LGPD OU LEI GERAL DE PROTEÇÃO DE DADOS

LGPD é a Lei Geral de Proteção de Dados, uma lei aprovada em agosto de 2018 no Brasil que impôs **regras sobre o tratamento de dados pessoais** e que tem como finalidade proteger o direito à liberdade, privacidade e livre desenvolvimento dos cidadãos. A lei não diz respeito apenas às informações mantidas em sistemas online, mas sua criação foi motivada pela complexidade que o tema gestão de dados ganhou na economia digital.

Afinal, estamos na Era da Informação, um período marcado pela hiperconexão e coleta contínua de uma quantidade imensa de dados o que chamamos de big data. Entre esses dados estão os dados pessoais, que, segundo a LGPD, são **quaisquer informações relacionadas à pessoa natural** identificada ou identificável. As regras da LGPD valem tanto para pessoas físicas quanto jurídicas (públicas e privadas), mas ela serve principalmente para que empresas e órgãos públicos sejam mais transparentes e responsáveis no manejo de dados alheios. A LGPD está publicada sob o **número 13.709**.

COMO SURGIU A LEI LGDP?

Já se falava na necessidade de uma lei de proteção de dados no Brasil bem antes da criação da LGPD. A discussão tomou corpo em 2010, quando o Ministério da Justiça lançou uma **consulta pública sobre o tema**. Nos anos seguintes, alguns parlamentares apresentaram projetos de lei dispondo sobre o tema.

Uma das inspirações era o GDPR, **Regulamento Geral sobre a Proteção de Dados**, vigente em países da União Europeia e Espaço Econômico Europeu, que foi assinado em janeiro de 2016 e substituiu a Diretiva de Proteção de Dados, criada em 1995.

Voltando ao Congresso Brasileiro, o Projeto de Lei da Câmara N° 53/2018 aglutinou as propostas que haviam surgido até então. O texto avançou até a aprovação, transformando-se na Lei Nº 13.709/2018. Ao aprovar o projeto, o então presidente, Michel Temer, vetou alguns dispositivos – como o que criava a **Autoridade Nacional de Proteção de Dados (ANPD)**.

Depois, porém, editou a Medida Provisória (MP) Nº 869/2018, instituindo a ANPD, mas com regras diferentes daquelas que a proposta original continha. A MP foi convertida na Lei Nº 13.853/2019, que acrescentou vários artigos à LGPD.

O Caso Cambridge Analytica

Como acabamos de explicar, já se falava na necessidade de criar uma **lei de proteção de dados** há vários anos. Mas o escândalo de Cambridge Analytica acelerou o processo. Cambridge Analytica foi uma empresa pertencente ao SCL Group (grupo britânico de consultoria e pesquisas diversas), que atuava na área de pesquisa e análise de dados para o processo eleitoral.

A empresa foi contratada para as campanhas do Brexit (movimento favorável à saída do Reino Unido da União Europeia) e do então candidato e hoje presidente americano Donald Trump. O que a Cambridge Analytica fez de errado foi **coletar dados de milhares de usuários do Facebook sob falsos pretextos**. A empresa lançou um aplicativo com um teste psicológico, alegando que os dados coletados seriam utilizados para fins acadêmicos. Para participar, os usuários faziam o login pela rede social. Desse modo, a Cambridge Analytica obtinha os dados pessoais dessas pessoas, além das respostas do teste e dos dados dos amigos de quem respondeu o quiz.

O que acontece é que a ação tinha outra finalidade: os **dados foram usados para produzir materiais pró-Trump e Brexit** direcionados e personalizados, de acordo com as informações obtidas. O episódio configurou uma grave violação das políticas do Facebook e uma ação inegavelmente antiética. Após a celeuma, tanto a Cambridge Analytica quanto o grupo SCL deixaram de existir. Os debates sobre a criação de uma lei de proteção de dados no Brasil já existiam antes de os escândalos virem à tona, no início de 2018, mas o episódio acabou tornando a tramitação do projeto mais rápida. É importante que existam leis e normas que regulamentem a ação de pessoas e empresas na internet.

A IMPORTÂNCIA DA LGPD

Um dos fatores que tornam a internet tão fascinante é seu caráter altamente democrático. Depois da **popularização dos computadores**, da banda larga e dos smartphones, todo mundo pôde encontrar seu espaço no meio virtual. Ao mesmo tempo, não é bom que a internet seja uma "terra de ninguém".

Sem regras, os internautas estariam sujeitos a **violações da privacidade**, da intimidade, da livre iniciativa e livre desenvolvimento da personalidade, entre outras consequências. Como você se sentiria se descobrisse que foi enganado por uma grande empresa e acabou colaborando sem querer para uma campanha eleitoral, como no caso da Cambridge Analytica?

Antes de serem internautas, as pessoas que utilizam a internet são cidadãos, com **direitos que devem ser assegurados** tanto no mundo offline quanto nos ambientes virtuais. Nesse contexto, a criação da LGPD é importante para dar mais clareza ao assunto, para que a determinação do que pode e o que não pode no tratamento de dados pessoais não seja subjetiva, questão de intuição ou opinião.

Assim, além dos usuários terem mais confiança em relação aos sistemas que coletam seus dados, as empresas podem ajustar seus processos com maior segurança jurídica, sem o **risco de cometer ilegalidades** sem saber. A LGPD criou uma diferenciação entre dados pessoais e dados sensíveis.

PRINCIPAIS DETERMINAÇÕES DA LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD dispõe sobre o **tratamento de dados** pessoais e dados pessoais sensíveis. Como o significado disso pode suscitar dúvidas em alguns, o artigo 5º da lei traz algumas definições.

Sendo assim:

- **Dado pessoal**: como já explicamos antes, é qualquer informação relacionada a pessoa natural identificada ou identificável
- **Dado pessoal sensível**: é uma informação pessoal "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"
- **Tratamento**: se refere a "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".

A partir daí, a lei traz uma série de regras para o tratamento dos dados.

O artigo 7º, por exemplo, determina quais as **hipóteses em que esse tratamento é permitido**.

São elas:

- Com o consentimento do titular
- Para o cumprimento de obrigação legal ou regulatória pelo controlador
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis
- Para a realização de estudos por órgão de pesquisa
- 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
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro
- Para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais
- Para a proteção do crédito.

Já o tratamento de dados pessoais sensíveis pode ocorrer em hipóteses ainda mais restritas, é claro, conforme determinado no artigo 11 da LGPD. Os parágrafos deste artigo ainda impõem **restrições à comunicação ou uso compartilhado** de dados pessoais sensíveis com o objetivo de obter vantagem econômica.

Outra determinação importante da lei é o direito do titular ao acesso facilitado às informações sobre o tratamento de seus dados pessoais. Ele tem o direito de saber **qual a finalidade específica** do tratamento, qual a forma e duração, quem e qual o contato do controlador, se há uso compartilhado e quais as responsabilidades dos agentes que realizam o tratamento.

No artigo 33, encontramos outra regra que vale a pena destacar, que se refere à transferência internacional de dados. A disposição impõe restrições a esse tipo de operação, que só poderá ocorrer para países que proporcionem grau de proteção de dados pessoais adequados ao previsto na LGPD ou em algumas situações específicas.

Em outros artigos, há regras diversas sobre **transparência**, orientações a serem seguidas pelos controladores e operadores de dados e outras minúcias que as empresas devem observar com cuidado.

DADOS SENSÍVEIS LGPD

Como já destacado, a LGPD prevê uma diferenciação entre dados pessoais e dados pessoais sensíveis. Recapitulando, os dados sensíveis são aqueles referentes a:

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.

O que muda é que a lei prevê algumas **regras específicas** para o tratamento de dados sensíveis, que exige uma atenção extra. O argumento para que as informações que listamos acima sejam consideradas sensíveis é que a irresponsabilidade no seu tratamento pode gerar danos ao cidadão. Isso porque tratam de assuntos com potencial para ocasionar uma **situação de discriminação**.

Por exemplo, se uma pessoa tem divulgados indevidamente dados sobre sua filiação política, pode vir a ser tratada de modo diferente em sua vida profissional.

Outra situação hipotética é quanto a informações sobre a orientação sexual de um indivíduo, que podem **gerar constrangimentos** na vida familiar, entre outros problemas.

A VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS

A princípio, a LGPD entraria em vigor 18 meses após sua publicação, ou seja, em fevereiro de 2020. A partir da **publicação da Lei Nº 13.853/2019**, que acrescentou e alterou artigos da LGPD, a regra é a seguinte, conforme consta no artigo 65:

Art. 65. Esta Lei entra em vigor:

I – dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B e

II – 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

Desse modo, a grande maioria dos dispositivos da LGPD entrariam em vigor em **agosto de 2020**.

Os artigos 55 e 58, que já passariam a valer em fevereiro, dizem respeito à criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Uma série de direitos precisam ser respeitados também no mundo virtual, como a liberdade de expressão.

Entretanto, em abril, a medida provisória 959/2020 colocou a vigência da Lei para maio de 2021, e, razão da pandemia mundial de Covid-19. Após vários desdobramentos, na terça-feira, dia 25/08, a Câmara dos Deputados votou a MP959/2020, aprovando-a com o texto que determinava a vigência da LGPD para 31/12/2020.

No entanto, ontem, dia 26/08, o Senado, em pauta única, votou e aprovou também a MP 959/2020, porém, sem o artigo que previa o adiamento da vigência da norma, tendo em vista que foi levantada questão de ordem sobre o regimento interno do Senado, pois a matéria já havia sido votada anteriormente quando da apreciação do PL 1179. Com a votação pelo Senado no sentido de recusar o adiamento da LGPD. A vigência da norma estaria posta desde o dia 14 de agosto de 2020 e as sanções administrativas para agosto de 2021.

Por fim, a LGPD já está valendo? A resposta é não!

O Senado Federal lançou nota explicativa informando que todos esses desdobramentos ainda dependem da sanção presidencial, ou seja, somente a partir da sanção do presidente Jair Bolsonaro (que pode acontecer em até 15 dias), a LGPD entrará em vigor.

Ainda ontem, o Decreto n° 10.474/2020, aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados – ANPD, órgão que tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pelo disposto na LGPD.

OS DIREITOS DO TITULAR DOS DADOS PESSOAIS

No seu artigo 2º, a Lei Geral de Proteção de Dados apresenta os fundamentos das disciplinas, que nada mais são que os **direitos a serem respeitados** no tratamento dos dados. A seguir, listamos eles:

- Respeito à 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, a livre concorrência e a defesa do consumidor
- **Direitos humanos**, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

DESCUMPRIMENTO DA LGPD

O capítulo VIII da LGPD traz disposições sobre a fiscalização e as **sanções administrativas** que incidem sobre quem não cumprir a lei. De acordo com o artigo 52, as possíveis sanções são as seguintes:

- Advertência, com indicação de prazo para adoção de medidas corretivas
- Multa simples, de até 2% do faturamento no seu último exercício, excluídos os tributos, limitada a R$ 50 milhões por infração
- Multa diária
- 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.

O parágrafo primeiro do artigo explica que as sanções são aplicadas após instaurado um **procedimento administrativo**, que deve prever a possibilidade de ampla defesa ao acusado. Para a definição da sanção, serão analisados critérios como a gravidade da infração, a boa-fé do infrator, possível reincidência e outros elementos listados na lei.

Segundo o artigo 55-J da LGPD, compete à Autoridade Nacional de Proteção de Dados (ANPD) a incumbência de fiscalizar e aplicar as sanções. É necessário que as empresas fiquem atentas à LGPD para não sofrer sanções.

COMO AS EMPRESAS DEVEM SE PREPARAR PARA A LGPD?

Afinal, quando a lei entrar em vigência, qual o impacto das novas regras para as empresas brasileiras? Esse tipo de preocupação é importante e mostra que você é um gestor interessado nas melhores práticas.

Em primeiro lugar, revise os processos da empresa em busca de áreas relacionadas com as novas regras. Pode haver muito mais dados de clientes armazenados do que o administrador tem conhecimento, principalmente nos setores de vendas e marketing.

O segundo passo é **mapear e controlar o processo**. Quem tem acesso aos dados, qual o uso que se faz dele? Documente isso tudo e revise se o *modus operandi* está alinhado com a LGPD.

Depois disso, desenhe os processos ideais, não apenas de manejo de dados, mas de prevenção a problemas. Se possível **busque soluções transparentes** de automação no monitoramento e processamento de dados.

Como se preparar para a LGPD?

PASSO A PASSO

Antes de embarcar em um projeto para atingir a conformidade com a LGDP é muito importante garantir o compromisso da alta administração. Este é, provavelmente, o fator mais significativo que poderá conduzir as entidades a um projeto de operação (e posterior implementação) bem-sucedido.

As primeiras questões que a alta gerência fará sobre o projeto provavelmente serão: (i) quais requisitos deverão ser cumpridos, (ii) quanto irá custar; e (iii) quando deverá estar pronto?

O ponto mais importante é que **a conformidade à LGPD não é opcional** e as multas previstas em caso de descumprimento são altas. Os requisitos a serem observados e os custos de adequação irão depender da avaliação de cada negócio, mas todos deverão estar em conformidade com a norma até meados de fevereiro de 2020.

Sumarizamos abaixo, em 8 tópicos, alguns *insights* destinados a fornecer um ponto de partida razoável para iniciar um projeto de conformidade à LGPD:

1. Estabelecer as necessidades e o contexto

Reunir as equipes e mapear a situação interna no que se refere às operações de processamento de dados, a fim de compreender em que medida a LGPD se aplica a seu negócio.

2. Identificar os riscos

Realizar um *gap assessment* (parte legal e técnica) para identificar as providências a serem adotadas.

3. Analisar e avaliar os riscos

Analisar e definir as bases legais para tratamento; avaliar os mecanismos de segurança das bases de dados.

4. Definir o projeto de acordo com os riscos

Definir responsabilidades; nomear um EPD; readequar e documentar os processos internos de tratamento de dados.

5. Educar funcionários

Incentivar a adoção de boas práticas e a mudança na cultura interna (através de treinamentos periódicos, por exemplo) e externa.

6. Implementar o projeto desenvolvido

Elaborar ou revisar (i) políticas de privacidade (internas e externas) e (ii) contratos com colaboradores e terceiros que impliquem no processamento de dados (operadores), assegurando-se dos meios para garantir sua execução.

7. Registrar o processo

Documentar as análises e procedimentos e implementar o Registro de Processamento de Dados.

8. Monitorar e notificar

Organizar uma política de tratamento dos incidentes para garantir o cumprimento de requisitos de comunicação às autoridades em caso de vazamentos ou uso indevido de dados pessoais.

Portabilidade de dados

Uma inovação da lei é o direito dado ao titular de obter seus dados pessoais através de um arquivo interoperável(27) (por exemplo, um arquivo .csv28), além de poder solicitar a transferência dos dados para outra organização(29). Constitui, assim, uma valiosa ferramenta de desenvolvimento e difusão de tecnologias com foco na privacidade do usuário, além de uma ferramenta para permitir que os indivíduos aproveitem a riqueza imaterial de seus dados pessoais: a possibilidade de poder transferir livremente os dados de um controlador para outro pode ser um instrumento de fomento à concorrência (observados os segredos comercial e industrial) e interoperabilidade entre plataformas, ao mesmo tempo em que reforça a capacidade de controle dos indivíduos sobre seus próprios dados(30).

Direitos do titular na LGPD

O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva, principalmente no que se refere à finalidade, forma e duração do tratamento, a identificação do controlador e seu contato, a informação sobre o uso compartilhado de dados e sua finalidade e as responsabilidades dos agentes de tratamento, além da menção explícita aos direitos do titular (31). São também garantidos ao titular, mediante requisição ao controlador, o direito de correção de seus dados, a eliminação de dados tratados com o consentimento do titular e a revogação do consentimento, sendo assegurado o direito de petição à autoridade nacional (32).

Consentimento

A concordância do titular quanto ao tratamento de seus dados pessoais deverá ocorrer de forma livre, informada, inequívoca e para uma finalidade determinada (33). O consentimento deverá ser fornecido por escrito (neste caso, de maneira destacada das demais cláusulas) ou por outro meio que demonstre a manifestação de vontade do titular (34), cabendo ao controlador o ônus da prova de que foi obtido na forma da lei (35). Serão consideradas nulas as autorizações genéricas para o tratamento de dados pessoais (36) e vedado o tratamento nos casos de vício de consentimento (37). O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente manifestado enquanto não houver requerimento da sua revogação (38).

Responsabilidade

Uma nova abordagem também envolve a responsabilidade por danos causados (patrimoniais, morais, individuais ou coletivos) pelos agentes de tratamento (39). A isto se acrescenta a responsabilidade solidária entre os sujeitos responsáveis (40) em determinados casos, a fim de garantir a efetiva indenização dos interessados. A lei também estabelece a possibilidade de inversão do ônus da prova em favor do titular dos dados, quando (i) for verossímil a alegação, (ii) houver hipossuficiência para fins de produção de prova ou (iii) quando a produção de prova pelo titular resultar-lhe excessivamente onerosa(41).

Término do tratamento

O tratamento deverá cessar quando alcançada a finalidade ou quando os dados deixarem de ser necessários ou pertinentes; ao fim do período de tratamento; mediante comunicação do titular; ou por determinação da autoridade nacional (42). Os dados devem ser eliminados após o término do tratamento, salvo exceções específicas (43).

Comunicação obrigatória

O controlador deverá comunicar, em prazo razoável, à autoridade nacional e ao titular sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante (44). A Autoridade Nacional verificará a gravidade do incidente e poderá determinar medidas como a ampla divulgação do fato em meios de comunicação, bem como outras medidas que entender necessárias para reverter ou mitigar os efeitos do incidente (45). Em situações como esta, pode haver um grande impacto negativo na reputação e na imagem da instituição envolvida (e, consequentemente, resultar em eventual desvalorização do valor de mercado e/ou perda da confiança por parte dos consumidores) (46).

Transferências internacionais de dados

As hipóteses para transferência de dados pessoais (para país estrangeiro ou organismo internacional do qual o país seja membro)(47) são previstas de forma taxativa pela lei, devendo ocorrer

apenas para aqueles que proporcionarem grau de proteção de dados pessoais adequado ao previsto na LGPD ou quando o controlador oferecer e comprovar a conformidade (através de disposições contratuais, normas corporativas, selos, certificados e códigos de conduta regularmente emitidos, com conteúdo definido ou verificado pela Autoridade Nacional)(48). Dentre as hipóteses legais, destaca-se também a necessidade de consentimento específico, em destaque e distinta de outras finalidades(49).

Encarregado pela Proteção de Dados

O EPD (semelhante à figura do *DPO – Data Protection Officer*, previsto na regulação europeia) é a pessoa natural, nomeada pelo controlador (empregado ou contratado externamento), que atuará como um canal de comunicação entre este, os titulares dos dados e a autoridade de proteção de dados(50). Será responsável por receber reclamações e comunicações de titulares e órgãos competentes, prestar esclarecimentos, adotar providências e orientar funcionários sobre as boas práticas, dentre outras atribuições(51). Sua identidade e informações de contato deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no site do controlador(52). Por não fazer nenhum ressalva específica, a análise da LGPD leva ao entendimento de que qualquer entidade que processe dados pessoais deverá, sob quaisquer circunstâncias, indicar um EPD, cabendo, porém, à autoridade nacional estabelecer normas complementares sobre a definição e a atribuição da pessoa responsável (incluindo hipóteses de dispensa de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados) (53).

Relatório de Impacto à Proteção de Dados Pessoais (RIPDP)

Semelhante ao DPIA (*Data Privacy Impact Assessment*, previsto na GDPR), refere-se à documentação do controlador que contém a descrição das atividades de processamento de dados que podem gerar riscos aos titulares de dados, bem como informações sobre a implementação de medidas, salvaguardas e instrumentos de mitigação de danos(54). Nada mais é que uma ferramenta para ajudar a identificar e minimizar os riscos na proteção de dados, que poderá ser requerida pela ANPD, quando o tratamento tiver como fundamento o legítimo interesse do controlador(55).

Registro de operações de tratamento

O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado em seu legítimo interesse(56). Assim,

> "toda e qualquer atividade de tratamento de dados pessoais deve ser registrada, desde a sua coleta até a sua exclusão, indicando quais tipos de dados pessoais serão coletados, a base legal que autoriza os seus usos, as suas finalidades, o tempo de retenção, as práticas de segurança de informação implementadas no armazenamento, e com quem os dados podem ser eventualmente compartilhados, metodologia também conhecida como '*data mapping*'"(Art. 57).

NOTA EXPLICATIVA

BIG DATA

É um processo de análise e interpretação de um **grande volume de dados** armazenados remotamente. Tudo que está disponível de forma online, de modo não sigiloso, por maior que seja a quantidade de informações, está ao alcance do Big Data, podendo ser agrupado conforme o interesse. E isso inclui não apenas os bancos de dados públicos, como o YouTube é para os vídeos, ou o Wikipédia, que funciona como a maior enciclopédia da internet.

O Big Data pode integrar **qualquer dado coletado sobre um assunto ou uma empresa**, como os registros de compra e venda e mesmo os canais de interação não digital (telemarketing e call center). Onde há um registro feito, a tecnologia o alcança. Só ficam de fora as informações realmente inacessíveis, como as suas movimentações financeiras e informações privadas de algumas organizações, por exemplo.

Já o que vaga pela web **pode ser acessado, coletado e agrupado**. O mais incrível é que isso é realizado em grande velocidade, através de ferramentas específicas de Tecnologia da Informação (TI). E se pararmos para pensar, é necessário que seja assim, dada a **gigantesca quantidade de informações** geradas a cada dia, por dispositivos diversos. Através do Big Data, portanto, é possível fazer a interpretação e a análise desses dados para variados usos. Entre eles, definir as estratégias de marketing de uma empresa, reduzir custos, aumentar a produtividade e dar um rumo mais inteligente ao próprio negócio.

Recentemente, gestores têm utilizado muito a "filosofia" de Big Data como uma **ferramenta de apoio estratégico**. O que acontece é que eles passaram a entender a sua importância para obter *insights* sobre as tendências de mercado e o **comportamento dos consumidores**, além de melhorar o próprio processo de trabalho. Os indicativos são capazes de ajudar na tomada de decisões mais assertivas e, principalmente, mais adiantadas do que a concorrência. Nem seria preciso dizer o quanto isso é fundamental para garantir o sucesso de qualquer negócio. Sendo assim, todas essas informações, **disponíveis online e também offline**, são capazes de ajudar a empresa a crescer.

BIBLIOGRAFIA

General Data Protection Regulation. A versão em português (de Portugal) está disponível em [https://eurlex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT].

MAZUI, Guilherme; CASTILHOS, Roniara. *Temer sanciona com vetos lei de proteção de dados pessoais*. Disponível em: [https://g1.globo.com/politica/noticia/2018/08/14/temer-sanciona-lei-de-protecao-de-dadospessoais.ghtml]. Acesso em 18/08/2018.
MONTEIRO, Renato L. *Lei Geral de Proteção de Dados do Brasil – Análise*. Disponível em: [https://baptistaluz.com.br/institucional/lei-geral-de-protecao-de-dados-do-brasil-analise/]. Acesso em 20/08/2018.

MARTÌ, Silas. *Entenda o escândalo do uso de dados do Facebook*. Folha de São Paulo, 22.03.2018. Disponível em: [https://www1.folha.uol.com.br/mercado/2018/03/entenda-o-escandalo-do-uso-de-dados-dofacebook.shtml]. Acesso em 20/08/2018.
WORKFRONT. *Data Discrimination: the dark side of big data*. Disponível em: [https://www.workfront.com/blog/data-discrimination-the-dark-side-of-big-data]. Acesso em 20/08/2018.
6 Lei 13.709/2018.