada área ou subárea que participarão de entrevista

individual na qual serão extraídas as informações acerca do tratamento de dados realizado durante suas atividades.

Nem sempre o gerente ou diretor do departamento é o mais indicado para participar dessas entrevistas. É preciso que esta etapa seja suportada por alguém que saiba descrever, em detalhes, quais os dados pessoais tratados, as finalidades, sistemas utilizados, fluxos e outras informações de acordo com as atividades desempenhadas pela área mapeada.

Assim, muitas das vezes participam dessas entrevistas funcionários que lidam diretamente com a atividade que tem contato com os dados pessoais, o que não descarta a participação de gerentes ou outros cargos de gestão que possam contribuir no mapeamento.

Independentemente de quem serão os funcionários que fornecerão as informações para elaboração do mapeamento, é importante constar no relatório quem é o gestor responsável pela área e quem foi a pessoa entrevistada. Essa medida visa manter um registro do focal responsável pelo fornecimento das informações com vistas a identificar responsabilidades futuras, esclarecer dúvidas e eventualmente atualizar o mapeamento.

Além disso, é essencial que o parceiro de negócio (consultoria ou escritório jurídico) contratado pela empresa tenha expertise e habilidades suficientes para conseguir coordenar as entrevistas de mapeamento de modo a extrair o máximo de informações possíveis do entrevistado, instigando-o a repensar seus processos e rastrear situações em que pode haver tratamento de dados pessoais. Também é prudente reforçar, antes de iniciar a entrevista, alguns conceitos chave como o que é dado pessoal, dado pessoal sensível e tratamento.

Antes de iniciar a entrevista, também é recomendável rememorar ao entrevistado que a empresa está passando por fase de diagnóstico para

posteriormente se adequar à lei, sendo certo que a entrevista não tem qualquer relação com processos de auditoria, podendo o entrevistado sentir-se à vontade para relatar de forma completa e verídica, todos os fluxos de tratamento realizados por sua área de negócio. Isso porque algumas vezes o entrevistado, receoso por eventualmente estar tratando dados de forma indevida, pode omitir informações, o que impacta diretamente no resultado dos trabalhos e coloca a empresa em risco já, que fluxos podem não ser identificados e, portanto, não se incluírem no rol de processos internos a serem adequados às disposições da LGPD.

O tamanho da empresa, volume de dados, valor de investimento e outros são fatores que impactam decisões sobre qual o melhor método para realizar o mapeamento. Atualmente tem-se observado a preponderância do mapeamento manual, através do preenchimento de planilha excel.

Todavia, a depender da escolha da empresa, poderão ser utilizados softwares e tecnologias para ajudar no suporte dessa fase. De todo modo, no geral, o mapeamento inclui os seguintes levantamentos:

- quais os dados pessoais coletados;
- qual o tipo de dado pessoal (sensível ou não);
- quem são os titulares (funcionários, clientes, etc);
- qual o tipo de tratamento;
- qual a finalidade do tratamento;
- quais os sistemas de armazenamento dos dados;
- com quem os dados são compartilhados e com qual finalidade;
- qual o período de retenção dos dados;
- se há transferência internacional dos dados e com qual finalidade;
- quais as medidas de segurança implementadas;
- qual o fluxo interno dos dados mapeados;
- quais os direitos que são disponibilizados aos titulares;
- entre outros

Cabe destacar que, durante o preenchimento do mapeamento de dados, é importante que se dê especial atenção ao campo da "finalidade do tratamento". Isso porque essa informação é de extrema importância para que a próxima etapa do programa de adequação - identificação de bases legais - seja efetuada com sucesso. É necessário que o advogado responsável por indicar as bases legais mais adequadas para cada uma das linhas de tratamento de dados, tenha acesso a informações mapeadas de forma completa, inteligível e com descrição detalhada sobre o motivo pelo qual o tratamento dos dados se faz necessário. Essa informação se mostra relevante, inclusive, para identificação do atendimento ao princípio da adequação, finalidade e necessidade (art. 6º, I, II e III da LGPD, respectivamente).

Após o mapeamento dos dados as organizações se tornam capazes de visualizar melhor seus fluxos e entender a dinâmica e ciclo dos dados pessoais. Muitas descobertas são feitas durante a realização do mapeamento e gaps já podem ser identificados e sinalizados com as respectivas medidas para saná-los.

O mapeamento não é apenas uma necessidade para possibilitar a implementação total do programa de adequação à LGPD, mas também uma exigência de vários artigos da lei que mencionam, expressamente, a necessidade de registro dos tratamentos de dados realizados por uma companhia.

Além do mais, mapear corretamente os dados tratados por uma empresa, rastreando todo o percurso do dado pessoal, desde a coleta até a eliminação, possibilita uma melhor avaliação da segurança dos dados e a implementação correta de medidas de segurança que mitiguem a ocorrência de eventuais incidentes.

Por fim, cabe mencionar que o mapeamento de dados não é uma providência única mas sim uma atividade contínua que deve ser incorporada nas práticas da empresa e se manifestar ao final como um inventário vivo, que deve ser

continuamente revisado e atualizado a fim de manter as melhores práticas de tratamento e segurança dos dados pessoais em posse da empresa.

Compartilhamento de dados com terceiros

Rachel Gonzaga

O Controlador dos Dados Pessoais ao compartilhar (aqui comportando qualquer forma em que o Operador tenha acesso aos Dados Pessoais, como a transferência, o repasse, a comunicação dentre outros) dados pessoais com Operadores (exemplo: empresas de armazenamento em cloud, empresas de processamento de folha de pagamento) é solidariamente responsável por qualquer dano causado pelo Operador aos Titulares do Dados Pessoais.

Ou seja, se a sua empresa enviar dados para armazenamento em nuvem e a empresa contratada não adotar as medidas de segurança necessárias e houver uma Violação de Dados Pessoais (vide glossário), ela estará sujeita às penalidades da LGPD bem como os titulares poderão acionar diretamente a sua empresa para fins de reparação de danos sofridos, independentemente de ter sido uma falha do Operador.

Além disso, existem diversas obrigações do Controlador (garantir que os Titulares exerçam seus direitos, notificar a ANPD no caso de Violação de Dados) que, a partir do momento em que ele compartilha os Dados Pessoais, muitas vezes precisarão de apoio e informações do Operador.

Assim, o Controlador precisa, ao compartilhar Dados Pessoais com Operadores formalizar um contrato que o resguarde em relação aos seguintes pontos:

1. Definição de quem é o Controlador e quem é o Operador;
2. Garantir que o Operador esteja adequado às obrigações da LGPD incluindo boas práticas, governança corporativa e medidas de segurança

da informação (dica: importante que o Controlador defina o padrão técnico de segurança da informação);

3. Garantir que o Controlador possa realizar auditorias para verificar se a declaração de adequação à LGPD é verdadeira;
4. Especificar claramente quais Dados Pessoais e Categorias de Titulares serão compartilhados, bem como a finalidade do Tratamento (dica: incluir vedação de Tratamento pelo Operador para qualquer outra finalidade de forma expressa);
5. Definir o Direito de Regresso do Controlador;
6. Criar obrigação do Operador em colaborar com o Controlador para cumprimento das obrigações deste, tais como, exercício dos direitos dos titulares, notificação e informação no caso de ocorrência de Violação de dados Pessoais

(Dica: elencar todos os direitos e definir todas as informações necessárias para o caso de o Controlador ter que notificar alguma Violação de Dados Pessoais);

7. Incluir regras sobre exclusão dos Dados Pessoais após a extinção do contrato;
8. Regras de subcontratação pelo Operador;
9. Regras para Transferência Internacional (vide tópico Transferência Internacional);

Por fim, caso o Operador for realizar o Tratamento dos Dados Pessoais em outro país que não o Brasil deverá ser adotada alguma das medidas definidas na LGPD para possibilitar a transferência internacional dos Dados Pessoais (vide tópico Transferência Internacional).

Lembramos que esta é uma das situações em que haverá o compartilhamento de Dados Pessoais com terceiros, existem outras situações em que a sua

organização, enquanto Controladora dos Dados Pessoais deverá se preocupar com tal compartilhamento.

Transferência internacional

Paulo Lilla

A transferência internacional de dados pessoais é um dos temas mais relevantes da LGPD, uma vez que, diante da globalização econômica e do caráter internacional de diversas operações, existem situações em que controladores de dados acabam compartilhando dados com operadores (ou mesmo com outros controladores) localizados fisicamente em outros países. Em outras palavras, ainda que os dados pessoais sejam coletados no Brasil, podem acabar sendo tratados em outra jurisdição.

Esse tipo de situação é muito comum, por exemplo, em casos de compartilhamento de dados de colaboradores entre empresas do mesmo grupo econômico (dados ficam armazenados na sede da matriz no exterior, por exemplo), contratação de servidores de *cloud computing* que utilizam data centers localizados em outros países, terceirização de SAC, dentre outras.

Se atualmente não há regras sobre essas operações de transferência internacional de dados, a LGPD mudará essa realidade, visando garantir a proteção e a transparência no fluxo internacional de dados.

Assim, a transferência internacional de dados pessoais de pessoas localizadas no Brasil passará a ser condicionado a regras que assegurem que os países de destino que possuam o mesmo nível de proteção de dados previstos na LGPD, bem como regras que ressaltem a transparência sobre os acordos internacionais ou regionais que tratem do tema.

De acordo com a LGPD, a transferência internacional de dados pessoais somente poderá ocorrer nas seguintes hipóteses:

1. transferência para países/organizações internacionais que assegurem grau de proteção adequado;
2. comprovação, pelo controlador, de que certas garantias foram atendidas (cláusulas contratuais, normas corporativas globais, selos, certificados, etc);
3. transferências em casos de cooperação internacional entre órgãos públicos de inteligência, investigação ou persecução;
4. quando necessária para a proteção da vida do titular;
5. autorizada pela Autoridade Nacional de Proteção de Dados ("ANPD");
6. em caso de compromisso assumido em acordo internacional;
7. quando necessária para a execução de política pública;
8. quando o titular tiver fornecido o seu consentimento específico; ou
9. quando necessário, para atender cumprimento de obrigação legal ou regulatória pelo controlador, para a execução de contrato ou de procedimentos preliminar relacionados a contrato do qual seja parte o titular, ou para o exercício regular de direitos em processo judicial, administrativo ou de arbitragem.

A LGPD prevê ainda que o tema será regulamentado pela ANPD. Desse modo, caberá à ANPD avaliar quais países ou organizações internacionais apresentam nível de proteção adequado, além de definir como as cláusulas-padrão, normas corporativas globais, selos, código de conduta, e outros padrões relacionados à transferência internacional de dados deverão ser implementados na prática. É certo que a experiência europeia em relação ao tema servirá como diretriz para a regulamentação do tema no Brasil pela ANPD.

Relatório de Impacto à Proteção de Dados

Marcilio Braz Jr.

Uma das principais ferramentas para evidenciar tanto para os cidadãos quanto ao poder público a aderência à lei consiste no *Relatório de Impacto à Proteção de Dados Pessoais* - RIPD.

Para além de uma obrigação, quando observamos pela dimensão de *Gestão de Riscos e Compliance* - GRC, a depender do apetite de risco da organização, um RIPD pode ser uma excelente ferramenta a ser utilizada voluntariamente quando da utilização de uma tecnologia ou atividade de processamento novas.

Ao encarar o RIPD dessa forma, incorpora e demonstra ao público externo um alinhamento da cultura organizacional orientada ao *Privacy by Design/Default.*

Em última análise, a confiança que inspira junto ao mercado como uma organização que efetivamente tem a privacidade e a proteção dos dados pessoais de seus clientes internos e externos como prioridade, olhar RIPD como uma ferramenta auxilia ainda mais no fortalecimento da reputação da empresa.

Por fim, mas não menos importante, um relatório bem conduzido, já nas fases iniciais de um desenho de processo, ajuda a identificar problemas no nascedouro, evitando assim desperdícios futuros de recursos (como dinheiro e tempo).

A definição do relatório de impacto encontra-se no artigo 5º, XVII da lei:

> Art. 5º Para os fins desta Lei, considera-se:
> *XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.*

Por sua vez, o artigo 38 esclarece o âmbito de aplicação do relatório, bem como, de modo extremamente sucinto, os elementos básicos que devem compô-lo:

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

Bases legais para tratamento de dados

Dayana Caroline Costa

Hoje existem 10 (dez) bases legais que podem fundamentar o tratamento de dados pessoais. É importante dizer, desde logo, que não há uma sobreposição hierárquica entre as bases legais estabelecidas pela Lei Geral de Proteção de Dados Pessoais - pelo menos quando o tratamento tiver relação com dados pessoais triviais.

Dentre as bases legais existentes, a mais conhecida e propagada é, de fato, o consentimento. Seja por quê o consentimento já era previsto em outros normativos, como o Marco Civil da Internet, seja porque o consentimento é a base legal em que o titular de dados pessoais tem uma maior interação com a atividade de tratamento de dados.

Porém, nem sempre o consentimento será a base legal mais indicada para estruturar a atividade de tratamento de dados pessoais, pois, para ser válido, o consentimento deverá ser uma "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*".

Portanto, existem certas situações em que a atividade de tratamento de dados pessoais, como por exemplo a coleta de informações pessoais, não poderá se estruturar por meio do consentimento, como é o caso, por exemplo, de uma relação laboral em que o empregador solicita o consentimento do empregado para determinada atividade de tratamento de dados pessoais.

No caso em tela, o empregado pode até vir a consentir por conta da própria relação laboral, mesmo que contra a sua vontade, porém, tal consentimento não será considerado válido, tendo em vista que não será livre e nem inequívoco.

Assim, podemos concluir que em que pese o consentimento ser a base legal mais conhecida, existem outras bases legais que devem ser analisadas ao realizar uma atividade de tratamento de dados pessoais. São elas:

1. **Consentimento**
2. **Obrigação legal ou regulatória**
3. **Execução de Políticas Públicas**
4. **Estudos por órgão de pesquisa**
5. **Execução de contrato ou de procedimentos preliminares relacionados a contrato**
6. **Exercício regular de Direitos em Processo Judicial, Administrativo ou Arbitral**
7. **Proteção da vida ou da incolumidade física**
8. **Tutela da saúde**
9. **Legítimo Interesse**
10. **Proteção do crédito**

❖ GESTÃO DE PROJETO E O PAPEL DE UM PROJECT MANAGEMENT OFFICE (PMO)

Viviane Corrocher Malanga

Um projeto pode ser exemplificado, como a construção de um edifício, a criação de um novo produto (remédios/alimentos), o desenvolvimento de um novo sistema para computadores, etc.

Vários recursos são empregados na construção de um projeto (pessoas, ferramentas, investimentos financeiros, etc). A administração desses recursos e as boas práticas no desenvolvimento de projetos foram reunidas em um guia denominado *Project Management Body of Knowledge* – PMBoK, atualmente na 6. edição.

Esse guia é a principal obra do PMI (*Project Management Institute*), instituto sem fins lucrativos, criado no final da década de 1960, para promover a pesquisa, a sistematização e a divulgação dos conceitos e técnicas da administração de projetos.

O PMBok define o seguinte conceito para projeto:

> *"Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. Os projetos e as operações diferem, principalmente, no fato de que os projetos são temporários e exclusivos, enquanto as operações são contínuas e repetitivas."*

Geralmente as organizações desenvolvem vários projetos ao mesmo tempo e em muitos casos há, por exemplo impacto/dependência do andamento ou término de um projeto para início de outro. Logo o atraso em um projeto pode comprometer o desenvolvimento de outros.

Diante desse cenário, a gestão do portfólio de projetos é uma tarefa importante, e faz parte da relação de boas práticas do PMBoK tendo como recomendação a atuação do PMO.

O PMO (Project Management Office - Escritório de projetos) tem como objetivo definir processos e metodologias de gerenciamento de projetos e orientar os gerentes de projeto sobre a utilização desses.

PMO também é responsável por acompanhar o desenvolvimento dos projetos obtendo status desses junto aos gerentes, realizando alinhamentos e reuniões para apresentar o andamento desses e respectivos KPIS (*Key performance indicators*) para os Executivos e Presidente da organização.

Durante o desenvolvimento de projetos, podem surgir situações que necessitam de alinhamento com a alta direção da organização. Essas situações são apresentadas nas reuniões / comitê de projetos para tomada de decisão.

Um programa de adequação à LGPD contempla desde a implantação e revisão em processos, sistemas, bases de dados, entre outros, o que implica desenvolvimento de projetos.

Podemos citar, como exemplo, os sistemas de uma organização que estão repletos de dados pessoais. Algumas possuem uma única base de dados dos clientes/colaboradores, simplificando o desenvolvimento de projetos para a adaptação desses a LGPD. No caso das empresas que possuem bases de dados múltiplas, serão necessários vários projetos de adaptação e controle.

Além dos projetos que contemplam adaptação das bases de dados, há projetos para adaptar os sites com relação a cookies e outros itens como envio de dados, projetos para restringir o acesso a dados de produção, implantação / manutenção em sistemas de segurança etc.

A atuação do PMO no acompanhamento e reporte desses projetos é fundamental para possibilitar:

- Mitigação de Riscos e Custos dos projetos;
- Desenvolver o projeto no prazo planejado;
- Alocação adequada dos Recursos (técnicos, humanos, etc);
- Performance do processo de adaptação a LGPD mensurável;
- Evitar falhas de comunicação.

O PMO mantém contato com os Gerentes de Projetos para obter informações sobre o andamento desses. Ele recebe, consolida e divulga indicadores sobre o desempenho dos projetos.

Para facilitar a obtenção de informações sobre o andamento dos projetos, geralmente são utilizadas ferramentas onde os Gerentes de Projetos alimentam dados financeiros, cronograma, equipe, escopo possibilitando uma visão em tempo real do andamento desses.

Através dos dados preenchidos e dos parâmetros configurados as ferramentas geram painéis (dashboards) apresentando graficamente a situação de cada projeto e o andamento do portfólio de projetos da organização.

Relacionamos a seguir um exemplo de dashboard de projetos:

Projeto ATENAS
Objetivo: Adequação da organização a LGPD
Status: Vermelho

Identificação	Fase	Nome do Projeto	Status Geral	Financeiro	Equipe	Escopo	Cronograma	Técnico
5800	Concluído	Sistema de Segurança de TI - Upgrade	VERDE	VERDE	VERDE	VERDE	VERDE	VERDE
3309	Em Andamento	Sistema de Portaria - Opção de consentimento/deleção	VERDE	VERDE	VERDE	VERDE	VERDE	VERDE
35	Em Andamento	Base de Dados Vendas - Limitação de Acesso	VERDE	VERDE	VERDE	VERDE	VERDE	VERDE
100	Em Andamento	Cadastro de Fornecedores de Supply Chain	VERDE	VERDE	VERDE	VERDE	VERDE	VERDE
930	Em Andamento	Base de Dados RH	AMARELO	VERDE	AMARELO	AMARELO	VERDE	VERDE
1010	Proposto	Ferramenta de TI	VERMELHO	VERMELHO	VERDE	VERDE	VERDE	VERDE
70	Cancelado	Website						

Fonte: produção da autora.

Observações sobre os status:

=> Projeto 0930 – Base de dados de RH – Status Amarelo:

Algumas planilhas importantes utilizadas pelo departamento foram identificadas na fase de desenvolvimento do projeto, ou seja, não foram relacionadas na fase de levantamento, aumentando o escopo. É necessário alocar novos integrantes na equipe para contemplar essa mudança de escopo.

Pendências: Alocação, com urgência, dos colaboradores, Fulano e Ciclano no projeto.

=> Projeto 1010 – Ferramenta de TI: Embaralhar – Status Vermelho:

O objetivo da aquisição dessa ferramenta é criar bases de dados (a partir de dados de produção) com informações embaralhadas para possibilitar testes de todos os sistemas da empresa mantendo o sigilo dos dados.

Pendência: Liberação de verba para aquisição da ferramenta.

O dashboard é apresentado na reunião / comitê de projetos com executivos para dar ciência do andamento dos projetos e tomada de decisão relacionada às pendências.

Esse material é preparado pelo PMO o qual tem a obrigação de realizar alinhamento com as áreas envolvidas, principalmente aquelas cujos projetos não estão com status verde.

PMO também pode atuar como um conciliador buscando uma solução prévia entre às áreas sobre às pendências, porém em algumas situações é necessário que a decisão seja tomada pela diretoria.

Em resumo: Podemos fazer uma analogia do papel do PMO e Gerentes de Projeto com uma orquestra: Cada músico, que compõe a orquestra, precisa estudar e praticar para que sua participação na música seja perfeita.

Os ensaios e a apresentação da orquestra são liderados pelo maestro, com todos os músicos tocando em harmonia. Os músicos são os Gerentes de Projetos e o maestro o PMO que acompanha e orienta os músicos para possibilitar o sucesso da apresentação /atingimento das metas baseadas em projetos da organização.

❖ TRATAMENTO DE DADOS

Hipóteses de Tratamentos aplicáveis

Fernanda Maia

A LGPD regulamentou todas as hipóteses legais que as empresas poderão tratar dados para fins comerciais. Antes da vigência desta lei as empresas deveriam seguir as diretrizes contidas em leis esparsas, como por exemplo, a Lei do Sigilo Bancário, Marco Civil da Internet, Código de Defesa do Consumidor.

Logo após a vigência da lei (16 de agosto de 2020) as empresas precisarão enquadrar o tratamento dos dados pessoais, que deverão ser analisadas, com base na atividade de tratamento de cada fluxo de dados, e encontrar a base legal adequada, entre as 10 bases que o texto legal possui, para justificar a finalidade do tratamento.

Por fim, as empresas precisarão distinguir as finalidades do tratamento, separando os dados que coletam e tratam, visto que, a lei carrega duas categorias diferentes de tratamento, uma para os dados pessoais e outra para os dados pessoais sensíveis. Dito isso, as 10 bases legais para o tratamento dos dados pessoais são:

1. Consentimento do Titular: consentimento tem que ser livre (o Titular tem que ter completa liberdade), informado (o Titular tem que saber para qual finalidade de Tratamento ele está consentindo), inequívoco (não pode haver dúvidas que o Titular quis dar o consentimento);
2. Cumprir uma obrigação legal ou regulatória;
3. Execução de um contrato com o titular;

4. A administração pública irá tratar os dados ou compartilhar para executar uma política pública para compartilhar dados pessoais com entes privados a Administração Pública deverá observar os seguintes requisitos:

    - Ter a necessidade de transferir os dados para execução descentralizada de atividade pública;
    - Ter a indicação de um Encarregado;
    - Houver previsão legal ou contrato, convênios;
    - Para prevenção a fraudes e irregularidades ou proteger a segurança do Titular; ou
    - Os dados foram publicizados (observados os limites das leis que regulam estes dados, Ex.; Lei de Acesso à Informação).

5. Órgãos de pesquisa irão tratar os dados para realização de pesquisas;
6. A empresa precisa dos dados para se defender em processos, judiciais, administrativos ou arbitrais;
7. Se o tratamento é necessário para proteger a vida ou segurança física do Titular ou terceiro;
8. Por profissionais da área de saúde, serviços de saúde ou entidades sanitárias, para a proteção da saúde das pessoas (médicos, enfermeiros), serviços de saúde (hospitais, centros de atendimento) ou entidades sanitárias (serviços de vigilância sanitária);
9. Para atender os legítimos interesses do controlador ou terceiros. Essa base se distingue das outras bases legais por não precisar de um motivo particular para sua aplicação (i.e. cumprimento de cláusula contratual); não pode ter outra base mais adequada para a atividade do tratamento; e o interesse legítimo pode ser tanto da empresa controladora dos dados, quanto de terceiros (um terceiro particular ou até mesmo a sociedade como um todo); ou
10. Para proteção do crédito. Como essa base é completamente nova no cenário legislativo global, ainda não se sabe ao certo qual a amplitude do conceito de Proteção do Crédito, contudo é correto afirmar que tratamentos realizado para fins de garantir que uma operação de crédito seja executada de forma legítima, segura, e cujos riscos da operação foram analisados poderá ser baseado nesta hipótese.

Observando os Dados Pessoais Sensíveis a lei, em seu artigo 11, elenca as bases aptas a atuar no tratamento dos dados sensíveis, que são:

1. Consentimento, que além de ter que observar todos os requisitos do consentimento para Tratamento de Dados Pessoais não sensíveis (Livre, informado e inequívoco) deverá ser também específico;
2. Cumprir uma obrigação legal ou regulatória, que além de utilizar a mesma lógica da hipótese de tratamento de dados pessoais existe a garantia de que o tratamento é indispensável para cumprir a obrigação legal ou regulatória;
3. A administração pública irá tratar os dados para executar uma política pública, que deverá ter a garantia que o tratamento é indispensável, ou seja, não tem jeito de executar uma política pública sem o tratamento do dado pessoal sensível;
4. Órgãos de pesquisa irão tratar os dados para realização de pesquisas; que deverá ter a garantia que o tratamento é indispensável, ou seja, não tem jeito de executar a pesquisa sem o tratamento do dado pessoal sensível;
5. A empresa precisa dos dados para se defender em processos, judiciais, administrativos ou arbitrais, que deverá ter a garantia que o tratamento é indispensável para a defesa;
6. Se o tratamento é necessário para proteger a vida ou segurança física do Titular ou terceiro, que deverá ter a garantia que o tratamento é indispensável para cumprir com a finalidade;
7. Por profissionais da área de saúde ou entidades sanitárias, para a proteção da saúde das pessoas, que deverá ter a garantia que o tratamento indispensável, ou seja, não tem jeito de proteger a saúde sem o Tratamento do dado pessoal sensível; e
8. Para a garantia da prevenção à fraude e à segurança do titular nos processos de validação cadastral, que deverá ser indispensável o tratamento de dados pessoais sensíveis para prevenção a fraude ou a segurança do titular na identificação ou autenticação de cadastros.

Funcionamento das hipóteses na prática

Raphael Dutra Campos

Antes de adentrarmos no funcionamento prático das hipóteses legais de tratamento de dados pessoais é importante reiterar que, independente da base legal escolhida, os princípios norteadores das atividades de tratamento deverão sempre ser observados.

Portanto, além de buscar assertividade no momento em que identificar a base legal mais adequada para um referido tratamento de dados pessoais, é imprescindível observar princípios como da finalidade, necessidade, adequação, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Como já visto, a Lei Geral de Proteção de Dados Pessoais nos trouxe um arcabouço de bases legais muito amplo para as atividades de tratamento de dados. Portanto, não há uma sobreposição hierárquica entre bases legais. A escolha de uma base legal dependerá, essencialmente, do contexto das atividades que são desenvolvidas pela organização.

Assim, diante de tantas hipóteses, devemos interpretar - caso a caso - aquela que mais se encaixa na nossa atividade.

(i) Consentimento: O consentimento se alinha à autodeterminação informacional do indivíduo, pois exige do titular uma participação ativa e, consequentemente, um maior controle sobre o fluxo de suas informações pessoais. Assim, com mais controle sobre suas informações, o consentimento tem algumas características que lhes são peculiares e para ser considerado válido, o consentimento deverá ser livre, informado, inequívoco e para uma determinada finalidade. Portanto, a adjetivação do conceito de consentimento retrata uma desaceleração no seu protagonismo, apesar do titular de informações pessoais continuar sendo o ponto focal das atividades de

tratamento de dados pessoais. Portanto, as atividades de tratamento de dados pessoais que decorrem do consentimento deverão - sempre - se referir à uma determinada finalidade.

(ii) Obrigação legal ou regulatória: a Lei Geral de Proteção de Dados Pessoais percebeu, assim como ocorreu com o desenvolvimento do tema na comunidade europeia, que existem situações em que o tratamento de dados pessoais ocorrerá por conta de alguma obrigação perante o ordenamento jurídico ou, até, perante o próprio regulador de determinado segmento econômico. Logo, o direito dos titulares de dados pessoais não será ilimitado, pois, caso haja alguma outra base legal para estruturar o tratamento de dados pessoais, tal atividade poderá continuar a ser desenvolvida. É o que ocorre, por exemplo, no caso de armazenamento de registros de conexão e de registros de acesso a aplicações de internet.

A Lei 12.965, conhecida como Marco Civil da Internet, estabelece o dever de guarda de registros de conexão pelo prazo de 1 (um) ano e, para os registros de acesso a aplicações de internet o prazo é de 6 (seis) meses. Tal obrigação decorre da lei e, portanto, a atividade de tratamento de tais registros, que se refere ao armazenamento de tais informações, será consubstanciada por meio da base legal "obrigação legal ou regulatória".

(iii) Execução de Política Pública: à Administração Pública foi concedida uma base legal específica para as suas atividades de tratamento e, além disso, a Lei Geral de Proteção de Dados Pessoais trouxe um capítulo inteiro para tratar do tema. Portanto, a grande questão no desenvolvimento de políticas públicas estruturadas em dados pessoais é equilibrar a relação entre Poder Público e cidadãos.

Como vimos anteriormente, não caberia instrumentalizar as atividades estatais por meio do consentimento dos cidadãos, pois, há uma assimetria que não

garante ao consentimento as características fundamentais que perseguem a sua validade. Logo, o tratamento de dados pessoais pelo Poder Público deve se orientar por meio dos princípios gerais de proteção de dados pessoais, como a finalidade, adequação, transparência e livre acesso, estabelecidos pela própria Lei Geral de Proteção de Dados Pessoais e, além disso, buscar equacioná-los com os princípios norteadores da própria administração pública - estabelecidos pelo artigo 37 da Constituição Federal. que visem reequilibrar a relação que se desenvolve entre o Estado e os indivíduos. Portanto, a ratificação de políticas públicas deve sempre buscar diminuir a assimetria que há entre o Estado e os cidadãos.

(iv) Estudos por órgão de pesquisa: é extremamente importante perceber, neste caso específico, o conceito de órgão de pesquisa, estabelecido pela própria Lei Geral de Proteção de Dados Pessoais, em seu artigo 5, XVIII: "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico". Além disso, o tratamento de informações pessoais por órgãos de pesquisa deverá sempre buscar a anonimização dos dados ou a pseudonimização, isto é, o meio pelo qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

(v) Execução de um contrato ou procedimentos preliminares: o caso aqui é bastante peculiar, pois, as atividades de tratamento de dados pessoais que podem se estruturar na referida base legal em comento, apenas poderão fazê-lo caso (i) o tratamento seja estritamente necessário para a execução do contrato do qual o titular é parte ou (ii) quando o tratamento for necessário no contexto contratual. Isto ocorre, por exemplo, em atividades de tratamento de dados

pessoais que decorrem de um contrato de prestação de serviço de transporte aéreo.

(vi) Exercício regular de direitos em processo judicial, administrativo ou arbitral: essa base legal é extremamente ampla e autoriza o tratamento de dados pessoais em processos de qualquer tipo, isto é, processos judiciais, administrativos ou arbitrais. Portanto, dados pessoais que constam em bases de dados relacionadas aos processos devem sempre respeitar as finalidades pelas quais foram disponibilizadas.

(vii e viii) Proteção da vida ou da incolumidade física e para tutela da saúde: inevitavelmente, ao nos referirmos à proteção da vida, da incolumidade física e à tutela da saúde, devemos lembrar do conceito de dados pessoais sensíveis. Portanto, quando estivermos analisando dados pessoais sensíveis, é importante destacar que nestes casos, há uma regra clara emanada pela Lei Geral de Proteção de Dados Pessoais. Tal regra traz o dever que, em relação ao tratamento de dados pessoais sensíveis, o consentimento é a regra e, portanto, o agente de tratamento deverá sempre buscar o consentimento antes de estruturar a sua atividade em outra base legal. Entretanto, quando estivermos nos referindo aos dados pessoais triviais, o legislador entendeu por bem não estabelecer tal regra e, portanto, caberá ao agente compreender qual é a melhor base legal para estruturar as suas atividades de tratamento de dados pessoais. Logo, a base legal em análise demanda uma compreensão do contexto de atividades que serão desenvolvidas e, além disso, caso não se utilize o consentimento, é importante ressaltar a obrigatoriedade em observar os princípios gerais e as garantias e direitos do titular.

(ix) Legítimo Interesse: o legítimo interesse é a base legal mais flexível e, portanto, pode ser utilizada como válvula de escape para o tratamento de informação pessoal. Logicamente que, tal tratamento deve ser precedido de um teste de proporcionalidade em que se valida a utilização ou não da referida base

legal. A referida base legal é fundamental diante do grande avanço tecnológico que estamos presenciando, pois, diante dessa nova economia digital, estruturada em dados, o legítimo interesse é - sem dúvida - a nova carta coringa para as atividades de tratamento de dados pessoais. O referido teste de proporcionalidade tem quatro passos e deverá avaliar (a) a legitimidade do interesse, isto é, verificar se a finalidade pela qual se busca o tratamento é, efetivamente, legítima e, além disso, se a situação é concreta, (b) a necessidade do referido tratamento, ou seja, se o tratamento estará sendo realizado de forma menos intrusiva possível, em conformidade com o princípio da minimização e, ainda, se existem outras bases legais que podem estruturar tal tratamento de forma menos onerosa, (c) o balanceamento entre o tratamento que se pretende realizar e a legítima expectativa do titular, assim como a não infringência de direitos e liberdades fundamentais e, por fim, (d) estabelecer salvaguardas e garantias que assegurem ao titular: transparência, mecanismos de oposição e mitigação de riscos.

(x) Proteção do crédito: a proteção do crédito como base legal para tratamento de dados pessoais criou um microssistema de proteção de dados pessoais em que, para esses casos, há o convívio pleno e integrado entre diversas normas consumeristas, por exemplo, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e a própria Lei Geral de Proteção de Dados Pessoais. Portanto, a referida base legal estrutura efetivamente um sistema em que se busca a prevenção à fraude e a proteção do crédito. É importante ressaltar que o tratamento de dados com base em outras bases legais, que não o consentimento, deverá sempre observar os princípios de proteção de dados pessoais e os direitos do titular.

Compartilhamento de Dados entre as organizações do mesmo grupo

Mariana de Souza Cruz Caparelli

O compartilhamento de dados pessoais entre empresas do mesmo grupo econômico, desde que as empresas estejam situadas no território nacional, deve, assim como qualquer outro tipo de tratamento realizado, observar os princípios indicados no artigo 6 da LGPD e possuir uma base legal que ampare o compartilhamento pretendido.

Nesse sentido, tratando-se de troca de dados dentro de um mesmo grupo econômico, importante verificar se o tal troca de dados ocorre entre controlador e operador, ou se a relação entre as partes é de controlador para controlador.

No caso de referida troca de dados ocorrer em um contexto de controlador para operador, considerando que o operador é aquele que realiza o tratamento de dados pessoais em nome do controlador, importante que fique clara a finalidade do tratamento a ser realizado e as formas de exercício dos direitos do titular. Por outro lado, em uma relação de compartilhamento de dados entre empresas do mesmo grupo, em uma situação na qual ambas figuram como controlador, ou seja, no caso de todas as empresas envolvidas serem responsáveis pela tomada de decisão referente ao tratamento de dados pessoais, importante que fiquem claros os limites e obrigações de cada uma das empresas envolvidas.

O cenário muda quando tal troca de dados ocorre entre empresas do mesmo grupo, mas que estão localizadas em países diferentes, pois, nesses casos, configura-se a transferência internacional de dados, que deve observar o disposto nos artigos 33 e seguintes da LGPD.

A LGPD prevê que a transferência internacional de dados somente é permitida nos seguintes casos:

(i) Transferência para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na própria LGPD: Quando a LGPD faz referência ao nível de proteção que será considerado adequado, a própria lei já traz como parâmetro que será levado em consideração (i) as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; (ii) a natureza dos dados; (iii) a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD; (iv) a adoção de medidas de segurança previstas em regulamento; (v) a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e (vi) outras circunstâncias específicas relativas à transferência de dados;

(ii) Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD: Seja na forma de cláusulas contratuais específicas, cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta regularmente emitidos;

(iii) Cooperação jurídica internacional: Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

(iv) Proteção da vida ou da incolumidade física: Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

(v) ANPD: Quando a Autoridade Nacional de Proteção de Dados autorizar a transferência;

(vi) Acordo de cooperação internacional: Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

(vii) Política pública ou atribuição legal do serviço público: Quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 da própria LGPD;

(viii) Consentimento específico: Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente está de outras finalidades; ou quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD;

A ideia de regular o fluxo internacional de dados pessoais foi justamente resguardar os direitos dos titulares, com transparência em relação a acordos internacionais e incentivando a adoção de padrões contratuais com reconhecimento na esfera internacional.

Ainda está pendente de regulamentação pela ANPD a definição sobre o conteúdo de cláusulas padrão que deverão ser aptas a garantir a segurança necessária, bem como o cumprimento dos princípios da LGPD e direitos do titular. Além disso, depende também de uma definição da ANPD a regulamentação das normas corporativas globais ou selos, certificados e códigos de conduta.

As hipóteses e os requerimentos para transferência internacional previstas na nossa legislação são similares ao disposto no GDPR, no entanto, o GDPR permite transferência internacional de dados pessoais com base no legítimo interesse do

controlador, desde que a transferência não seja repetitiva, seja apenas com relação a um número limitado de titulares e sejam fornecidas as garantias adequadas e medidas de segurança.

Nesse sentido, o GDPR traz em seu considerando número 48 a seguinte explicação:

> "*Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected*".

A LGPD, embora fortemente inspirada no GDPR, destoou do Regulamento Europeu com relação a este ponto, inexistindo o fundamento do legítimo interesse para transferência internacional de dados pessoais, mesmo que entre empresas do mesmo grupo econômico.

❖ SEGURANÇA

Angela Maria Rosso & Paulo Rogério Dias de Oliveira

Elaboração de Política de Segurança de Informação

A Lei Geral de Proteção de Dados prevê que as empresas adotem boas práticas de segurança da informação e de governança dos dados como fator determinante.

É fato que segurança da informação e proteção de dados não se confundem, são coisas distintas, mas também é verdade que não há como falar em proteção de dados sem falar de segurança da informação, não é ousadia afirmar que a primeira não existe sem a segunda.

Primeiramente é preciso compreender que informação é o que se obtém ao colocar um dado em um contexto em que ele ganha significado. Assim, informação é tudo aquilo que tem valor para a organização e que tem um ciclo de vida que vai desde a sua produção até o descarte. Pode-se afirmar que na economia atual a informação é o ativo de maior valor dentro de uma organização e que por isso ela merece ser protegida é nesse ponto que entra a Segurança da Informação como suporte de proteção.

Pode-se então dizer que Segurança da Informação é o fornecimento de proteção aos dados e às informações de forma a garantir que:

- não sejam acessadas por quem não é autorizado para isso (confidencialidade);
- que quando acessada ela esteja íntegra e represente a verdade conforme foi produzida (integridade); e
- que esteja acessível sempre que alguém autorizado dela necessitar (disponibilidade).

A Segurança da Informação, fundamental ao contexto das leis de proteção de dados, é, portanto, além da implantação de conceitos técnicos que transitam pela aquisição de equipamentos e de sistemas, antes de tudo uma mudança cultural que necessita ser fomentada dentro da organização. Assim, para que se chegue a um ambiente seguro é preciso considerar sempre a tríade pessoas, processos e tecnologias. São as pessoas o fator mais importante e o engajamento delas é fundamental para que se consiga incorporar uma cultura de SI na organização.

Diante disso, em face da necessidade de diretrizes que orientem como entender e tratar a segurança da informação dentro das organizações, é que surge a Política de Segurança da Informação (PSI). A PSI encontra previsão em diversos frameworks mundialmente relevantes, como por exemplo PCI-DSS e a ISO/IEC 27001. No caso da ISO 27001, cuja última versão data de 2013, trata-se de uma norma que estabelece as melhores práticas para estabelecimento de um Sistema de Gestão de Segurança da Informação. Tal documento estabelece que a PSI é

uma declaração sobre como a alta administração da organização espera que seja tratada a Segurança da Informação dentro do seu ambiente, ou seja, a PSI não vai garantir que o dado esteja seguro, ela não é um controle, este documento estabelece diretrizes de como quem gerencia o negócio espera que deve ser tratada a Segurança da Informação dentro da organização.

Em virtude disso é fundamental que cada organização desenvolva a sua própria política, considerando suas características e as regulamentações a que se submete, uma vez que o objetivo da PSI é prover orientação de como deve ser tratada a segurança da informação. PSI genérica não é PSI, porque o modelo que atende plenamente uma empresa pode não atender a outra.

De acordo com a ISO 27001:2013, é a administração que deve providenciar uma PSI adequada ao propósito da organização, garantindo, assim, o comprometimento da direção com a aplicação dos requisitos da segurança da informação e com a melhoria contínua do Sistema de Gerenciamento da Segurança da Informação existente na organização.
De acordo com a ISO/IEC 27001:2013 a PSI deve:

- Ser um documento disponível;
- Ser divulgado dentro da organização;
- Estar acessível para todas as partes interessadas, quando apropriado.

De forma prática a PSI não é um documento único, ela é na verdade uma norma principal composta por tantas normas acessórias específicas quantas forem necessárias para cobrir todas as áreas em que a organização necessitar garantir a segurança da informação. Também não há um formato que seja padrão. Assim, o documento principal da PSI deve contemplar minimamente as diretrizes gerais, os objetivos, requisitos, os princípios, as definições dos termos usados e as sanções em caso de violação das normas estabelecidas nas normas auxiliares.

Abaixo segue uma sugestão de documentos que devem compor a PSI, contudo, a depender das características da organização, tais documentos podem variar e por isso a importância de no desenvolvimento da política, considerar o cenário real da organização.

A melhor PSI, é aquela construída pela própria organização de forma que mais se adeque às suas necessidades do negócio em relação à Segurança da Informação.

- **Acesso Físico e Lógico** - tem o objetivo de normatizar como acontecerá o acesso físico às instalações da organização bem como de estabelecer a política de controle de acesso ao ambiente computacional (quais as pessoas que estão autorizadas a acessar e como será o procedimento para liberação e remoção de acesso);

- **Acesso Remoto** - cada dia mais importante devido às possibilidades de teletrabalho ou home office. A norma deve prever como acontecerá a liberação de acesso externo ao ambiente computacional da organização, estabelecendo critérios e regras de acesso com o principal objetivo de evitar acessos sem controle e não autorizados;

- **Classificação e Tratamento da Informação** - objetiva determinar como se dará a classificação da informação observando critérios de confidencialidade, por exemplo. Esta diretriz deverá receber uma atenção especial, pois poderá ser aqui onde constará os níveis de classificação da informação a luz da Lei Geral de Proteção de Dados;

- **Tratamento de Dados Pessoais** – Neste documento deverá constar orientações sobre o que são dados pessoais e sensíveis e a devida forma de coleta, armazenamento, processamento e exclusão destas

informações. Também deverá constar quem é o DPO e suas atribuições além de explicar o fluxo de vida dos dados dentro da organização;

- **Liberação de Acesso e Senhas** - têm o objetivo de estabelecer quais os critérios de liberação de acesso aos sistemas e como serão definidas/constituídas as senhas;

- **Correio eletrônico e comunicadores instantâneos (mensageiros)** - regular o modo de utilização do e-mail corporativo e dos mensageiros instantâneos;

- **Tratamento e resposta à incidentes de Segurança da Informação** - como será o processo de contingenciamento em caso de um incidente de Si, quem são os responsáveis por responder aos incidentes e como devem atuar os empregados e demais colaboradores diante de um incidente de SI;

- **Recursos computacionais - uso aceitável** - estabelecer como se dará a utilização dos recursos computacionais dentro da organização, a quais recursos cada usuário terá acesso, o que é permitido e o que é proibido na utilização desses recursos;

- **Utilização da Internet e da Intranet e comportamento nas redes sociais** - determinar o que é aceito e o que é proibido na utilização da Internet e da Intranet dentro da organização;

- **BYOD - Equipamentos pessoais no ambiente corporativo** - determinar como ocorrerá o acesso de equipamentos pessoais ao ambiente corporativo;

- **Proteção contra códigos maliciosos** - estabelecer diretrizes acerca das medidas a serem adotadas para coibir ameaças e códigos maliciosos de qualquer natureza;

- **Políticas de backup** - determinar como acontecerão os procedimentos de backup com o objetivo de proteger as informações armazenadas em meio digital;

- **Monitoramento de ativos e serviços da informação** - normatizar como se dará o acompanhamento do cumprimento das determinações contidas na PSI e seus anexos;

Deve-se ainda salientar que a PSI não se refere somente às informações armazenadas ou produzidas em meio digital, ela envolve também as informações existentes em meios físicos e deve se preocupar com o ambiente físico em que elas estão armazenadas.

Importante destacar que a adoção da PSI como uma norma de cumprimento obrigatório deve ser tratada como tal, no sentido de que aquele que descumpri-la deve submeter-se às sanções nela previstas. A abordagem precisa ser firme nesse sentido, desvios de conduta das pessoas que têm acesso às informações da organização não devem ser tolerados sob pena de enfraquecimento e posterior esquecimento dos regramentos nela contidos.

Desta forma ressalta-se a importância da divulgação da PSI para todos os colaboradores, terceiros e fornecedores, de maneira clara e objetiva, preferencialmente em forma de treinamento que envolva a parte teórica - explicando o conteúdo do documento - concluindo com uma avaliação, que pode ser no formato de teste ou de estudo de caso, que valide o entendimento do indivíduo sobre o assunto.

Por fim, ressalte-se que a PSI não é um documento definitivo, ele deve ser revisto periodicamente ou a qualquer momento em que ocorra modificação significativa na infraestrutura e/ou no negócio da organização. A revisão se faz necessária para que sempre reflita da melhor forma possível a realidade informacional da organização.

Proteger as informações da organização implica em proteger os dados pessoais tratados em seu âmbito e faz parte do processo de conformidade da organização com a Lei Geral de Proteção de Dados Pessoais.

❖ JURÍDICO

Gustavo C. Godinho

Com a nova Legislação, tão importante quanto mapear os dados e garantir os novos direitos dos titulares, passou a ser documentar corretamente e da forma mais precisa possível as relações jurídicas entre empresas e agentes envolvidos no tratamento de dados pessoais.

Agora, o Controlador continuará responsável pelos incidentes e desvios ocorridos em qualquer elo da sua cadeia de custódia. As informações e dados pessoais confiados por um Titular ao Controlador continuarão a ser responsabilidade jurídica deste, mesmo que o tratamento seja terceirizado para um Operador.

Isto significa que a relação jurídica entre os Agentes de Tratamento deverão ser precisas, para que um Operador não faça nem mais, nem menos do que o necessário com os dados recebidos.

Por sua vez, caberá ao Controlador a verificação dos requisitos e hipóteses de tratamento, bem como a verificação prévia de que dados precisarão de consentimento ou sob que forma serão tratados.

Em um caso de incidente ou questionamento pela ANPD, as evidências da contratação deverão ser apresentadas em prazo razoável para apuração das responsabilidades.

Desta forma, sugere-se que a relação jurídica entre o Controlador e Operador preveja, minimamente:

- As partes do Contrato e qual a função de cada uma delas na relação jurídica.
- Identificar o titular dos dados, bem como a quem pertencerá o resultado econômico dos produtos desenvolvidos.
- Quais são os requisitos de segurança e políticas que deverão ser seguidas para acesso, monitoramento, inclusão, modificação ou exclusão de dados, seja a pedido do Controlador ou do Titular.
- Direito de acesso às informações, possibilidade de auditoria e realização de testes de segurança.
- Prazo de guarda dos dados e hipóteses de rescisão.
- Possibilidade ou não de acesso aos dados pelas Autoridades ou Titulares

Dependendo do caso, pode-se aproveitar o Contrato para discutir cláusulas mais complexas, como:

- Service Level Agreements (SLAs), forma de comunicação e prazos de respostas em caso de incidentes envolvendo dados pessoais.
- Limitação de responsabilidade contratual ou a solidariedade em caso das sanções previstas em Lei;
- Contratação de Seguro Ciber e outras.

❖ ACESSIBILIDADE E DIREITOS DOS TITULARES

Fernanda Maia & Ana Caroline da Silva

Antes da promulgação da LGPD, o Brasil já possuía uma série de regulações setoriais que garantiam aos titulares de dados uma série de garantias, dentre os quais é possível citar a própria Constituição Federativa da República de 1988, o Marco Civil da Internet, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, Lei do Cadastro Positivo[1].

É certo que as regulações setoriais mencionadas não dispunham de forma organizada, ampla e detalhada de todos os direitos e obrigações envolvendo o tratamento de dados pessoais, de modo que somente com a LGPD, o Brasil passou a ter de fato um sistema de proteção de dados pessoais cujas regras relativas à coleta e tratamento de dados pessoais, direitos e obrigações dos titulares, e sanções por descumprimento de prerrogativas fundamentais são claras.

Todavia, um olhar atento aos diplomas legais anteriores à LGPD demonstra que os direitos dos titulares, previstos no Capítulo III de tal lei, já estavam presentes na legislação brasileira, dentre os quais, destaca-se o direito do titular saber quais dados seus estão sendo coletados e como estes serão usados, o chamado "*Direito à Informação*".

Nesse sentido, a Lei nº 8.078/90, chamada de 'Código de Defesa do Consumidor' ou 'CDC', regulação aplicável às relações de consumo que estabelece, como princípios fundamentais de tais relações, a transparência e a boa-fé como norte, determina, em seu artigo 43, o consumidor tem direito de ter acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

[1] Lei nº 12.965 de 2014, Lei nº 8.078 de 1990, Lei nº 12.527 de 2011 e Lei nº 12.414 de 2011, respectivamente.

Ainda nesse sentido, a Lei nº 12.414/2011 ou 'Lei do Cadastro Positivo', que "*disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito*" dispõe em seu artigo 5º que é direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais.

Dito isto tem-se que o "Direito à Informação" pode ser definido como o direito que um titular de dados pessoais possui de receber informações claras e adequadas a respeito do tratamento e compartilhamento de seus dados pessoais por pessoas jurídicas públicas ou privadas.

Desse modo, sob a ótica da LGPD, tal direito é classificado como direito à confirmação dos tratamentos dos dados pessoais. O artigo 18 da referida lei abrange todos os direitos que os titulares possuem, o que os garantem maior poder e controle acerca de suas próprias informações pessoais.

Assim, o Titular poderá solicitar (para qualquer entidade, pública ou privado):

1. quais são os dados pessoais, a seu respeito, que possuem (direito a acesso);
2. a correção e/ou atualização de tais informações (direito à correção);
3. a anonimização de seus dados (direito a anonimização);
4. a portabilidade de tais informações para qualquer outra entidade, de maneira estruturada (direito a portabilidade);
5. a eliminação de seus dados (direito a eliminação);
6. informação de que as entidades públicas e privadas que a empresa realizou compartilhamento dos dados;
7. as consequências em relação a possível negativa de consentimento por parte do Titular; e
8. revogar o consentimento fornecido anteriormente. Além de poder se opor ao tratamento realizado pela empresa e peticionar para a ANPD contra o tratamento de seus dados realizado pela empresa.

O importante para as empresas terem em mente é que a partir de 16 de agosto de 2020 elas terão que possuir mecanismos para cumprir com todas as solicitações supracitadas.

Dessa forma, conforme adotado pela Europa, as empresas terão que ter canais de comunicação direto com os titulares para cumprir com as solicitações, seja criando um canal apartado ou adaptando o canal de ouvidoria, a comunicação é só o primeiro passo para a implementação, visto que, a empresa terá que possuir mecanismos para, por exemplo, entregar, de forma legível para o Titular, a lista de seus dados; controlar todos os fluxos de dados baseados em consentimento para identificá-los e interrompê-los no caso de revogação; e/ou ter mecanismos para deletar os dados quando solicitados, entre cumprir com os demais direitos.

❖ GESTÃO DE INCIDENTES, CASOS DE QUEBRA DE SIGILO E VAZAMENTOS

Núria Baxauli

De acordo com o artigo 48 da Lei nº 13.709/18 ("Lei Geral de Proteção de Dados" ou "LGPD"), é obrigação do controlador comunicar a autoridade nacional e ao titular qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

O conceito de incidente não está definido pela LGPD, entretanto, podemos entender como incidente qualquer ocorrência acidental ou ilícita relacionada a segurança dos dados, incluindo o acesso indevido e a perda ou apagamento sem intenção dos dados. Neste sentido, podemos utilizar também como parâmetro o conceito de "violação de dados pessoais" do Regulamento Europeu nº 679/2016 ("*General Data Protection Regulation*" ou "GDPR") que consiste em evento acidental ou ilícito, que ocasione a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

A LGPD também determina que a comunicação de incidentes deverá ser realizada em prazo razoável, a ser determinado pela autoridade nacional, e a qual deve conter o seguinte conteúdo, minimamente:

a) a natureza dos dados afetados;
b) informações sobre os titulares envolvidos;
c) indicação das medidas de segurança adotadas para proteger os dados, resguardados os segredos comerciais e industriais;
d) os riscos relacionados ao incidente;
e) os motivos da demora, caso a comunicação não tenha sido imediata; e
f) as medidas que serão adotadas para reverter ou mitigar os riscos ou danos causados.

A depender da gravidade do incidente e caso seja necessário para proteger os titulares, a autoridade nacional poderá determinar medidas para reverter os prejuízos e/ou a ampla divulgação do incidente em meios de comunicação. A LGPD também determina critérios para avaliação da gravidade do incidente, dentre eles, o principal é a adequação das medidas técnicas adotadas para que os dados sejam ininteligíveis para acesso por terceiros não autorizados, a exemplo de medidas de encriptação, quando for adequado.

Adicionalmente, o artigo 50 menciona que um programa de governança em privacidade deve contar, no mínimo, com um plano de resposta a incidentes.

Diante deste panorama legal é possível concluir que três principais tópicos estão relacionados a uma abordagem correta de incidentes de segurança: (i) a elaboração prévia de um plano de resposta a incidentes; (ii) a devida comunicação à autoridade nacional e titulares; e (iii) aplicação de medidas que mitiguem ou neutralizem os riscos ou danos causados.

I – Plano de Resposta a Incidentes

Na maioria dos casos envolvendo incidentes de segurança de dados, os primeiros a descobrirem uma irregularidade são funcionários de baixo escalão sem poder decisório dentro de uma organização. Ocorre que, além de muitas vezes estes funcionários não possuírem uma visão global do negócio e entenderem os possíveis riscos do incidente, é possível que eles decidam não comunicar o incidente aos seus superiores por não entenderem a importância da questão e até por receio de serem considerados responsáveis pelo ocorrido. Já nos casos em que o funcionário resolve informar aos superiores, é comum que o fluxo da comunicação sobre o incidente ocorra de forma desorganizada e ineficiente, prejudicando a possibilidade de mitigar os riscos do incidente, caso não haja um plano de resposta a incidentes bem definido.

Portanto, um requisito básico de um plano de resposta efetivo é a obrigatoriedade pelos funcionários de comunicar qualquer irregularidade operacional relacionada a proteção de dados, bem como previsão de penalidades para qualquer um que omitir uma informação relacionada a um incidente. Em seguida, será necessário estabelecer um fluxo de comunicações que leve de forma mais rápida possível a informação sobre o vazamento a um superior com poder decisório dentro da respectiva organização, o qual possa, finalmente, levar o assunto a um comitê multidisciplinar pré-selecionado para situações de incidentes.

Tal plano de resposta a incidentes deve englobar os prestadores de serviços que sejam considerados processadores de dados, principalmente diante da responsabilidade solidária entre controlar e processador de dados.

Mesmo com um plano definido, diversas variações podem ocorrer em cada caso e por isso, o comitê disciplinar para lidar com o caso se mostra relevante. Em diversos casos em que hackers invadem os sistemas da empresa, é comum que seja pago o valor de “resgate” exigido para que os mesmos devolvam a base de

dados da empresa e após o incidente, os mesmos dados serem encontrados a venda na *deep web*. Assim, será necessário avaliar a conveniência desse pagamento, por exemplo, em casos em que há cópia da base de dados em servidores não afetados que possibilitam a operação normal da empresa, e portanto, diante da falta de garantia sobre o que será feito com os dados pelos criminosos após o pagamento de um resgate de valor alto, pode ser ainda mais vantajoso para empresa não efetuar o pagamento exigido e investir esse valor em medidas de segurança diversas.

II – Comunicação à Autoridade e Titulares

Embora a Autoridade Nacional de Proteção de Dados no Brasil ainda esteja em fase inicial, e portanto, não sabemos como a mesma vai atuar, se fala muito sobre as vantagens de sua atuação ser direcionada a educação da sociedade, auxílio na minimização dos riscos causados por incidentes e direcionamento da organização sobre as melhores medidas de proteção a serem adotadas, e não apenas ter uma atuação sancionadora.

Portanto, além do conteúdo mínimo exigido pela lei, é recomendável que a empresa compartilhe o maior número de informações possíveis disponíveis sobre o incidente com a autoridade responsável na ocasião da comunicação para que a partir de uma análise conjunta, controlador de dados pessoais e autoridade concluam sobre as melhores medidas a serem adotadas para mitigar ou neutralizar os riscos causados pelo incidente. Outro documento que pode ajudar a Autoridade Nacional a analisar a situação é o registro das operações de tratamento de dados e medidas adotadas para a proteção dos mesmos, o que demonstra a importância da atualização periódica dessa documentação pela organização.

Já a comunicação sobre o incidente aos titulares deve ser muito bem redigida para informar os envolvidos de forma adequada e alinhada com a estratégia definida pela empresa para tanto. Portanto, é prudente contar com um trabalho

conjunto de diversas áreas da empresa, como o jurídico, que conhece o conteúdo mínimo exigido por lei para uma comunicação desse tipo; o time de tecnologia da informação, que analisa os detalhes técnicos do incidente; e a equipe de comunicação e marketing, que pode elaborar a melhor estratégia de comunicação ao cliente sobre o ocorrido.

III – Aplicação de Medidas Mitigadoras

Uma medida prévia que mitiga riscos causados pelo vazamento de dados é a encriptação de dados pessoais. Isto porque, dados vazados que estejam encriptados não podem ser facilmente traduzidos por indivíduos que não tem acesso a respectiva chave de desencriptação. Entretanto, apesar de ferramentas de encriptação serem facilmente encontradas no mercado, a maioria das empresas ainda não implementa essa medida de segurança.

Posteriormente ao incidente, se recomenda a análise de medidas como:

(i) a negociação com hackers criminosos e a conveniência do pagamento de valor de "resgate" aos mesmos;

(ii) a própria comunicação correta a autoridade e clientes, ou até comunicação pública, que alerte sobre a possibilidade de os dados envolvidos no acidente serem utilizados de forma indevida;

(iii) condução de investigações internas e criminais, quando aplicável, sobre o incidente; e

(iv) implementação de novas medidas de segurança para evitar que incidentes se repitam ou que chaves de segurança importantes para desencriptação dos dados sejam acessadas indevidamente.

Casos:

Abaixo vamos tratar de dois casos emblemáticos sobre incidentes de segurança no Brasil que podem servir de parâmetro sobre o que fazer e o que não fazer com relação aos incidentes de segurança.

Apesar de a autoridade nacional de proteção de dados brasileira ter sido criada recentemente e a LGPD ainda não estar em vigor, o Ministério Público do Distrito Federal e Territórios ("MPDFT") vem atuando na investigação de vazamentos de dados no país. As investigações sobre os casos descritos abaixo foram conduzidas pelo MPDFT recentemente.

Banco Inter: Em investigações, o MPDFT identificou o vazamento de dados cadastrais e certificados digitais, bem como de chave privada do banco do Banco Inter S/A, conhecido por um dos incidentes mais graves do país diante do envolvimento de dados de 100 mil correntistas. Ocorre que no primeiro contato com as autoridades no início de 2018, o Banco Inter tentou encobrir o incidente de segurança e portanto, dificultou a tomada imediata de medidas que poderiam mitigar os riscos e danos causados aos titulares. Principalmente por esse motivo, o Banco Inter foi condenado ao pagamento de multa no valor aproximado de 1,5 milhão de reais.

Netshoes: No caso do vazamento de dados cadastrais de aproximadamente 2 milhões de clientes da Netshoes, que ocorreu no início de 2018, o MPDFT recomendou que a empresa realizasse contato telefônico e informasse cada um dos clientes afetados sobre o incidente de segurança para que fossem mitigados os riscos causados. Uma vez implementada a medida indicada e diante da cooperação do Netshoes com as investigações, o caso já é conhecido como um exemplo de resolução de conflito de forma consensual, com o devido ressarcimento da sociedade, sem que a empresa tenha sido devidamente onerada. A empresa deverá pagar indenização de R$ 500.000,00 ao Fundo de Defesa de Direitos Difusos.

❖ RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS ou DATA PRIVACY IMPACT ASSESSMENT - DPIA

Gustavo Rocha & Carolina Braga

A Lei Geral de Proteção de Dados (LGPD) estabeleceu uma série de direitos e obrigações para as pessoas, físicas e jurídicas, que processam dados pessoais. Dentre os princípios elencados pela lei há o princípio da prestação de contas e responsabilidade (*accountability*) que determina que os agentes de processamento de dados (controladores e operadores) devem documentar suas atividades relacionadas a dados pessoais.

Considerando que alguns processamentos de dados pessoais podem ocasionar em riscos elevados, tanto para seus titulares como para a sociedade em geral, a lei estabelece o dever do controlador, em determinadas situações, a realização de um Relatório de Impacto à Proteção de Dados Pessoais (DPIA na sigla em inglês).

A sua definição encontra-se no artigo 5º, XVII da lei que estipula tratar-se de "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".

Trazendo à luz um pouco de conceito e história do termo, citamos Maria Hosken:

> *Avaliação de Impacto sobre a Proteção de Dados (ou DPIA, derivado do acrônimo em inglês Data Privacy Impact Assessment) é o nome dado ao processo que analisa e documenta o impacto futuro que o processamento dos dados pessoais terá sobre seus titulares. Por "impacto na privacidade" entende-se as consequências – possivelmente indesejadas – que o processamento de dados pode impor aos indivíduos ou à sociedade.*

A ideia de avaliações de impacto na privacidade surgiu nos anos 1970, mas seu conceito amadureceu durante o período 1995-2005, como uma reação pública tardia contra as ações cada vez mais invasivas de privacidade por parte de governos e corporações durante a segunda metade do século XX. A adoção de DPIAs pelas organizações se consolidou ao longo dos anos, sendo incorporada às estruturas de avaliação de risco como resultado dos danos reputacionais decorrentes de violações à privacidade, então já considerada uma variável estratégica.

Embora o termo DPIA tenha se tornado popular, não há um método sistemático para realizá-lo, havendo inúmeras orientações e listas de verificação publicadas por autoridades nacionais e organizações especializadas. Entretanto, algumas características distinguem tais relatórios de outros tipos de atividades pelas seguintes características:

- *Possui natureza antecipatória (ou seja, uma PIA é distinta de uma auditoria de privacidade);*
- *Tem amplo escopo (em relação às dimensões de privacidade, perspectivas externas e expectativas dos titulares e governos);*
- *É orientado para analisar o surgimento de problemas e elaboração de soluções;*
- *Enfatiza o processo de avaliação, incluindo troca de informações, aprendizado organizacional e adaptação de design;*
- *Exige engajamento e envolvimento intelectual da alta direção (diretores e gerentes seniores).*

Convém esclarecer, ainda, a distinção entre a DPIA e um PIA (*Privacy Impact Assessment*), ainda que até mesmo algumas autoridades nacionais, como a CNIL (autoridade francesa), tratem as duas como sinônimas.

Muito embora tenham origem comum o PIA trata-se de uma avaliação mais abrangente dos impactos de uma ação à privacidade. A DPIA, por sua vez, concentra-se num recorte limitado a atividades de processamento específicas, a

saber as que envolvam e que possam vir a comprometer a proteção dos dados pessoais e violação aos direitos do indivíduo.

Como podemos perceber, não há uma regra, uma receita de bolo pronta para aplicar ao relatório a ser produzido, entretanto, algumas regras devem ser observadas. Para auxiliar nesta reflexão, destacamos o exarado por Giuseppe Mateus Boselli Lazarini:

> *DPIA é a sigla para Data Protection Impact Assessment, uma metodologia amplamente adotada pela legislação europeia de proteção de dados pessoais, a General Data Protection Regulation ("GDPR"). A LGPD importou o conceito, sob o nome de relatório de impacto à proteção de dados pessoais. Ele consiste basicamente em uma documentação que descreve os processos de tratamento[1] de dados pessoais que podem gerar algum risco aos direitos dos titulares, além das medidas e mecanismos empregados para mitigar esses riscos.*

Embora encontre base no Regulamento Europeu de Proteção de dados (GDPR) a lei brasileira, ao contrário do que ocorreu no Regulamento europeu, acaba por não oferecer maiores esclarecimentos e definições quanto à metodologia e forma que o relatório deve adotar. O seu art.38 apenas aponta que a autoridade nacional de proteção de dados (ANPD) poderá impor que o controlador realize uma DPIA.

No entanto, ainda que a empresa não seja requisitada pela autoridade nacional, a produção prévia do relatório deve ser incentivada, pois pode trazer grandes benefícios à empresa.

Cabe apontar, contudo, que pode ser interessante publicar um documento derivado do relatório, visto que este contém informações confidenciais, relacionadas a segredos comerciais da empresa, ou então que, caso fossem divulgadas, podem representar algum risco à segurança dos dados tratados.

Ademais, publicar um documento que contenha as principais conclusões do relatório, bem como as ações adotadas para entrar em conformidade, contribui para alimentar a confiança dos titulares de dados nas práticas da empresa e a melhorar a sua imagem, pois demonstra, além da conformidade com a legislação, o comprometimento com a transparência do tratamento dos dados pessoais pela empresa. Dessa forma, mais do que um custo, a conformidade em LGPD é uma oportunidade de alavancar negócios.

Cabe, então, considerar quando deve ser realizada uma DPIA. Diferente da GDPR, a LGPD não considera a necessidade de existência de um risco elevado para que seja exigível a realização de uma DPIA. Dessa forma, caso a lei fosse interpretada de forma literal, poderia-se entender que o relatório deveria ser realizado em todas as atividades de tratamento, o que inviabilizaria muitas dessas atividades desnecessariamente.

Dessa forma, guiando-se pelos parâmetros estabelecidos pela GDPR (artigo 35), pode-se dizer que a DPIA deve ser realizada quando o tratamento proposto envolve:

- uma avaliação sistemática e exaustiva dos aspectos pessoais relativos às pessoas singulares baseado em processamento automatizado, incluindo perfis, e que servem de base para decisões que produzem efeitos legais relativos à pessoa singular ou que produzem efeitos similares em pessoas naturais;

- tratamento em grande escala de categorias especiais de dados referidas no nº 1 do artigo 9º (dados pessoais revelando origem racial ou étnica, opiniões, convicções religiosas ou filosóficas, ou filiação sindical, e o processamento de dados genéticos, dados biométricos com a finalidade de identificar unicamente uma pessoa relativa à saúde ou a dados relativos à vida sexual ou orientação sexual de uma pessoa singular) ou Dados pessoais relativos a condenações penais e infracções previstas no artigo 10.º; ou

- um acompanhamento sistemático de uma área de acesso público em grande escala

Dessa forma, na ausência de um parecer da autoridade nacional delimitando a aplicação da lei, considera-se que a DPIA deve ser realizada em projetos nos quais um ou mais dos seguintes itens se aplica:

a. informações sobre pessoas naturais serão coletadas e processadas pela primeira vez;

b. as informações sobre os indivíduos serão compartilhadas com pessoas ou organizações que anteriormente não tinha acesso a ele;

c. mudança de uso (finalidade) de dados pessoais existentes

d. o uso de nova tecnologia que coleta ou usa dados de natureza pessoal, por ex. biometria;

e. os dados pessoais existentes serão usados para tomar decisões como parte de um processo automatizado;

f. pode-se razoavelmente esperar que um titular de dados possa considerar qualquer aspecto do projeto demasiadamente intrusivo;

Com a sanção presidencial da Medida Provisória nº 869 em julho de 2019, após sua passagem pelo Congresso Nacional, a Autoridade Nacional de Proteção de Dados poderá ser finalmente criada. Dessa forma, espera-se um detalhamento e orientações mais claras quanto à metodologia a ser utilizada quando da confecção do relatório.

Por fim, antes de adentrar nas fases que compõem a DPIA é necessário, como lembrado por Marcílio Braz Jr., que a empresa se faça os seguintes questionamentos:

- Foi realizada uma consulta junto aos stakeholders internos com relação aos possíveis riscos relativos à atividade de processamento em análise, bem como os riscos de não conformidade ante a LGPD e os instrumentos internos de

controle (políticas, processos e procedimentos voltados a proteção de dados e privacidade)?

- Foram de igual forma consultados os stakeholders externos? Em caso afirmativo, quem, quando e com qual propósito objetivou-se a consulta?
- Adicionalmente à identificação dos riscos envolvidos, ambas consultas levaram em consideração medidas de mitigação ou minimização destes riscos?"

Uma vez realizadas as considerações levantadas acima, dá-se início efetivo ao processo de elaboração do relatório.

O escopo de um *Data Protection Impact Assessment* - DPIA não é eliminar os riscos por completo (o que seria utópico), mas sim dar um direcionamento aos fluxos para minimizar os riscos ou justificar a existência dos mesmos.

Inclusive, em visão corroborada por Marcílio Braz Jr. na sua publicação DAS ETAPAS DE ELABORAÇÃO DE UM DPIA, publicado no portal Jota (e como autorização expressa do autor para republicar o mesmo) o DPIA pode ser uma excelente ferramenta de construção de gestão interna das empresas, posto que amplia os conceitos de *compliance* interno e auxilia a encontrar os riscos e as oportunidades de melhorias.

Na mesma publicação, de forma muito didática, o autor explicita um caminho simples e objetivo como sugestão/ideia para a elaboração de um relatório de DPIA, transcrito abaixo:

Visão macro - 3 etapas:

1. Entendimento da organização e processos envolvidos (Contexto)
2. Risk Assessment (Processo de avaliação de riscos)
3. Risk Management (Gerenciamento de riscos)

Visão micro - 6 fases

Fase 1 – Detalhamento do processamento

Fase 2 – Análise do processamento tendo em conta possíveis relações com terceiros e respectivo contato para colaboração na elaboração das fases seguintes

Fase 3 – Identificação de controles

Fase 4 – Listagem e análise de eventos e ameaças para o titular de dados quanto ao processamento dos dados pessoais

Fase 5 – Produção de relatório com sumário de análise, controles existentes e mitigação de risco, bem como propostas de medidas técnicas e organizacionais apropriadas para mitigar o risco do titular de dados, caso estas não estejam em prática

Fase 6 – Envio para aprovação ou recusa ao DPO

Resta diáfano que não existe uma receita de bolo pronta, que poderia ser aplicada em todos os casos, entretanto, ter um norte para criar o próprio caminho já auxilia em muito o processo como um todo.

Diante destas premissas básicas e iniciais, podemos começar a concluir alguns aspectos relevantes ao relatório DPIA:

Seu bojo será construído de forma individualizada, estruturada em cada negócio e focada em riscos conforme atuação da empresa.

Quanto mais dados forem informados ao elaborador/criador do relatório, mais será possível ter uma visão abrangente e completa sobre os reais riscos e nuances necessárias para a análise.

Se as informações não estiverem organizadas/sistematizadas, o relatório poderá levar mais tempo para ser elaborado ou até mesmo perder uma análise mais coerente por falta de informações.

Além das pessoas de operação - que vivenciam coleta, uso, gestão dos dados - pessoas de gestão devem contribuir em conjunto para que o relatório demonstre

uma realidade da empresa como um todo e não uma maquiagem de algo que na prática ocorre diferente.

Claramente terá o relatório que ser elaborado por pessoas que compreendam o nicho de trabalho da empresa, suas nuances, parceiros, fornecedores e meandros internos da organização, pois justamente no dia a dia, nos documentos que não estão em no sistema, nos e-mails que não saem em relatórios que as falhas acontecem e sem esta visão profunda da empresa, fica inviável de ter uma mitigação de riscos adequada.

Para ter, portanto, um relatório de DPIA mais assertivo, pense nas pessoas envolvidas, nos dados a serem coletados, no mercado e suas particularidades, enfim, pense com abrangência para perceber ou prever possíveis riscos e passivos. E, sendo você que será o responsável pela elaboração e/ou pela aprovação do mesmo (DPO), cuidado: Sua chancela tem o poder de realmente mitigar riscos ou deixar brechas para multas volumosas previstas na lei.

❖ PRIVACY BY DESIGN

Angela Maria Rosso

"A privacidade tem sido vista historicamente como um impedimento à inovação e ao progresso, mas esse é um modelo de negócios ultrapassado e não efetivo. Sem a confiança do usuário, tecnologias não avançam". Ann Cavoukin

▪ Introdução

Em uma economia em que o tratamento dos dados pessoais se tornou importante ferramenta para as atividades de marketing, venda, saúde e análise de risco embutida nas atividades das seguradoras, por exemplo, não demorou para que a utilização desse insumo passasse a ser abusiva. Foi a partir do tratamento indiscriminado e não disciplinado de dados pessoais que chegou-se

a meios de discriminação das pessoas, os titulares dos dados. Com o objetivo de regular a utilização de forma que ela auxiliasse na construção da sociedade sem prejudicar o indivíduo é que foram criadas leis que tinham como objetivo garantir que esses processos fossem transparentes de modo a garantir que o proprietário dos dados pudesse sempre saber exatamente com qual finalidade e por quem suas informações pessoais são utilizadas.

Nesse sentido é o teor do Recital 4 do Regulamento Geral de Proteção de Dados da União Europeia - RGPD ao estabelecer que o "processamento dos dados pessoais deve ser projetado para servir a humanidade" sendo este pensamento que também norteou a criação da lei brasileira e que motiva as discussões acerca do direito à proteção de dados no mundo.

Ao longo do tempo, contudo, identificou-se que ter leis e regulamentos que determinavam que o direito à proteção de dados deveria ser garantido, mas que não diziam quais recursos deveriam ser utilizados para implementá-lo, não eram mecanismos suficientemente eficazes. Assim, as normas passaram a estabelecer alguns padrões fundamentais para garanti-lo, sendo a abordagem de que a proteção dos dados deveria ocorrer desde a fase de projeto de um sistema, produto ou serviço um desses preceitos.

Foi assim que a expressão *Privacy by Design* (PbD) surgiu no contexto legal como um princípio de aplicação obrigatória para todos aqueles que se submetem ao Regulamento Geral de Proteção de Dados da União Europeia - RGPD ou da Lei Geral de Proteção de Dados Pessoais do Brasil - LGPD onde tem sido traduzida como Privacidade desde o Desenho ou desde o Projeto. A conceituação do Princípio é simples e consiste no desenvolvimento de serviços e produtos com a proteção à privacidade embutida desde a concepção, entretanto a aplicação é complexa e envolve compreender todo o processamento a que o dado pessoal é submetido. Nesse contexto, a PbD tornou-se o ponto chave para a

implementação e para a demonstração da conformidade de um produto, negócio ou serviço com as leis de proteção de dados.

Dessa forma, tornou-se um princípio basilar das leis de proteção de dados cuja falta de implementação já ocasionou sanções na Europa, devendo, portanto, a Privacidade desde o Projeto ser aplicada por todos aqueles que realizarem tratamentos de dados pessoais. Saliente-se que aplicar os princípios que formam a PbD é também uma forma de agregar valor ao produto ou serviço resultante do processo, uma vez que traz como consequência a transparência de todo o ciclo de vida que o dado percorrer dentro da organização, tornando o caminho totalmente auditável gerando confiança dos clientes e também dos stakeholders.

- **Histórico, definição e princípios**

A preocupação com a proteção da privacidade tem sido uma constante na sociedade com o consequente desenvolvimento de abordagens e modelos principiológicos que contemplam e servem como melhores práticas na implementação do conceito.

As primeiras regulamentações a tratarem do tema determinavam que a garantia da privacidade dos dados pessoais passava pelo respeito aos Princípios FIPs *(Fair Information Practices)*, no desenvolvimento de um sistema, produto ou serviço que são os seguintes:

1. Especificação da finalidade e uso limitado (*Purpose Specification and Use Limitation);*
2. Participação do usuário e transparência *(User Participation and Transparency);*
3. Segurança forte (*Strong Security).*

Quando esses Princípios foram adotados, na década de 90, como requisito suficiente para preservar a privacidade dos indivíduos visto que o padrão de utilização dos dados pessoais era muito diferente do que o padrão atual.

Contudo, diante da evolução tecnológica constante, em que céu é o limite para as possibilidades de utilização de informações pessoais, os três princípios, embora ainda essenciais, já não se mostram mais suficientes para garantir a proteção da privacidade dos indivíduos.

Com o tempo teve-se a percepção de que por melhor empregados que fossem chegava-se inevitavelmente no dilema: quanto mais privacidade era fornecida, menos inovação se tornava possível e quanto mais se privilegiava a inovação menor o nível de privacidade oferecido - o que é entendido como soma zero - porque ao se contemplar um aspecto necessariamente abre-se a mão de outro tão importante quanto, o quê, em se tratando de sistemas, serviços ou produtos caracteriza uma entrega ruim.

Esse impasse eleva o nível de risco ao qual a organização está exposta, porque, por exemplo, se o nível de proteção à privacidade contemplado no sistema não é o suficiente a organização pode estar descumprindo alguma lei, expondo-se à situações de violação de dados (*data breachs*).

Nesse contexto em que se precisa - e se deve - proteger mais a informação pessoal e tornar transparente a utilização de dados, em que se deseja retirar do usuário a responsabilidade exclusiva pela proteção das próprias informações e ainda equilibrar a relação inovação e proteção de dados em uma relação ganha-ganha em que um objetivo não precisa ser sacrificado pelo outro é que tomou forma a metodologia PbD.

A PbD é um conjunto de princípios que englobam as práticas previstas pelo FIPs, adotando uma abordagem evolutiva em que a proteção à privacidade deixa de ser uma mera questão de compliance (época dos FIPs) para se tornar uma questão de negócio e que atinge hoje o patamar de diferencial competitivo: produtos e serviços desenvolvidos contemplando os 7 princípios de PbD fazem

com que o indivíduo olhe para a organização que o implementa com confiança. O usuário/cliente passa a confiar que seus dados recebem o tratamento adequado e que isso independe de qualquer atitude sua.

Para o controlador de dados há ainda mais ganho se considerado que eventos de quebra da privacidade (*privacy breaches*) podem ter uma capacidade altamente destrutiva para a organização, uma vez que, além de serem causa de grandes prejuízos - as legislações têm previsto sanções cada vez mais severas - impactando nas finanças: multas, processos judiciais por danos materiais ou morais ainda tem o poder de marcar a imagem da organização perante a sociedade, ou seja, o prejuízo além de econômico é social e por vezes irreparável, é preciso lembrar sempre: não há como desfazer um *data breach*, se os dados caíram na rede eles ficarão por lá.

Sob esse cenário Ann Cavoukian enquanto Comissária de Informação e Proteção de Dados em Ontário no Canadá apresentou ao mundo o conceito de Privacy by Design.

Para ela só é possível que sistemas e serviços garantam que estão tratando adequadamente a privacidade dos indivíduos se forem projetados para isso. Em acordo com a autora a abordagem Privacy by Design encontra-se fundada em 7 princípios que lhe dão forma. São eles:

1. **A proteção deve ser preventiva não reativa** - eventos que tenham potencial para violar a privacidade dos dados pessoais devem ser previstos antes que aconteçam, é preciso antecipar práticas ruins e corrigi-las antes que sejam exploradas;

2. ***Privacy by default* (Privacidade por padrão)** - acima de qualquer coisa uma implementação orientada pela PbD deve garantir que se o

usuário não fizer nada para proteger sua privacidade seus dados ainda assim estarão protegidos por padrão (by default):

- a finalidade para a qual o dado será utilizado deve ser claramente informada para o proprietário dos dados antes ainda deles serem coletados - a informação tem que ser dada de forma completa e relevante e a utilização do dado pessoal deve se restringir a essa finalidade;

- sempre que possível transações que envolvam dados pessoais devem por padrão serem feitas com dados não identificáveis e mais a utilização de informações pessoais deve ser reduzida ao mínimo possível (data minimization), a privacidade é presumida e deve ser garantida.

3. **Privacidade embarcada no projeto** - a privacidade deve estar integrada ao sistema, desde o projeto passando pela arquitetura, todos devem trabalhar de forma que ela seja garantida, mas sem diminuir a funcionalidade, exige-se criatividade dos projetistas e arquitetos que devem entregar as duas características;

4. **Funcionalidade total** - a PbD prevê um sistema de ganha-ganha, não se devem fazer trocas desnecessárias, ou seja, não se deve perder em funcionalidade para garantir a segurança, assim como não se deve trocar a privacidade por uma melhor funcionalidade;

5. **Segurança ponto a ponto** - o dado pessoal deve ser protegido durante todo o seu ciclo de vida na organização. O quinto princípio da metodologia trata da proteção do dado durante todo o ciclo de vida. Não se admitem lacunas (gaps) em nenhuma fase do tratamento do dado, desde o berço (coleta) até a sua morte (destruição) ele deve contar com a melhor proteção que possível. A implementação desse ponto passa por garantir a segurança do dado pessoal a partir da observação dos pilares da Segurança da Informação: confidencialidade, integridade e disponibilidade,

acrescentando métodos seguros de destruição, encriptação e forte controle de acesso aos sistemas.

6. **Visibilidade e transparência** - a questão aqui é permitir que qualquer parte envolvida no processo tenha total e transparente acesso ao que ocorre com os dados tratados, de forma a que seja possível responsabilizar quem não o faça dentro dos parâmetros acordados previamente (antes da coleta), ou seja, permite a responsabilização (accountability) de quem processa ou controla o dado. Outro ponto importante é que visibilidade e transparência permitem monitorar se a organização está em conformidade com a legislação (compliance);

7. **Respeito pela privacidade do usuário** - o interesse do usuário deve estar no centro de qualquer projeto que envolva o tratamento de dados pessoais: consentimento, correção, acesso e conformidade são direitos que estão embutidos nesse princípio.

Inicialmente a abordagem defendida por Ann Cavoukian não passava dos portões acadêmicos uma vez que sua aplicação prática era entendida como inviável pela complexidade e como prejudicial ao desenvolvimento tecnológico de nichos do mercado que cada vez mais se utilizava de dados pessoais como motor para os negócios e para a inovação.

Contudo, já na Diretiva de Proteção de Dados 95/46/EC, lei precursora do RGPD, podiam ser encontradas referências à abordagem. Em seu recital 46 a Diretiva 95 referenciava as medidas que se destinavam a promover a proteção das liberdades e direitos dos indivíduos através da Proteção de Dados deveriam ser aplicadas desde o projeto do sistema de processamento de dados bem como durante o processamento.

Importante movimento no sentido de reconhecer a abordagem Privacy by design como fundamental ao contexto de Proteção de Dados Pessoais ocorreu em 2010 com a aprovação de uma resolução sobre o tema que reconheceu que somente as leis e políticas de proteção de dados existentes não eram suficientes como garantia da privacidade e admitindo que a abordagem PbD pode ser aplicada de forma holística dentro da organização em sistemas de tecnologia, práticas de negócios, processos, projetos físicos e rede estruturada.

A partir desse reconhecimento as autoridades foram convidadas a promover os conceitos derivados da PbD de forma que o modelo fosse adotado por todos como boa prática em se tratando de proteção de dados.

Entretanto, as recomendações contidas na Diretiva e na resolução não foram suficientes diante de um contexto econômico em cada vez mais impulsionado pelo uso dos dados pessoais, o grupo de trabalho do Artigo 29 (WP 29) entendeu pela necessidade de recomendar que o novo regulamento deveria obrigar desenvolvedores de tecnologia e os controladores de dados a adotarem medidas de proteção dos dados pessoais desde a fase de planejamento do sistema ou processo.

Ainda em 2010 a Autoridade Europeia para Proteção de Dados (EDPS) emitiu um parecer posicionando-se no sentido de que a utilização da abordagem PbD era fator determinante para o aumento da confiança na tecnologia da informação e que tal princípio deveria estar previsto na legislação geral da União Europeia bem como nas legislações internas dos países membros.

Já em 2017 houve a proposição para a ISO no sentido de que PbD em produtos e serviços fornecidos para consumidores fosse convertida em uma nova ISO de forma que se transformasse em um padrão reconhecido também para o desenvolvimento de bens e serviços de utilização doméstica que atendem aos requisitos de proteção de dados.

- **PbD no RGPD e na LGPD**

As leis que abordaram o tema e o trouxeram para a seara da obrigatoriedade não se referiram expressamente ao nome Privacy by Design adotando nomenclaturas equivalentes. Assim, o RGPD fala expressamente em Proteção de Dados desde a Concepção e Proteção de Dados por Padrão (Data Protection by design e Data Protection by Default) em seu artigo 25 que atribui ao controlador dos dados o dever de implementar as medidas técnicas apropriadas desde a fase de projeto do produto ou serviço passando pela fase de operação com o fim de garantir a devida segurança ao tratamento dos dados pessoais.

O referido artigo cita as técnicas de pseudo anonimização e de minimização da coleta como maneiras de proteger os direitos fundamentais dos indivíduos cujos dados são processados. Ressalta, todavia, que essas medidas devem ser tomadas levando-se em conta algumas características do processamento dos dados, tais como estado da arte, o custo e a finalidade do tratamento entre outras. Estabelece ainda que para que se reconheça a existência da Privacidade por Padrão (*Privacy by Default)* é necessário que "**somente os dados necessários para cada finalidade específica podem ser tratados**".

Complementa o referido artigo o Recital 78 que explica que a proteção prevista para os dados pessoais requer a aplicação das técnicas apropriadas garantindo que os requisitos do RGPD sejam atingidos. Explica também que deve o controlador adotar os Princípios pertencentes à PbD para demonstrar a conformidade do tratamento dos dados realizado com as previsões legais pertinentes.

Já na lei brasileira (LGPD) a referência à abordagem PbD está no seu artigo 46, §2º:

> *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*
>
> *§ 2º As medidas de que trata o caput deste artigo deverão ser observadas* ***desde a fase de concepção do produto ou do serviço até a sua execução*** *(grifamos).*

Importante destacar que diferentemente da lei europeia que determina que a implementação da PbD é de responsabilidade do controlador de dados, na lei brasileira tal obrigação é de incumbência de todos os agentes de tratamento o que obriga também os operadores de dados.

Dessa forma, conforme mostram as leis, a abordagem PbD não é mera boa prática ou recomendação, sendo na verdade um conjunto de princípios de aplicação obrigatória para todos aqueles que atuem como controladores de dados na UE e como agentes de tratamento de dados no Brasil.

- **Como implementar produtos e serviços com *Privacy by Design* embarcada**

De acordo com a Parecer 5/2018 a implementação dos Princípios da PbD está diretamente ligada à existência de um programa de gestão de Segurança da Informação efetivo que garanta que os dados processados pela organização estejam adequadamente protegidos, especialmente quanto à confidencialidade e à integridade, e com os riscos de violação mitigados. Na LGPD a segurança é um requisito necessário para o tratamento de dados pessoais e está presente no

artigo 6, VII. A garantia de segurança se dá a partir da adoção de medidas técnicas e administrativas que evitem acessos indevidos ou ilícitos aos dados.

O Recital 78 do RGPD prevê que as medidas que podem ser implementadas para atender aos requisitos da PbD consistem nas seguintes: minimização do processamento dos dados pessoais equivalente ao Princípio da Necessidade previsto no art. 6, III que determina que somente deve ser realizado aquele tratamento de dado pessoal que esteja dentro da finalidade para o qual foi coletado; pseudoanonimização sempre que possível, equivalente ao art. 13, §4º; transparência no processamento de dados, de tal forma que o titular dos dados consiga monitorar como são utilizados seus dados, na LGPD a transparência é outro princípio presente no artigo 6º, VI que prevê que deve-se garantir ao sujeito dos dados facilidade de acesso às informações a ele pertinentes acerca do tratamento e dos agentes de tratamento.

Assim, a abordagem de Privacidade desde o Projeto (*Privacy by design*) exige que várias dimensões sejam observadas para que sejam contemplados seus princípios. O EDPS no Parecer 5/2018 destaca quatro delas, a saber:

1. o princípio deve ser atendido por todos os softwares que de forma completa ou parcial processem dados pessoais sendo que as garantias de segurança devem ser aplicadas durante toda a vida do dado, devendo ser tais medidas devidamente identificadas dentro dos requisitos do projeto;
2. deve ser adotada uma abordagem de gerenciamento de riscos que tenha como objetivo selecionar e implementar medidas que garantam a efetiva proteção dos dados;
3. as medidas adotadas devem ser apropriadas e efetivas para garantir a proteção dos dados pessoais e também para demonstrar o *compliance* com as leis;
4. integrar as medidas de segurança previstas na lei no processamento. As leis apresentam algumas medidas de segurança que devem ser obrigatoriamente implementadas, assim, elas devem ser integradas ao processo e apresentadas aos titulares dos dados através das políticas de privacidade.

Enquanto a construção de projetos adequados à *Privacy by Design* envolve um processo de criação bastante com complexo a implementação dos conceitos da Privacidade por Padrão (*Privacy by default)* envolve uma parte mais operacional, uma vez que traduz-se no cumprimento dos requisitos da finalidade, da minimização (RGPD) ou da necessidade (LGPD), da transparência.

A observância desses Princípios elencados pela lei implica obrigatoriamente que por padrão qualquer outro uso que possa ser feito do dado pessoal diferente da finalidade para o qual foi coletado deve ser deixada desativada por padrão, ou seja, só podem ser realizados aqueles tratamentos do qual o titular dos dados tenha conhecimento ou tenha condições de conhecer.

- **PbD em produtos e serviços existentes, é possível?**

A orientação pela utilização de PbD é recente e mais ainda o é a sua obrigatoriedade. No Brasil, por exemplo, somente com a aprovação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) é que se começou a olhar a metodologia com mais cuidado e, embora, o modelo seja realmente desejável, fica a pergunta:

- o que fazer nas circunstâncias atuais em que muitos dos serviços e produtos sequer atendem ao FIPs?
- É possível adequar sistemas, produtos e serviços existentes a essa regulamentação que prevê que a utilização de PbD é obrigatória?
- É possível incorporar PbD e utilizar isso como um diferencial competitivo diante de um mercado que cada vez mais demonstra estar preocupado com isso?

É preciso lembrar que a raiz da PbD está no comportamento preventivo e não no reativo, é característica da abordagem, e é o seu primeiro princípio, de modo que, embarcá-la no projeto desde o início é, sem dúvidas, a alternativa mais fácil,

menos onerosa e mais viável. Contudo, precisamos reconhecer que não há a menor possibilidade de se refazer tudo, a boa notícia é que é possível incorporar PbD em produtos, sistemas e serviços já existentes. A concretização dessa adequação passa por contemplar alguns pontos que constam como Princípios de Ética para Ciência de Dados no modelo adotado pelo governo da Inglaterra, são eles:

1. **Estabelecer claramente quais as necessidades do usuário**/cliente e quais os benefícios para ele: o que o meu cliente/usuário ganha ao consentir com o tratamento que eu faço dos dados?

2. **Minimizar a coleta de dados:** quais dados eu preciso para atingir o objetivo de atender as necessidades do meu usuário/cliente? Quais dados eu preciso tratar para atingir a finalidade do meu negócio (legítimo interesse)? Quais dados eu posso (e preciso) coletar para atender aos requisitos legais. Somente os dados necessários devem ser coletados, nada além disso;

3. **Criar modelos consistentes de Ciências de Dados** - é importante que não existam lacunas nesses modelos, eles devem ser destinados a atender exclusivamente às finalidades previstas para os dados pessoais (legítimo interesse, bases legais e a previsão no termo de consentimento); sempre que possível os modelos devem utilizar como insumo dados anonimizados ou pseudoanonimizados. Deve-se ter em mente que quanto mais difícil de identificar o titular do dado a partir da informação tratada, mais seguro é o modelo e, portanto, maior o nível de proteção à privacidade minha organização oferece;

4. **Estar atento para a percepção do usuário/cliente** - a existência de reclamações, de pedidos de correção, de retirada do consentimento ou de pedidos de explicação pode ser considerado um importante indicativo

de que há incongruências no sistema. Ouvir o que o usuário/cliente tem a dizer e, se necessário, adequar a metodologia de tratamento de dados é também uma forma de agir preventivamente;

5. **Seja o mais transparente possível** - mostrar que a preocupação com a proteção da privacidade é inerente à organização, adotando processos auditáveis e que possam ser mostrados ao usuário/cliente/autoridade/auditor, obviamente, sem expor a inteligência do negócio, é um dos requisitos para atendimento dos princípios de PbD;

6. **Torne os dados seguros** - este é, na verdade, um comportamento já esperado de qualquer organização e que já deveria ter sido adotado desde sempre no tratamento dos dados pessoais. Investir em treinamento de pessoal, testes de penetração, políticas de acesso, ou seja, ter uma política de segurança de dados aculturada e fielmente cumprida; investir em infraestrutura de tecnologia, criptografia de dados, pseudoanonimização - precisamos compreender que a segurança dos dados é investimento, não custo;

7. **Adequar a Política de Privacidade existente para a realidade operacional da organização** - a política de privacidade deve refletir a realidade da organização. Não adianta ter uma política de privacidade ideal se o processo é falho, ser honesto e mostrar que a prática está representada na teoria é importante e gera confiança - estou para ver o dia que política de privacidade falsa seja considerada fraude;

8. **Destacar termos de consentimento**, estando eles em linguagem clara, simples e onde seja possível ao cliente/usuário saber de forma específica, objetiva e prévia ao "OK" (consentimento) quais são as finalidades com as quais ele está assentindo compartilhar seu dado.

Conclusão

Incorporar os Princípios de PbD em novos projetos é uma tarefa desafiadora, exige-se uma mudança na cultura de privacidade das organizações que passa pela conscientização e pelo comprometimento de todos os *stakeholders* envolvidos no tratamento dos dados. Embarcar PbD nos projetos é mais do que desenvolver um processo de acordo com um método, exige-se uma mudança no jeito de pensar os produtos, sistemas e serviços de forma a privilegiar a proteção da privacidade sem prejudicar o desenvolvimento tecnológico.

Há uma mudança de paradigma ditada pelos princípios fundadores da Privacidade desde o Projeto e da Privacidade por Padrão a partir da obrigatoriedade de se adotar uma postura preventiva em detrimento da relativa em relação aos eventos que coloquem em risco a privacidade dos titulares dos dados. Não basta mais reagir aos vazamentos de dados ou aos incidentes que prejudiquem a confidencialidade ou a integridade dos mesmos, é preciso que se antecipe qualquer possibilidade de violação da segurança do dado durante todo o seu ciclo de vida na organização, seja por desvios no tratamento do dado, seja por violações causados por ataques hackers, por exemplo.

Saliente-se que as organizações podem extrair muitos benefícios da adoção da abordagem de PbD, uma vez que ao adotá-la torna-se possível conhecer todo o caminho percorrido pelo dado, todo o seu ciclo de vida, identificando exatamente quais os dados que são fundamentais ao negócio. Cria-se, assim, a possibilidade, de eliminar àqueles que sejam excessivos à finalidade descrita e por consequência diminuindo o risco de uso indevido. Outra consequência é a minimização da quantidade de dados coletados ou armazenados, por exemplo, ou ainda a melhora na percepção do real valor de determinado dado como ativo da organização, permitindo que aqueles mais valiosos sejam protegidos de forma ainda mais efetiva.

Para Ann Cavoukian, implementar PbD exige uma evolução no modo como políticas e regulamentos que abordam a proteção da privacidade são construídos, sair do reativo para o preventivo é mais do que uma escolha é uma necessidade.

❖ GOVERNANÇA DE DADOS

Gisele Kauer

Se há uma questão que deve ser prioridade zero quando uma corporação toma a decisão de implementar um programa de proteção de dados, é a Governança de Dados. Como já mencionado no capítulo referente à segurança da informação, ainda que a proteção de dados pessoais esteja hoje nos *highlights* em termos midiáticos, está só poderá ser implementada de maneira efetiva uma vez que tenhamos os três pilares denominados "CID": Confidencialidade, Integridade e Disponibilidade. E, uma vez que seja assegurado que os três pilares da segurança da informação se fazem presentes, podemos falar sobre governança de dados.

Aqui, cabe ressaltar: ainda que um grande parte das empresas demonstre um anseio pela elaboração das políticas e procedimentos, estas devem entrar nas últimas etapas da implementação, sendo um tanto quanto contraproducente contar com quaisquer documentos sem antes haver uma busca por conhecer o processamento realizado pela própria empresa, bem como as áreas que seguirão estas políticas e procedimentos.

A governança de dados abrange em si a compreensão de como é realizado o processamento de dados dentro da companhia.

Neste contexto, falamos em processamento (ou "tratamento", termo utilizado na LGPD) levando em consideração o rol exemplificativo trazido no artigo 5º, X, da lei brasileira de proteção de dados pessoais, como *"toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,*

arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Nesta etapa, é ideal que já se tenha um prévio parecer em matéria de segurança da informação, para que então seja possível entrar especificamente nas matérias de proteção de dados pessoais.

Todavia, tão importante quanto (ou até mesmo mais importante que) saber quais os tipos de processamento, é a identificação de fluxos de dados. Aqui, temos várias opções oferecidas pelo mercado, especialmente em questão de mapeamento jurídico e mapeamento técnico. O mapeamento jurídico, de forma geral, consiste em entrevistas; isto é, perguntas aos responsáveis pelos setores da empresa (RH, jurídico, *supply chain*, etc) com o intuito de identificar a entrada e saída de dados pessoais. Ainda que seja uma prática reiterada esse tipo de mapeamento, não podemos afirmar que se trata de algo equivalente ao mapeamento técnico, ou que o substitua. Somente através do mapeamento técnico se faz possível a identificação fática da veracidade das afirmações fornecidas no mapeamento jurídico.

O mapeamento tem por objetivo fornecer um norte para que se façam possíveis as demais etapas do programa de proteção de dados - isto é, para que se conheça o terreno em que estamos pisando. O documento gerado após a finalização desta etapa é o Parecer de Mapeamento de Dados, o qual pode conter organogramas dos fluxos, demonstrando a entrada e saída de dados, bem como, no que diz respeito às formas de tratamento, fazer menção às hipóteses legais de tratamento apresentadas pelas leis e regulamentos de proteção de dados pessoais.

Outro ponto que se faz importante observar é que o mapeamento (bem como tudo aquilo englobado na Governança de Dados) deve contar com uma abrangência de todos os setores, não descartando a possibilidade de fluxos em

áreas que inicialmente não levantem fortes alardes; no mesmo sentido, é importantíssimo considerar que terceiros envolvidos nos fluxos e atividades da empresa também devem ser considerados nessa etapa; na ótica da LGPD, o controlador é responsável por fornecer instruções claras ao operador sobre como proceder com o tratamento. Qualquer companhia que figure no organograma como controlador deve ter preocupação quanto às atividades do processador, uma vez que este é responsável legalmente em diversas hipóteses caso o processador não esteja em *compliance* com a lei brasileira de proteção de dados.

Sendo assim, o que podemos concluir acerca da governança de dados é que, tal como determinado pelas normas de segurança da informação, é necessário que as informações da empresa estejam em bases de dados estruturadas. Isso é essencial para que o programa possa ser implementado de forma plena, e será relevante para elaboração de políticas, procedimentos, e até mesmo em caso de incidente, para que se saiba o que fazer para mitigar, em quais áreas e fluxos será necessário agir, e até mesmo para que se identifique qual foi a porta de entrada que gerou o incidente.

Por fim, é importante lembrar que é um tanto errônea a concepção de que a governança de dados se trata apenas de um momento inicial do projeto; compreendendo a necessidade de que a governança seja um processo constante com revisões periódicos e atualizações tempestivas.

❖ GOVERNANÇA DE PRIVACIDADE

Remilina Yun (Remi)

A construção de um programa de privacidade robusto está atrelada a adoção de uma governança apropriada, conformidade frente às legislações e normas de privacidade, e atingimento dos objetivos da organização.

Na governança de privacidade alguns componentes devem ser observados:

- Missão e visão de privacidade da organização estabelecidas;
- Escopo do programa de privacidade estabelecido;
- Adoção de uma estrutura de privacidade adequada;
- Estratégia de privacidade da organização
- Estrutura de um time de privacidade;

A. Missão e visão de privacidade da organização

A missão e visão de privacidade de uma organização são fatores chaves que estabelecem as bases de um programa de privacidade que deve estar alinhado com o propósito mais amplo da organização. Ela tem relação direta com a identidade da organização.

Enquanto isso a visão organizacional representa sobre um objetivo a ser alcançado num futuro próximo. Sua redação normalmente se resume numa pequena sentença de maneira clara e concisa, e muitas vezes já seguem dispostas na missão geral da organização e/ou código de conduta.

B. Escopo do programa de privacidade

Uma vez estabelecida a missão e visão da organização, é necessário definir o escopo do programa de privacidade, cabendo a cada uma dessas organizações identificar suas legislações e normas para se buscar conformidade com suas obrigações, principalmente no tocante a privacidade e proteção de dados. Uma maneira de definir o escopo é seguindo duas etapas:

1. Identificar os dados pessoais coletados e tratados

Para atender essa etapa, abaixo seguem alguns questionamentos para *Data Mapping* (Mapeamento de Dados).

- Quem coleta, usa e mantém dados pessoais relacionados a pessoas, clientes, empregados e terceiros?
- Quais tipos de dados pessoais são coletados?
- Qual é a finalidade da coleta?
- Onde os dados são armazenados fisicamente?
- A quem os dados foram transferidos?
- Quando os dados foram coletados?
- Como os dados foram coletados
- Por quanto tempo os dados são retidos?
- Como os dados são excluídos?
- Quais controles foram estabelecidos para proteger os dados?

2. Identificar as legislações e normas à relativas privacidade e proteção de dados

Quanto essa etapa, recomenda-se associar a etapa anterior com:

- Tipo de segmento ou indústria;
- Tipo de produto e/ou serviço;
- Matriz e subsidiárias;
- Mercado interno ou global;

C. Desenvolver e Implementar uma estrutura (*Framework*)

Uma vez identificadas as legislações aplicáveis, uma estrutura adequada deve ser estabelecida para adoção de controles necessários, bem como a gestão dos dados pessoais mapeados.

A implementação e gestão de um programa de proteção de dados relativos a diversos direitos e obrigações para cada regulamento de privacidade é um grande desafio.

Contudo, a adoção de uma estrutura de privacidade adequada para construção de um programa efetivo de privacidade poderá:

- Ajudar a atingir a conformidade com as legislações e normas de privacidade no escopo da sua organização;
- Servir como uma vantagem competitiva para organização que demonstrar o valor na proteção de dados pessoais, gerando assim, confiança;
- Identificar processos em desuso, desatualizado e/ou inadequado, gerando oportunidade de revisão;
- Apoiar o compromisso e os objetivos do negócio das partes interessadas, clientes, parceiros, entre outros;

O termo framework é amplamente utilizado para os vários processos, modelos, ferramentas, leis e padrões que podem orientar o profissional de privacidade no gerenciamento do programa de privacidade. Eles podem ser agrupados em três categorias.

1. Princípios e padrões

- Direito dos Titulares – notificar, escolher, consentir e acesso a dados pessoais;
- Controle de Informação – segurança e qualidade de informação;
- Ciclo da Informação – coleta, uso, retenção e divulgação

2. Leis, regulações e programas

- Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation – GDPR*), HIPPA, Canadian PIPEDA, entre outros;

3. Gerenciamento do Programa de Privacidade

- Privacidade desde a concepção (*Privacy by Design - PbD*);
- Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology – NIST*)
- Agência Europeia para a Segurança das Redes e da Informação (*European Union Agency for Network and Information Security – ENISA*);

As questões mais frequentes nos frameworks são:

- Existe privacidade?
- Os riscos de privacidade são definidos e identificados adequadamente na organização?
- A organização tem atribuído responsabilidade e obrigações pelo gerenciamento de privacidade?
- A organização entende sobre incidentes no gerenciamento de privacidade?
- A organização realiza monitoramento no gerenciamento de privacidade?
- Os empregados estão devidamente treinados?
- A organização segue as boas práticas de sua indústria tais como inventários de dados, gerenciamento de riscos e relatório de impacto à privacidade (RIP)?
- A organização possui um plano de resposta a incidente?
- A organização faz as comunicações de privacidade e atualiza o material quando necessário?
- A organização faz uso de uma linguagem comum para atender e gerenciar os riscos de cibersegurança no negócio e suas necessidades?

D. Desenvolver a estratégia de privacidade

Essencialmente, a estratégia de privacidade refere-se a abordagem adotada pela organização quanto à comunicação e suporte frente ao programa de privacidade, ou seja, os dados pessoais podem ser coletados e utilizado por uma organização caso haja uma proteção adequada.

Importante ressaltar que nenhuma solução mitigará todos os riscos de privacidade, da mesma maneira não existe uma receita que englobe todas as estratégias.

Adoção de estratégias de privacidade resultam em benefícios positivos enquanto vem crescendo a conscientização sobre a importância da proteção de dados pessoais e os impactos financeiros quanto uma gestão inadequada.

Convencer os níveis apropriados quanto essa boa prática ainda é um desafio, pois a construção de uma estratégia de privacidade significa a mudança do

mindset e a perspectiva de uma organização. Abaixo algumas frentes a serem consideradas na estratégia:

- Toda organização em suas funções deve estar comprometida em proteger os dados pessoais em todo seu ciclo de vida;
- a gestão deve aprovar o financiamento quanto aos recursos, equipamentos, tecnologias, entre outros para devida execução das atividades do time de privacidade;
- a gestão deve suportar as iniciativas relativas à privacidade através de treinamentos e ciência, responsabilizando os colaboradores quanto o comprometimento e cumprimento das políticas e procedimentos de privacidade;
- A área de vendas deve proteger os dados de seus contatos comerciais;
- Desenvolvedores e engenheiros de novos produtos, serviços, entre outros devem incorporar um controle de segurança efetivo, criar websites seguros, bem como soluções que exijam coletas ou uso apenas de dados necessários para atingimento da finalidade;
- Toda organização deve ter conhecimento e empregar boas práticas para proteção de dados pessoais;

Um dos maiores desafios na implementação de um programa de privacidade e obtenção do suporte necessário para definição da estratégia se encontra no convencimento ou consenso dos membros da organização. Dessa maneira a construção e a obtenção desses consensos é uma obrigação.

O primeiro passo e mais importante está na condução de conversas/ entrevistas informais e individuais com executivos da organização que tem responsabilidades na gestão de dados e/ou segurança, riscos, *compliance* ou decisões legais. Além disso, parceiros internos como recursos humanos, jurídico, segurança da informação, marketing, gestão de riscos e TI devem também ser incluídos nessas conversas.

Com isso, deve ser escolhido um "patrocinador" do programa de privacidade, ou seja, uma pessoa que entende a importância da privacidade e age em defesa do programa. Essa pessoa tem que ser experiente dentro da organização, respeitado pelos colegas de trabalho, bem como acesso aos responsáveis para definição e concessão do budget.

Workshops sobre privacidade devem ser conduzidos, pois não se pode presumir que todos da organização se encontram no mesmo nível de conhecimento e conscientização sobre as normas vigentes e/ou complexidade envolvida.

E. Estruturar um time de privacidade

Por fim, a estruturação do grupo ou time de privacidade que deve estar alinhado com os objetivos de negócio e da organização. Basicamente, essa etapa alinha a governança de privacidade com estratégia da organização.

F. Modelo de Governança

Em relação aos modelos de governança, importante destacar que não existe uma estrutura padrão, dependerá do formato da organização, tipo de indústria ou se essa governança estará dentro da guarda-chuva de TI (tecnologia de informação) ou jurídico, no entanto, independente do modelo adotado, algumas condições precisam ser consideradas:

- Envolvimento da alta liderança;
- Envolvimento dos stakeholders;
- Desenvolvimento de parcerias internas;
- Estabelecer flexibilidade;
- Alavancar comunicações;
- Alavancar colaborações;

G. Estabelecer um modelo organizacional com estrutura de responsabilidade e reporte

Um modelo geral de privacidade da organização deve considerar em sua estrutura as estratégias, operações e gestão de responsabilidades e reporte. Nessa estrutura, independentemente do tamanho da organização algumas funções ou papéis devem ser considerados, tais como:

- CPO – *Chief Privacy Officer*;
- Gerente de Privacidade;
- Analistas de Privacidade;
- Líderes de Privacidade nas linhas de negócios;
- Primeira linha de resposta (por exemplo resposta a incidente);
- Encarregado de Proteção de Dados ou DPO – *Data Protection Officer*

As organizações podem usar diferentes tipos de estruturas, cuja inclusão de princípios permite a manutenção e desenvolvimento de processos necessários para se atingir sua eficiência. Para isso alguns pontos devem ser destacados:

- **Hierarquia** – a autoridade da gerência sênior, líderes e o time executivo para estabelecer a trilha de responsabilidade;
- **Definições de papéis/funções** – definição clara quanto às responsabilidades para estabelecimento de expectativas e desempenhos individuais;
- **Avaliação dos resultados** – métodos para determinar as forças, oportunidades, fraquezas e ameaças, corrigindo o que for necessário;
- **Alteração da estrutura organizacional** - capacidade de permanecer dinâmico e alterar quando necessário para atingimento de objetivos, adoção de novas tecnologias ou reagir aos concorrentes;

Definir uma abordagem de governança de privacidade apropriada é complexo e desafiante, mas quando adotada e implementada, assegurará a organização

quanto à conformidade com as obrigações legais, em linha com os objetivos do negócio que devem estar suportados por todos os níveis da organização.

❖ CONSIDERAÇÕES FINAIS

Angela Maria Cosso

Chegamos ao final desta obra escrita por tantas mãos de pessoas com as mais diversas experiências, o que dá a ela o colorido da multidisciplinaridade que é característica fundamental para o sucesso do processo de adequação à LGPD.

Esperamos ter acrescentado um pouco de luz ao caminho obscuro que tem se mostrado o mundo da proteção de dados. Desejamos que este trabalho seja útil tanto para profissionais que atuam na área de Privacidade e Proteção de dados quanto para as organizações que precisam compreender o que é essa lei que traz tantas novas obrigações e tantos novos conceitos.

Por fim, agradecemos a cada pessoa que doou tempo e conhecimento para compor esta obra, bem como a cada leitor que chegou até aqui.

Ressaltamos que em se tratando de Proteção de Dados nenhuma obra pode ser considerada acabada e que a realidade tem nos mostrado que estamos apenas iniciando um longo caminho.

Aqui na forma de ebook deixamos nossa contribuição.

ANEXO 1 - DEFINIÇÕES/GLOSSÁRIO

Dayane Caroline Costa & Remilina Yun (Remi)

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

Agentes de tratamento - controlador e operador.

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 de Proteção de Dados (ANPD) - é órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD;

Bases Legais para Tratamento – trata-se de normativos jurídicos que autorizam o tratamento de dados pessoais;

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;

Consentimento do Titular dos Dados Pessoais - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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 – dados pessoais de crianças e adolescentes os quais apenas podem ser tratados mediante 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 e operador, 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 objetivo do 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;

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.

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)** - ou avaliação de impactos sobre privacidade com o objetivo de identificar e minimizar os riscos relativos à privacidade. Este diagnóstico 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;

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

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

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

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;

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;

ANEXO 2 - RELAÇÃO DE NORMAS RELACIONADAS À PROTEÇÃO DE DADOS

Remilina Yun (Remi)

- Constituição Federal de 1988;
- Lei 7.232/84: Dispõe sobre a Política Nacional de Informática (art. 2º, VIII);
- Lei 8.078/90: Código de Defesa do Consumidor;
- Lei 12.527/2011: Lei de acesso à informação (Art. 4º IV e Art. 31);
- Lei 12.737/2012: Crime de invasão de dispositivos informáticos (Lei Carolina Dieckmann);
- Lei 12.965/2014: Marco Civil da Internet;
- Lei 9.296/96: Lei de Interceptação Telefônica, Telemática e Informática;
- Lei 9.472/97: Lei Geral de Telecomunicações (Art. 3º, IX);
- Lei 9.983/2000: Crime de inserção de dados falsos em sistemas de informações da administração pública;
- Lei 10.703/2003: Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências;
- Lei 12.414/2011: Disciplinou o cadastro positivo e certos aspectos sobre proteção de dados pessoais no ambiente creditício (julgamento STJ);
- Decreto 3.505/2000: Política de Segurança da Informação da Administração Pública Federal;
- Decreto 6.135/2007: Dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal;
- Decreto 6.523/2008: Regulamenta o serviço de SAC;
- Decreto 7962/2013: Regulamenta comércio eletrônico;
- Decreto 8.771/2016: Regulamentou o Marco Civil da Internet;
- Decreto 8.777/2016: Institui a Política de Dados Abertos do Poder Executivo federal.
- Resolução CFM Nº 1.821/07: Dispõe sobre prontuário eletrônico e pro. de dados médicos;

- Portaria nº 5/2002 da SDE/MJ: Tornou abusiva cláusulas em contratos de consumo que autorizam o envio de dados pessoais sem o consentimento prévio;
- ISO 27001 - padrão para sistema de gestão da segurança da informação
- ISO 27701 - sistema de gerenciamento de informações de privacidade (PIMS - *privacy information management system*)
- ISO 31000 - gestão de riscos
- COBIT - é framework de boas práticas para a governança de tecnologia de informação (TI).
- IBGC - Instituto Brasileiro de Governança Corporativa
- COSO ERM - Gerenciamento de Riscos Corporativos

ANEXO 3 - MAPEAMENTO DOS PRINCIPAIS ARTIGOS DA LGPD

Remilina Yun (Remi)

OBRIGAÇÕES	LGPD
Nomear um encarregado de proteção de dados em um papel de supervisão independente	Artigo 41
Manter um inventário de dados pessoais	Artigo 37
Manter registros do mecanismo de transferência usado para fluxos de dados (por exemplo, cláusulas padrões, normas corporativas globais, aprovação de reguladores)	Artigo 33
Uso das normas corporativas globais *(Binding Corpore Rule – BCR)* como um mecanismo de transferência de dados	Artigo 33
Uso da avaliação do nível de proteção de dados pela ANPD como um mecanismo de transferência de dados	Artigo 33, 36
Manter uma política de privacidade de dados	Artigo 6, 14, 15, 50
Bases Legais para o processamento de dados pessoais	Artigo 7, 10, 11, 14
Manter políticas / procedimentos para coleta e uso de dados pessoais sensíveis (incluindo dados biométricos)	Artigo 11
Manter políticas / procedimentos para coleta e uso de dados pessoais de crianças e adolescentes	Artigo 14
Manter políticas / procedimentos para manter a qualidade dos dados	Artigo 6
Manter políticas / procedimentos para revisar o processamento conduzido total ou parcialmente por meios automatizados	Artigo 20
Manter políticas / procedimentos para obter consentimento válido	Artigo 8

Integrar a privacidade de dados nas práticas de retenção de registros	Artigo 16
Integrar a privacidade de dados em práticas de pesquisa (por exemplo, científico e pesquisa histórica)	Artigo 13
Realizar treinamento quanto à proteção de dados pessoais	Artigo 41, 50
Integrar o risco de privacidade de dados em avaliações de risco de segurança	Artigo 50
Integrar privacidade de dados em uma política de segurança da informação	Artigo 6, 46, 49
Manter medidas técnicas de segurança (por exemplo, acessos não autorizados, firewalls, monitoramento)	Artigo 46
Manter os requisitos de privacidade de dados para terceiros (por exemplo, clientes, fornecedores, operadores, afiliados)	Artigo 39
Realizar a devida diligência em torno da privacidade dos dados e postura de segurança de fornecedores / operadores	Artigo 39
Manter um aviso de privacidade de dados que detalha as práticas de tratamento de dados pessoais para a organização	Artigo 6, 7, 9, 14
Fornecer aviso de privacidade de dados em todos os pontos onde os dados são coletados	Artigo 9, 14
Manter procedimentos para resolver reclamações	Artigo 50
Manter procedimentos para responder a pedidos de acesso a dados pessoais	Artigo 6, 18, 19
Manter procedimentos para responder a solicitações e/ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais	Artigo 18

Manter procedimentos para responder a solicitações quanto aos direitos do titular dos dados pessoais	Artigo 8(§5), 18, 20
Integrar a Privacy by Design no desenvolvimento de sistema e produto	Artigo 46
Conduzir RIPD para novos programas, sistemas, processos	Artigo 38
Manter um plano de resposta a incidentes / violações de privacidade de dados	Artigo 48, 50
Manter uma notificação de violação (para titulares de dados) e protocolo de comunicação (para reguladores, agências de crédito, aplicação da lei)	Artigo 48
Realizar auto avaliação quanto ao gerenciamento de privacidade	Artigo 50
Realizar auditorias internas do programa de privacidade	Artigo 50
Envolver um terceiro para realizar auditorias / avaliações	Artigo 50
Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de contas	Artigo 6, 50
Identificar os requisitos de conformidade de privacidade em andamento, por exemplo, lei, jurisprudência, códigos, etc.	Artigo 50

ANEXO 4 – PERGUNTAS & RESPOSTAS

O que é a Lei Geral de Proteção de Dados Pessoais - LGPD?

É a Lei nº. 13.709, de 14 de agosto de 2018 que dispõe sobre a proteção de dados pessoais e altera o marco civil da internet.

Quando a LGPD entrará em vigor?

Em 16 de agosto de 2020.

Quais setores serão impactadas pela LGPD?

Todos os setores da economia brasileira, desde as pequenas até as grandes organizações, uma vez que ela se refere ao tratamento de dados pessoais, inclusive nos meios digitais por pessoa natural ou jurídica.

Quem é o titular de dados pessoais?

É a pessoa natural (pessoa física) a quem se referem os dados pessoais que são objeto de tratamento;

O que é dado pessoal?

Qualquer informação, de qualquer natureza relativa a uma pessoa singular identificada ou identificável, ou seja, o titular dos dados. Por exemplo: *nome, CPF, e-mail, endereço, data de nascimento, hábito de consumo, geolocalização, entre outros.*

E 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.*

Quem é o controlador?

A pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Em outras palavras, toda pessoa física ou jurídica que recolha informações pessoais é considerada um controlador.

Quem é o operador?

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

Quem está submetido à LGPD?

Qualquer operação de tratamento realizado, desde que:

- a operação de tratamento **seja realizada no território nacional;**
- a atividade de tratamento tenha por **objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;** ou
- os dados pessoais objeto do tratamento **tenham sido coletados no território nacional**.

Em que situações/ tratamentos a LGPD não será aplicada?

- realizado por pessoa natural *para fins exclusivamente particulares e não econômicos;*
- realizado para fins exclusivamente: *jornalístico e artísticos, ou acadêmicos;*
- realizado para fins exclusivos de: *segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais, ou*
- 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 nesta Lei.

5

Qual o conceito de tratamento de dados?

Tratamento é 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;*

Quais são as finalidades a serem considerados no momento do tratamento?

O tratamento de dados pessoais coletados deve apresentar propósitos:

8

Quais são os 10 princípios da LGPD?

1) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

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

3) 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;

4) 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;

5) 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;

6) 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;

7) 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;

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

9) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

10) 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.

Quais são os direitos dos titulares dos dados pessoais?

O titular dos dados pessoais tem direitos diversos junto ao controlador em relação aos seus dados, a qualquer momento e mediante requisição:

- ✓ **CONFIRMAÇÃO** da existência de tratamento
- ✓ **ACESSO** aos dados
- ✓ **CORREÇÃO** de dados incompletos, inexatos ou desatualizados
- ✓ **ANONIMIZAÇÃO**, bloqueio ou eliminação de dados
- ✓ **ELIMINAÇÃO** dos dados pessoais tratados com o consentimento
- ✓ **PORTABILIDADE** dos dados pessoais
- ✓ **REVOGAÇÃO** do consentimento
- ✓ Ciência sobre o **COMPARTILHAMENTO** dos dados realizado pelo controlador
- ✓ **REVISÃO** das decisões automatizadas de dados pessoais
- ✓ **INFORMAÇÃO** sobre a opção de não consentir e sobre as consequências da negativa
- ✓ **RECLAMAR** junto à ANPD
- ✓ **OPOSIÇÃO** ao tratamento, se irregular

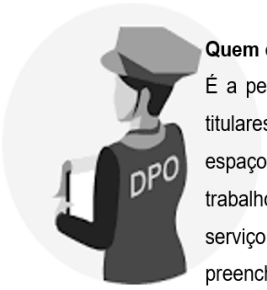
Quais são as bases legais para o tratamento de dados pessoas a luz da LGPD?

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

1. mediante o fornecimento de **consentimento** pelo titular;
2. para o **cumprimento de obrigação legal ou regulatória** pelo controlador;
3. pela administração pública, para o tratamento e uso compartilhado de dados necessários à **execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
4. para a realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;
5. 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;
6. para o **exercício regular de direitos** em processo judicial, administrativo ou arbitral;
7. para a **proteção da vida** ou da incolumidade física do titular ou de terceiro;
8. para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
9. quando necessário para atender aos **interesses legítimos do controlador ou de terceiro**, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
10. para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente.

Quais penalidades poderão ser impostas frente aos tratamentos de dados em desconformidade com a LGPD?

- **ADVERTÊNCIA**, com indicação de prazo para adoção de medidas corretivas;
- **MULTA SIMPLES**, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, **limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;**
- **MULTA DIÁRIA**, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- **PUBLICIZAÇÃO DA INFRAÇÃO** após devidamente apurada e confirmada a sua ocorrência;
- **BLOQUEIO** dos dados pessoais a que se refere a infração até a sua regularização;
- **ELIMINAÇÃO** dos dados pessoais a que se refere a infração;
- **SUSPENSÃO TOTAL ou PARCIAL** do banco de dados por até 6 (seis) meses, prorrogável por igual período, até a regularização;
- **PROIBIÇÃO TOTAL ou PARCIAL** das atividades relacionadas a tratamento de dados.



Quem é o encarregado de proteção de dados ou *Data Protection Officer* (DPO)?

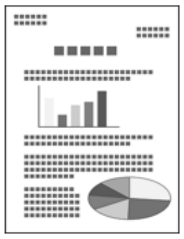
É a pessoa indicada pelo controlador e operador para atuar como canal de comunicação junto aos titulares dos dados e a ANPD autoridade nacional. Não precisa ser uma pessoa natural, abrindo espaço, desta forma, para a possibilidade de indicação de pessoas jurídicas, ou comitês, ou grupos de trabalho, que podem exercer tais funções. Ainda, deixa clara a possibilidade de terceirização de tal serviço, e não impõe limitações para que esta pessoa, ou time, estar em território nacional, desde que preenchidos os requisitos para se qualificar como um encarregado.

Principais responsabilidades:

- ✓ Receber reclamações e comunicações dos titulares dos dados pessoais, prestar esclarecimentos e orientar sobre as providências;
- ✓ Receber comunicações de órgãos reguladores e adotar as providências que couberem;
- ✓ Orientar os funcionários envolvidos no tratamento de dados pessoais dos usuários;
- ✓ Orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais dos usuários;
- ✓ Manter registros de todas as práticas de tratamento de dados pessoais conduzidas pela empresa, incluindo o propósito de todas as atividades desenvolvidas.

O que é a Autoridade Nacional de Proteção de Dados - ANPD?

É órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD. Ainda, poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca da segurança.



O que é o Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) ou *Data Protection Impact Assessment* (DPIA)?

É a 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;

Quais são os benefícios quanto à adequação?

- **Melhora no relacionamento com cliente através da confiabilidade e respeito à privacidade**
- **Aumento da segurança jurídica para atuar através de dados pessoais**
- **Segurança cibernética aprimorada e fluxos de trabalhos mais conscientes**
- **Valorização do marketing e aumento de sua produtividade**

BIBLIOGRAFIA

1. Comparing privacy laws: GDPR v. LGPD, DataGuidance by OneTrust e Baptista Luz Advogados

2. Guia PMBOK 5a edição - EUA: Project Mangmente Institute, 2013.

3. O que é e como agir diante de um Data Breach ou Incidente de Segurança, Baptista Luz Advogados

4. https://www.jota.info/opiniao-e-analise/artigos/das-etapas-de-elaboracao-de-um-dpia-27042019

5. Handbook on European Data Protection Law. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

6. Brazil – LGPD Accountability Handbook - NYMITY

7. Privacy Program Management 2º Edition – IAPP Publication - Russell Densmore, CIPP/E, CIPP/US, CIPM, CIPT, FIP