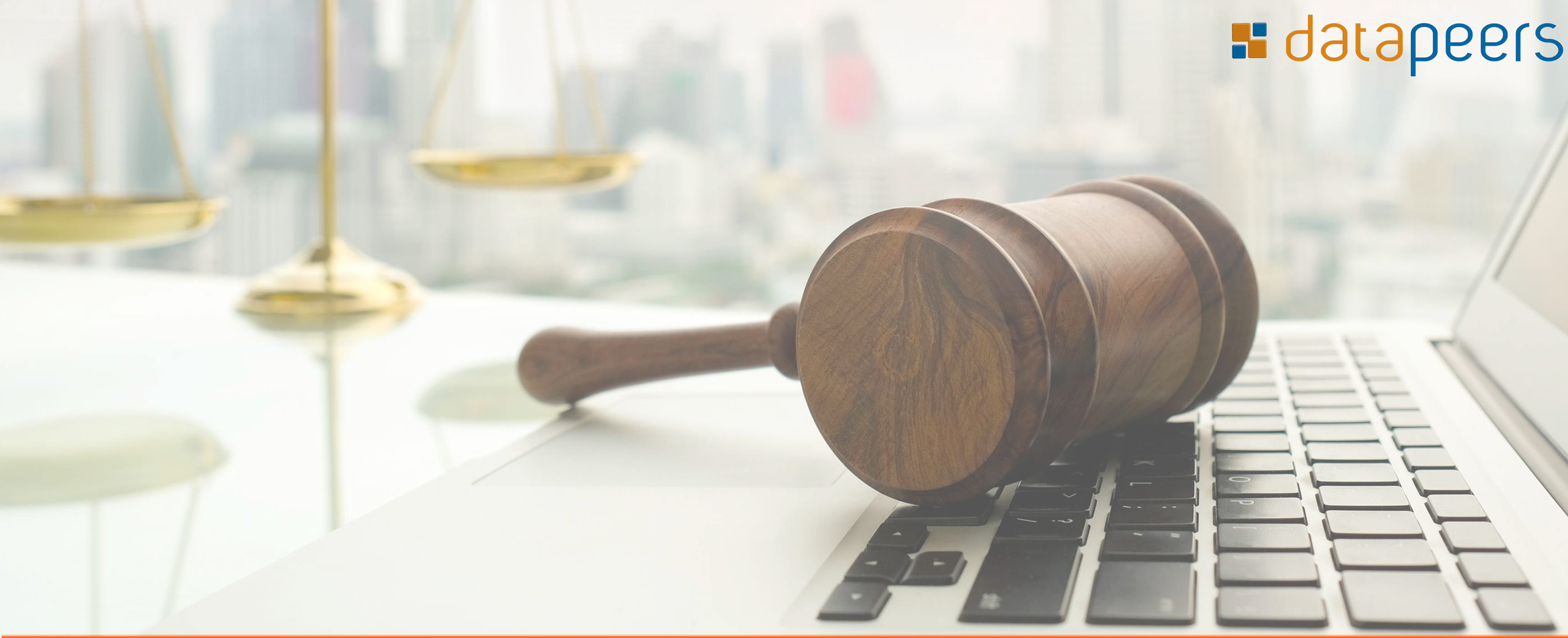

# TUDO O QUE PRECISA DE SABER

## SOBRE A NOVA LEI DE PROTEÇÃO DE DADOS BRASILEIRA

# CONTEÚDOS

- Introdução
- Linhas gerais da nova lei (LGPD)
- Princípios da nova lei
- O que vai mudar nas empresas
- Como cumprir os requisitos da LGPD

# A NECESSIDADE DE PROTEGER A INFORMAÇÃO

78%

das empresas em todo o Mundo sofreu pelo menos um ataque informático nos últimos dois anos

92%

dos ataques sofridos acontece devido a falhas de segurança internas

35%

dos ataques sofridos acontece devido a perdas de informação em dispositivos móveis

57%

das empresas não protege a sua informação com soluções de proteção dos dados

61%

de perda de produtividade em cada ataque informático

42%

de perda de receita em cada ataque informático

# INTRODUÇÃO

As empresas em todo o Mundo enfrentam ameaças crescentes de segurança e confidencialidade dos dados, o que as obriga a reavaliar as suas estratégias de gestão dos dados. Atualmente, todas as pessoas, em algum momento, fazem alguma coisa online que envolva o envio de dados pessoais, como comprar um produto, subscrever um serviço ou efetuar uma transferência bancária.

As novas tecnologias potenciam um grande número de oportunidades a nível da otimização dos recursos, mas quando são mal utilizadas podem comprometer a segurança da informação dos cidadãos. Uma das maiores preocupações de todas as empresas é a proteção da informação. Nunca antes como agora a necessidade de proteger os dados foi tão evidente.

Os cidadãos devem ter controlo sobre os respetivos dados pessoais e deve simplificar-se e clarificar-se o quadro legal dos negócios digitais. Isto porque, infelizmente, muitas vezes os dados pessoais dos usuários são capturados de forma ilícita, o que pode comprometer toda a sua privacidade. Todo este cenário potenciou a criação do Regulamento Geral de Proteção de Dados (RGPD) para a União Europeia, que entrou em vigor em maio deste ano, e agora o Brasil se prepara para receber uma nova lei muito semelhante à que já existe na Europa. Após mais de 8 anos de debates na sociedade civil, eis que chega a Lei nº 13.709/2018, a lei de proteção de dados brasileira. A legislação (LGPD) foi sancionada no dia 14 de agosto e prevê-se que entre em vigor definitivamente em fevereiro de 2020.

# LINHAS GERAIS DA NOVA LEI

A lei menciona, logo em seu **artigo 1º**, que o seu objetivo é proteger “os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

De seguida, no **artigo 2º** a lei refere seus fundamentos: privacidade, autodeterminação informativa, liberdade de expressão, de informação, de comunicação e de opinião; inviolabilidade da intimidade, da honra e da imagem, desenvolvimento econômico e tecnológico e a inovação, livre iniciativa, livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, dignidade e o exercício da cidadania pelas pessoas naturais.

O **livre desenvolvimento da personalidade, da cidadania e da dignidade** diz respeito à necessidade de saber com exatidão qual o destino dos dados pessoais colectados, uma vez que atualmente muitos desses dados são processados por diversos algoritmos que conseguem fazer diagnósticos e classificações dos usuários. Essa classificação vai ser usada para limitar as escolhas dos usuários (pois só lhes é dado a conhecer um determinado tipo de produto, por exemplo). Os seus dados pessoais podem ainda ser utilizados para uma tentativa de manipulação de suas crenças e opiniões, sobretudo no setor político.

# LINHAS GERAIS DA NOVA LEI

A lei brasileira define **dados pessoais** como toda a “informação relacionada a uma pessoa natural identificada ou identificável”. Esta nova legislação faz ainda a diferenciação de dados pessoais e **dados pessoais sensíveis**. Os dados pessoais sensíveis são aqueles dados pessoais sobre “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

O **titular dos dados** é a pessoa que a lei visa proteger e é o portador “dos dados pessoais que são objeto de tratamento”, pelo que as pessoas jurídicas de carácter coletivo ficaram de fora da alçada da nova lei: esta lei é exclusivamente para proteger as pessoas.

O conceito de **tratamento de dados** é muito importante nesta legislação e é definido como “toda a 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”. Este contexto é muito amplo e aplica-se a todas as operações de tratamento de dados realizadas por pessoa individual ou coletiva, tanto no setor público como no setor privado. Para que a lei se aplique, esse tratamento de dados deve ser realizado em território brasileiro. Nos casos de cidadãos estrangeiros, os dados pessoais estão sujeitos à nova lei quando são recolhidos no Brasil e quando o seu tratamento tem como objetivo o fornecimento de bens ou serviços no Brasil.

# LINHAS GERAIS DA NOVA LEI

Existem, contudo, **exceções para o tratamento dos dados**. Estão excluídos da nova lei os tratamentos de dados: (a) realizado por pessoas individuais para finalidades exclusivamente particulares e não económicas; (b) para fins exclusivamente jornalísticos, artísticos e académicos; (c) para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação; (d) provenientes do estrangeiro e que não são objeto de comunicação, uso partilhado 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.

# PRINCÍPIOS DA NOVA LEI

A parte inicial da legislação contém os princípios que devem orientar o tratamento de dados. Estes princípios são muito importantes para que se consiga aplicar os novos requisitos da nova lei para o tratamento de dados.

**(i) princípio da finalidade:** é descrito como “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”;

**(ii) princípio da adequação:** diz respeito à “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”;

**(iii) princípio da necessidade:** refere-se à “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”;

**(iv) princípio do livre acesso:** é a “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”;

**(v) princípio da qualidade dos dados:** é a “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento”;

# PRINCÍPIOS DA NOVA LEI

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

**(vii) princípio da segurança:** obriga à “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”;

**(viii) princípio da prevenção:** é a “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”;

**(ix) princípio da não-discriminação:** refere-se à “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”;

**(x) princípio da responsabilização e prestação de contas:** obriga a uma “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.”

# O QUE VAI MUDAR NAS EMPRESAS

### Obrigatoriedade de eliminar os dados quando exigido pelo usuário

Os cidadãos vão poder exigir às empresas que eliminem os respetivos dados pessoais, sempre que haja solicitação por parte dos usuários. O novo regulamento permite que os dados pessoais de cada cidadão sejam destruídos por sua solicitação.

### Portabilidade dos dados

Os cidadãos poderão exigir às empresas que lhes enviem os seus dados pessoais num formato que permita que sejam enviados para outra empresa, facilitando a sua migração e tornando mais simples a mudança de prestação de serviços. Sempre que um cidadão mudar de Banco ou de prestador de serviços de televisão, não terá que fornecer novamente os seus dados pessoais, pois estes podem ser facilmente migrados de uma empresa para outra.

### Necessidade de autorização expressa do usuário

Os cidadãos terão informação total sobre o modo como as empresas tratam os seus dados, de que modo os armazenam, por quanto tempo os guardam e com quem partilham a sua informação. A nova lei aplica-se a todas as atividades que envolvam utilização de dados pessoais, incluindo tratamento pela internet.

# O QUE VAI MUDAR NAS EMPRESAS

**Obrigatoriedade de notificar em caso de violação de dados pessoais**

As empresas e as organizações têm o dever de notificar a Autoridade competente em situações que coloquem os indivíduos em risco e comunicar ao cidadão em causa todas as violações de alto risco o mais rapidamente possível, de modo a que se possam tomar as medidas adequadas. Em caso de vazamento dos dados, a empresa deverá comunicar o facto ao órgão competente (Autoridade Nacional de Proteção de Dados , órgão da administração pública indireta, ligado ao Ministério da Justiça), que será responsável por zelar, implementar e fiscalizar o cumprimento da lei, dentro de um “prazo razoável”, que será definido pelo referido órgão.

**No caso de vazamento de dados ou qualquer outra violação à lei, as multas previstas poderão chegar a 2% do faturamento, com o limite de R$ 50 milhões, podendo também implicar na suspensão das atividades da empresa**

# COMO CUMPRIR OS REQUISITOS DA LGPD

## Defina um plano

Deverá haver um plano de ação estratégico para a implementação e avaliação constante da LGPD. Todas as áreas da empresa deverão estar envolvidas e neste plano deve constar a identificação, avaliação e categorização dos dados privados que a empresa  tem armazenados.

## Aconselhamento jurídico

O aconselhamento de profissionais é essencial para que a LGPDA seja implementada de forma correta. O consultor jurídico identificará os passos já implementados e os que faltam para cumprir a LGPD. O levantamento de necessidades é muito útil caso precise de recorrer a um parceiro para fazer as alterações necessárias.

## Atualização da política de privacidade

A política de privacidade dos dados deve ser atualizada de acordo com as novas exigências da legislação. Deve ser definida uma escala de classificação e de tratamento dos dados pessoais. O departamento jurídico da empresa deve estar envolvido neste processo.

# COMO CUMPRIR OS REQUISITOS DA LGPD

### Tornar a informação mais segura

A empresa deve implementar processos que permitam detetar, reportar e resolver problemas de violação de dados pessoais, mantendo sempre presente a questão da segurança.

### Modificação dos canais de atendimento

Os procedimentos de atendimento a clientes devem ser preparados para receber todos os pedidos em conformidade com a nova lei, sejam eles online ou offline. É essencial garantir que a segurança dos dados dos cidadãos não fica comprometida.

### Garantia de cumprimento do RGPD por parte dos fornecedores

Todos os fornecedores envolvidos no processamento de dados devem cumprir os requisitos do novo RGPD. Por exemplo, ao comprar uma base de dados deverá assegurar-se que a entidade subcontratada também cumpre a nova lei.

### Mascaramento dos dados

A empresa deve garantir que os dados altamente sensíveis estão mascarados, para que não haja o risco de serem expostos e a empresa ser vítima das pesadas multas que constam no novo regulamento.

# datapeers

### Interoperabilidade
Datapeers é puramente baseado em meta-modelos e, por isso, permite o uso de vários tipos de bases de dados

### Mascaramento de dados
Oferece uma variedade de técnicas scrambling sofisticadas para proteger dados sensíveis, substituindo-os de forma irreversível por dados fictícios mas realistas

### Integridade dos dados
Deteta automaticamente dependências de dados e captura correlações ocultas

### Aumento da produtividade
Minimiza o tempo e melhora a qualidade de implementação de ambientes não produtivos

### Segurança dos dados
Proporciona a partilha de dados de forma segura através do mascaramento de dados sensíveis

### Redução de custos
Além de reduzir substancialmente os custos, o Datapeers aumenta a eficiência das equipas de TI e a agilidade de desenvolvimento das aplicações

datapeers


PHONE +351 220 101 587

OFFICE Rua Eng. Frederico Ulrich 3210, 1º andar. s. 101, 4470-605 Maia

EMAIL datapeers.info@itpeers.com

WEBSITE https://datapeers.itpeers.com/