A essa altura, você provavelmente já ouviu falar sobre a Lei Geral de Proteção de Dados (LGPD). Aprovada em agosto de 2018 e em vigor desde agosto de 2020, com sanções administrativas sendo aplicadas a partir de agosto de 2021, a LGPD é a resposta brasileira a um movimento global de países que reconheceram a necessidade de estabelecer novas relações em uma sociedade cada vez mais movida por dados (data-driven society). Esse movimento começou há décadas em outros países e blocos econômicos e ganhou força em 2018, com a vigência da nova regulação de proteção de dados da União Europeia - a General Data Protection Regulation (GDPR).

Agora, o Brasil não só superou o atraso nessa pauta, como soube se valer desse atraso, aprovando uma regulação equilibrada, que conjuga a garantia de direitos com o fomento à inovação. A LGPD, assim como a GDPR, tem a função de proteger a privacidade e outras liberdades fundamentais dos cidadãos, ao mesmo tempo em que promove o estímulo a modelos de negócios e políticas públicas que são viabilizadas através do tratamento de dados pessoais e/ou a monetização dessas informações.

Apesar de uma nova regulação causar receios em relação aos custos de conformidade (o "**Custo Brasil**"), a LGPD representa uma janela de oportunidades. Primeiro, porque as organizações terão que colocar "ordem na casa", na medida em que terão que conhecer melhor todas as suas bases de dados e lhes atribuir uma finalidade específica. É um exercício que poderá trazer insights para se repensar o próprio modelo de negócio e até mesmo para lançar novos produtos e serviços. Segundo, a adequação à legislação de dados pessoais pode melhorar a reputação da empresa, na medida em que o tratamento adequado dos dados pode ser explorado no seu plano de comunicação para reforçar a confiança com o titular da informação. Terceiro, porque a lei traz uma série de exigências relacionadas à segurança da informação no sentido não só de prevenir o "vazamento" de dados, mas, também, de remediá-los da forma mais eficientes caso ocorram. Certamente, organizando esses quesitos, será mais fácil identificar e remediar qualquer tipo de incidente. Tratam-se de medidas cujo saldo final pode **agregar valor e competitividade** a uma organização.

A partir de agosto de 2020, todo negócio que fizer o uso de dados pessoais já deveria estar em conformidade com as novas premissas. Por isso, o processo de adequação caso não tenha sido executado precisa se iniciar agora. Para te ajudar com isso, este material faz um sobrevoo sobre a LGPD, explicando quais são seus objetivos, quais são os seus pilares, as penalidades envolvidas e o que você, como gestor em uma empresa, precisa fazer para se adequar às exigências e canalizá-las como **um benefício** para sua respectiva organização.

Acompanhe conosco **e boa leitura!**

LGPD
para quê?

Cada vez mais, organizações e iniciativas, aprendem a agregar valor e otimizar as suas atividades a partir do uso de dados pessoais do seu público alvo. Em muitos casos, isso implica, repetindo um mantra ecoado há décadas, na "melhoria da experiência" de usuários-clientes, que passam a contar com serviços mais personalizados e oferecidos em momentos mais oportunos. Por outro lado, preocupações emergem à medida que as pessoas passam a ser enxergadas e julgadas através dos seus dados pessoais. Isso porque esses dados podem não só revelar muito sobre a vida de seus titulares, mas também embasar decisões a serem tomadas a seu respeito - como conferir ou não crédito, conseguir ou não um emprego, aprovar ou não a contratação de um plano de saúde, etc.

Nesse contexto, a LGPD estabelece o **direito** de cada pessoa ter o controle dos seus dados pessoais, ao mesmo tempo em que procura oferecer aos responsáveis pelos tratamentos de dados a **segurança jurídica** necessária para que possam investir em suas atividades com a tranquilidade de que estão conduzindo uma atividade legal.

A quem se aplica? LGPD

Como o próprio nome diz, a LGPD é uma lei "geral", ou seja, ela não se restringe a um único setor. Não atinge somente negócios que exercem atividade na internet, mas também os setores mais tradicionais da economia (como o de saúde, automobilístico, energia elétrica, varejo, etc.).

Na verdade, a LGPD aplica-se sempre que for feito algum tipo de tratamento de dados pessoais, dentro ou fora da internet, utilizando ou não de meios automatizados. Dessa forma, aplica-se às atividades online e offline, tanto do setor público como do privado.

Considera-se tratamento **toda operação realizada com dados pessoais,** o que inclui:

- **coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, entre outros.**

Nesse sentido, considerando que a LGPD se aplica, em regra, a qualquer uma das atividades acima descritas, a organização como um todo terá que se preparar, desde o departamento de recursos humanos ao time de marketing.

Além disso, a LGPD, a exemplo do que fez a GDPR europeia, estabeleceu um vínculo de solidariedade entre quem é uma espécie de gestor da cadeia de tratamento de dados – o controlador – e quem é o seu terceirizado, parceiro comercial – o operador. Assim, se houver um dano causado pelo terceirizado, o gestor poderá ser acionado diretamente a repará-lo. Nesse sentido, obriga-se, diretamente ou indiretamente, que controladores contratem apenas operadores que estejam em conformidade com as regras de proteção de dados pessoais. Com isso, os próprios atores da cadeia de tratamento de dados mais do que fiscalizar uns aos outros, tendem a escantear aqueles não em conformidade. Portanto, quem estiver em conformidade passa a ter uma vantagem competitiva frente aos seus pares retardatários, o que pode se traduzir, inclusive, na valorização dos seus serviços e produtos.

Por fim, é importante dizer que a lei deverá se aplicar não somente aos tratamentos de dados pessoais dentro do território brasileiro, mas também aos que são realizados fora do país, quando:

ROCKER COMPUTER®

•Os dados pessoais forem coletados no Brasil;

•os dados forem relacionados a indivíduos localizados no território brasileiro;

•o tratamento tiver por objetivo a oferta de produtos e/ou serviços ao público brasileiro;

Por todos esses motivos, o seu impacto regulatório será maior do que já experimentamos com o Código de Defesa do Consumidor na década de 90. É uma regulação que vai muito além da relação do setor privado com seus consumidores na "ponta", mas, também, que abraça seus vínculos com parceiros comerciais, com seus colaboradores e, por fim, com a administração pública e seus concessionários que lidam com os dados pessoais dos cidadãos

Mas o que são dados pessoais?

Em uma regulação de proteção de dados, o conceito de dado pessoal tem um papel central, na medida em que define a abrangência desta lei. Tudo que for entendido como dado pessoal deverá ser manipula- do de acordo com as regras da LGPD.

O conceito adotado pela lei é bastante amplo: dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável. Assim, dados pessoais são toda e qualquer informação que iden- tifique uma pessoa (como o nome, RG, CPF ou a bi- ometria) ou que permita a sua identificação, por estabelecerem um vínculo indireto com ela (como apelidos, fotos, endereços de e-mail, endereços residenciais e endereços de IP).

Para alguns desses dados pessoais, a lei reserva um regramento ainda mais cuidadoso. Isso porque en- tende que esses podem ser usados com fins dis- criminatórios. Nesse sentido, dados que revelem a origem racial ou étnica, a convicção religiosa, opinião política ou mesmo dados referentes à saúde ou à vida sexual do seu titular, entre outros elencados na lei, são chamados de dados pessoais sensíveis.

Como saber se a minha empresa pode ou não realizar determinados tratamentos de dados?

Levando sempre em conta os princípios e direitos previstos na LGPD, as organizações públicas e privadas só poderão tratar dados pessoais quando identificarem uma base legal que justifique esse tratamento. Dessa forma, a partir da intenção de se realizar um tratamento, é preciso buscar na lei a fundamentação mais adequada para que esse tratamento seja legal.

Na linha da GDPR, a LGPD reconheceu que a "regra de ouro" do consentimento não poderia mais ser a única a legitimar um tratamento de dados. Assim, em determinados casos, outras bases legais como o cumprimento de uma obrigação legal ou obrigação contratual serão mais adequadas para permitir o tratamento, e não será necessário requerer o consentimento do titular. Entre as 10 (dez) bases legais previstas na lei, constam também as hipóteses de exercício regular de direitos, proteção da vida, formulação de políticas públicas, proteção ao crédito e da incolumidade física do titular.

Há, em especial, uma base legal que tem sido apontada como a mais flexível: o legítimo interesse. É uma hipótese que não constava das primeiras versões do anteprojeto de lei, a qual foi incluída com o propósito de não engessar a inovação, servindo de "apoio e promoção das atividades do controlador". Contudo, o bônus do legítimo interesse vem acompanhado de um ônus, que é a documentação dessa atividade de tratamento de dados que deve passar no teste de 4 fases que a própria LGPD propõe, com respostas afirmativas para as **seguintes perguntas:**

1°

Existe uma finalidade legítima para esse tratamento, baseada em uma situação concreta?

A finalidade não deve ser proibida por lei e não deve ser especulativa, devendo ser articulada da forma mais detalhada possível.

2°

Está sendo tratado o mínimo de dados necessário para atingir os fins propostos?

Deve-se refletir se com menos dados eu ainda consigo alcançar meu objetivo: "menos é mais".

3°

A ação proposta é compatível com a legítima expectativa do titular em relação ao tratamento dos seus dados?

É necessário um exercício de empatia, pelo qual a organização se coloca no lugar da pessoa cujos dados estão sendo acessados e reflete como ela se sentiria caso suas informações fossem manipuladas de determinada forma.

4°

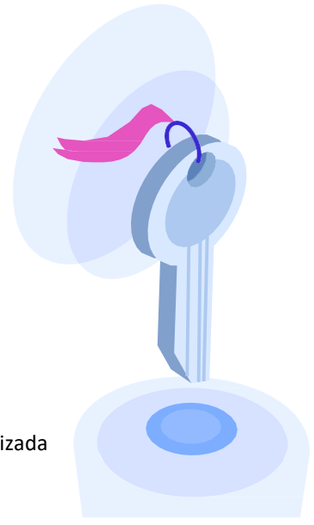
Serão implementados mecanismos de mitigação de riscos, bem como de garantias de transparência e mecanismos de oposição para o titular?

Um dos principais pontos a ser observado é conferir visibilidade ao tratamento de dados realizado com essa base legal, viabilizando que o titular manifeste sua eventual discordância.

É importante destacar, no entanto, que a base legal do legítimo interesse não pode ser utilizada para legitimar o tratamento de dados sensíveis. Outros pontos de destaque da lei que precisam ser levados em consideração são:

- Os dados de crianças (até 11 anos) só poderão ser tratados com consentimento dos pais ou responsáveis legais;

- Se houver mudança de finalidade ou a intenção de realizar um novo tratamento para os mesmos dados, deverá ser identificada a base legal mais adequada a autorizar esse tratamento específico, que pode ou não coincidir com a base legal que autorizou o primeiro tratamento.



Como deve se dar o **tratamento de dados**?

A privacidade dos usuários deve ser considerada pela empresa desde a fase de concepção de um serviço ou produto até a sua execução (privacy by design). De maneira geral, só se pode tratar dados se isso servir a uma finalidade na prestação de serviços e desde que eles sejam necessários e adequados para esse fim. Os dados devem ser corretos e atualizados e os titulares devem ter livre acesso a eles, bem como a empresa deve ter uma política mecanismos de transparência, no sentido de que o titular de dados saiba exatamente como seus dados estão sendo tratados e utilizados. Por fim, a empresa deve garantir a segurança dos dados, prevenindo vulnerabilidades, bem como se responsabilizar por eles e prestar contas sobre suas ações.

Além dos princípios mencionados, os direitos dos titulares também devem ser levados em conta e instrumentalizados pelos controladores e operadores. Entre as garantias que a lei prevê, estão as de:

- pedir a eliminação, bloqueio ou anomização (desidentificação) dos dados;

- ter seus dados armazenados de forma segura e ser avisado em caso de violações;

- acessar e modificar dados incompletos, incorretos e desatualizados;

- pedir a portabilidade dos dados para outros fornecedores;
- saber onde, por quanto tempo e por que os dados são usados;

- revogar o consentimento de uso das informações e se opor ao tratamento de dados tratados com base em outras bases legais (e.g., legítimo interesse);

- obter informações sobre as entidades com quem o controlador compartilha os dados.

Entrando em ação

Para iniciar um projeto de conformidade é importante estar aberto a necessidade de criar uma nova cultura de privacidade na sua empresa, alinhada com os princípios da LGPD, considerando sobre tudo, a possibilidade de realizar treinamentos para os colaboradores. Tão importante quanto soluções tecnológicas, é o elemento humano para que, holisticamente, a organização tenha uma mudança de mentalidade.

De maneira geral, será preciso entender a própria organização e os tratamentos de dados envolvidos em suas atividades para avaliar os riscos envolvidos. Em seguida, será preciso estabelecer uma estratégia de gerenciamento desses riscos. Trata-se, portanto, de um tripé: cognição, mensuração e controle de riscos.

Assim, tendo em mente todo o conjunto de normas que se aplica às atividades desenvolvidas pela sua empresa, será importante criar um programa de governança de privacidade, que deverá envolver toda a instituição.

É recomendável que se estabeleça um comitê interno de privacidade, que precisa ser escalonável para atender as diferentes áreas da empresa e os respectivos dados pessoais tratados. Nesse sentido, a diretoria, a gerência, o jurídico/complicance, as áreas de tecnologia da informação, recursos humanos, marketing, etc. terão diferentes atribuições para a execução de um trabalho coletivo. Enquanto o jurídico precisará desenvolver atividades como a revisão dos contratos, políticas de proteção de dados e códigos de conduta. O RH, por exemplo, deve colaborar com a implementação do programa em relação aos dados dos funcionários e alinhar com eles suas expectativas de privacidade.

A seguir, apresentaremos uma possível metodologia a ser adotada para dar início a um processo de conformidade:

1° Fazer um primeiro **inventário dos dados** da empresa **(data mapping)**

O primeiro passo é saber o que você tem. É preciso mapear os dados pessoais em posse sua empresa, como nomes, endereços, endereços IP e outros identificadores eletrônicos, dados de geolocalização, dados de pagamento etc. Da mesma forma, precisarão ser identificados eventuais dados pessoais sensíveis ou de crianças. Será preciso entender de onde eles vêm, como a empresa os acessa, utiliza, descarta, enfim, o ciclo de vida desses dados. Esse mapeamento dos dados e de seus fluxos dentro da estrutura de processamento da empresa permitirá que se consiga enxergar eventuais pontos de desconformidade e a necessidade de readequação.

Uma vez mapeados os fluxos de dados envolvidos nas atividades da empresa, é importante apontar os funcionários relacionados ao programa de governança

2° Nomear um **encarregado**

de privacidade ou mesmo um comitê. A LGPD estabelece a necessidade de nomeação de pessoa que será o canal de comunicação entre o controlador, o operador, os titulares de dados e a Autoridade Nacional de Proteção de Dados: o encarregado. Não há a necessidade de ser uma pessoa física, podendo ser, por exemplo, o próprio Comitê Interno de Privacidade ou uma entidade externa. No entanto, em todos os casos, é necessário conhecer bem as regras de proteção, bem como desempenhar atividades importantes como coordenar as práticas educacionais e elaborar o relatório de impacto à proteção de dados pessoais.

Já com a fotografia dos dados dentro da empresa e a atribuição de responsabilidades a quem vai atuar no programa de governança de privacidade, é recomendável que se elabore um relatório de impacto à proteção de dados pessoais.

3° Elaborar **relatório(s)** de **impacto**

Elaborado com a ajuda de diferentes setores da empresa, o relatório de impacto à proteção de dados (RIPD) tem a função de documentar os três processos principais em que uma organização precisa se engajar para estar em conformidade com a lei ou sempre que inicie um novo tratamento de dados por conta de um novo produto, serviço ou revisão do seu modelo de negócio:

Entender	Avaliar os riscos	Mitigação e Gerencia- mento de riscos
A partir do mapeamento de dados (data mapping), identificar quais são os pontos de desconformidade regulatória, o que vai desde o tratamento de dados lastreado em uma base legal não apropriada até questões de segurança da informação.	Analisar o risco em relação às atividades de tratamento de dados em desconformidade com a legislação de dados, classificando-os, por exemplo, como de baixo, médio ou alto risco, bem como a sua probabilidade de concretização.	Nessa etapa, devem ser apresentadas as medidas que a organização vai empregar para estar em conformidade com a lei e diminuir as chances de incidentes com os dados.

A LGPD não define o "passo a passo" do relatório de impacto, cabendo a cada or- ganização definir o formato de documento que melhor se adeque à sua realidade. Da mesma forma, não precisa existir apenas um relatório de impacto. Muitas vezes, será mais adequado elaborar diferentes relatórios para diferentes tipos de tratamentos de dados ou mesmo para diferentes produtos ou serviços ofertados pela empresa.

Segundo a LGPD, a ANPD (Autoridade Nacional de Proteção de Dados) poderá exigir esse(s) documento(s) do controlador de dados em algumas situações, como nos casos em que uma organização realiza determinado tratamento de dados valendo-se da base legal do legítimo interesse. Dessa forma, o objetivo do legislador foi prever uma ferramenta de compliance que espelhasse o diagnóstico e prognóstico de uma organização em relação ao tratamento de seus dados, especialmente o que foi constatado, avalia do e modificado para se adequar à lei. Apesar de não ser, via de regra, um documento obrigatório, considerando os benefícios que o RIPD podetrazer, recomenda-se a sua elaboração de maneira regular, independente de determinação da ANPD. Além de ser uma ferramenta pelo qual a organização presta contas sobre o seu estado de conformidade com a legislação, é um exercício que pode trazer insights para o seu modelo de negócio e ser um gatilho de inovação da maneira com que são manipulados os dados.

Afinal, representa uma ação preventiva diante da possibilidade de futuros questionamentos por órgãos reguladores e também de alinhamento e consolidação das próprias políticas de tratamento de dados dentro da organização. Nesse sentido, recomenda-se até mesmo a sua publicação, quando possível, por gerar fiabilidade e confiança junto ao seus respectivo público-alvo.

4° Mão na massa

A partir do programa de governança elaborado, é preciso garantir que as atividades de controle e tratamento correto dos dados sejam incorporadas em todos os níveis da empresa. Isso deve incluir, em especial, o treinamento de todo o time de colaboradores e dos usuários de TI, fazendo uso, sempre que possível, de soluções tecnológicas que possam contribuir com essa adequação. Esse é um dos pontos mais críticos, sendo necessário o engajamento de toda a organização para uma efetiva mudança de mentalidade com relação ao uso de dados pessoais.

E se ocorrer um incidente com os dados?

É preciso ter em mente que as empresas estarão sempre passíveis a incidentes, por mais que se engajem no processo de adequação à LGPD e da promoção de seus valores. Existem riscos de destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso indevido a dados pessoais. Por esse motivo, a LGPD oferece ferramentas para mitigar esses incidentes.

Se ocorrer uma violação de dados, essa deverá ser comunicada a ANPD e aos titulares dos dados atingidos em um prazo razoável, o que deverá ser precisado em regulação posterior. Em relação às possíveis penalidades aplicáveis, a LGPD prevê advertências (com indicação de prazo para adoção de medidas corretivas), a necessidade de tornar pública a infração, o bloqueio dos dados pessoais envolvidos no tratamento indevido e até mesmo a eliminação desses dados. Isso sem falar nas multas, que poderão representar até 2% do faturamento da empresa limitada, com o limite de R$ 50 milhões por infração. De qualquer forma, a postura habitual da empresa em relação aos seus tratamentos de dados será levada em consideração para o estabelecimento de penalidades pela Autoridade Nacional de Proteção de Dados (ANDP). Esse é um outro motivo pelo qual é tão importante implementar um bom programa de conformidade.

ROCKER COMPUTER®