LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL

BAPTISTA LUZ
ADVOGADOS

BAPTISTA LUZ ADVOGADOS
R. Ramos Batista . 444 . Vila Olímpia
04552-020 . São Paulo – SP
baptistaluz.com.br

/ Renato Leite Monteiro

Lei Geral de Proteção de Dados do Brasil – Análise

Contexto

No dia 10 de julho de 2018, foi aprovado no plenário do Senado Federal o PLC 53/2018, o qual dispõe sobre a proteção de dados pessoais e altera a Lei 12.965/16 (Marco Civil da Internet), consolidando-se assim como a Lei Geral de Proteção de Dados brasileira ("LGPD"). O processo público e legislativo começou em 2010, com a abertura de uma consulta pública sobre o tema, promovida pelo Ministério da Justiça, que resultou, posteriormente, na propositura do PL 5276/2016, anexado ao PL 4060/2012, perante a Câmara dos Deputados. Agora, após 2 anos de trâmite no Congresso Nacional (Câmara e Senado), duas consultas públicas, mais de 2500 contribuições de atores nacionais e internacionais, de todos os setores e inúmeros eventos, chega ao seu fim e segue para sanção (e, talvez, veto parcial) presidencial. Se aprovado pelo presidente Michel Temer, o projeto passa a ser lei, com um período de adaptação de 18 meses.

Ap[illegible]el on/offline
Harmonia entre proteção de dados e inovação

A LGPD cria todo um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores privados e públicos. Importante salientar que o País já dispunha de mais de 40 normas que direta e indiretamente tratavam da proteção à privacidade e aos dados pessoais. Todavia, a LGPD vem substituir e/ou complementar esse arcabouço regulatório setorial, que por vezes era conflituoso, pantanoso, trazia insegurança jurídica e tornava o País menos competitivo no contexto de uma sociedade cada vez mais

movida a dados. O texto, fruto de uma ampla discussão, visa não somente garantir direitos individuais, mas também fomentar o desenvolvimento econômico, tecnológico e a inovação por meio de regras claras, transparentes e amplas para o uso adequado de dados pessoais. Ao ter uma Lei Geral, o Brasil entra para o rol de mais de 100 países que hoje podem ser considerados adequados para proteger a privacidade e o uso de dados.

Quais são os objetivos da Lei Geral de Proteção de Dados?

- Direito à privacidade: garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos ao permitir um maior controle sobre seus dados, por meio de práticas transparentes e seguras, visando garantir direitos e liberdades fundamentais.

- Regras claras para empresas: estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para empresas.

- Promover desenvolvimento: fomentar o desenvolvimento econômico e tecnológico numa sociedade movida a dados.

- Direito do consumidor: garantir a livre iniciativa, a livre concorrência e a defesa do consumidor.

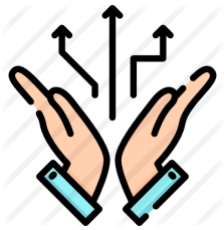
- Fortalecer confiança: aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais.

- Segurança jurídica: aumentar a segurança jurídica como um todo no uso e tratamento de dados pessoais.

Quais são as vantagens da Lei Geral de Proteção de Dados?

- Unificar regras: regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia.

- Maior flexibilidade: autorizar formas mais flexíveis para o tratamento de dados pessoais, tais como legítimos interesses, que levam em consideração uma sociedade movida a dados em tempos de big data.



- Redução de custos: diminuir custos operacionais causados por incompatibilidades sistêmicas de tratamentos feitos por agentes diversos, além de fomentar uma maior qualidade dos dados em circulação no ecossistema como um todo.

- Adequar as regras no Brasil: tornar o Brasil apto a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar, principalmente, os setores de tecnologia da informação.

- Portabilidade: indivíduos poderão transferir seus dados de um serviço para outro, aumentando a competitividade no mercado.

Fatores que levaram à aprovação da Lei

Como dito acima, a LGPD não foi aprovada de uma hora para outra - pelo contrário, foram anos de intensa discussão, que levaram a um texto extremamente maduro quando comparado com a primeira versão de 2010. Todavia, alguns fatores podem ser listados que forçaram a aceleração do trâmite na sua reta final:

General Data Protection Regulation - GDPR

No último dia 25 de maio, entrou em vigor a nova regulamentação europeia de proteção de dados, conhecida como GDPR. Apesar de ser

uma lei da União Europeia, por diversos fatores, ela tem eficácia e aplicação extraterritorial, além dos limites geográficos do velho continente. Isso inclui o Brasil. Diversas empresas nacionais que têm filiais em algum dos 28 países da UE, ou que oferecem serviços a pessoas localizadas neles, tiveram que se adaptar, sob pena de sofrerem multas milionárias ou perderem contratos com empresas que diretamente devem estar em conformidade com a nova regulamentação. Ainda, a GDPR cria obstáculos para a transferência internacional de dados pessoais para países que não possuem um nível adequado de proteção de acordo com a análise da União Europeia. O Brasil, agora com a LGPD, pode, em breve, passar a compor o rol de países para os quais tais dados podem ser transferidos, o que terá fortes impactos econômicos e comerciais.

Tais elementos aumentaram a pressão não só para a aprovação da lei geral, mas também moldaram as discussões que culminaram numa redação muito similar à da GDPR, até mesmo superior em alguns pontos, como na abordagem dada a dados anonimizados quando estes forem utilizados para a formação de perfis comportamentais.

Cambridge Analytica

O escândalo envolvendo a empresa Cambridge Analytica escancarou as graves consequências que podem advir do uso não autorizado e indevido de dados pessoais, que extrapolam o plano individual, ao ponto de repercutir nos rumos democráticos de uma nação, como se suspeita que tenha acontecido com a eleição do Presidente Donald Trump nos EUA e com a saída do Reino Unido da União Europeia. Ficou claro o impacto que a ausência de regras claras sobre o uso de dados e de uma autoridade que as aplique e supervisione pode ter.

No Brasil, a empresa já pretendia atuar no futuro pleito eleitoral para a presidência da república, por meio do oferecimento de conteúdos e

propagandas direcionadas a eleitores baseadas nos interesses inferidos dos seus dados pessoais, possivelmente coletados e utilizados de forma indevida, com a finalidade de influenciar os seus votos. Por este motivo, o escândalo teve grande repercussão também em solo brasileiro, tanto que uma investigação foi aberta pelo Ministério Público para averiguar se realmente houve coleta e uso não autorizado de dados pessoais para essas finalidades. Todavia, na ausência de uma lei geral, uma zona interpretativa cinzenta prevalece quanto à (i)legalidade no uso dos dados, uma vez que inexistiria, em alguns contextos, limitações claras ao tratamento destes. Dessa forma, ficou à época ainda mais evidente a necessidade de uma LGPD brasileira.

Organização para a Cooperação e Desenvolvimento Econômico - OCDE

O Brasil está para pleitear a sua entrada na Organização para a Cooperação e Desenvolvimento Econômico (OCDE, ou OECD, no seu original). A organização foi uma das primeiras a especificamente lidar com a regulação do uso de dados pessoais, com foco principal nas transferências internacionais inerentes a muitos modelos de negócio. Suas primeiras orientações foram publicadas já em 1980 (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), e em 2013 foram atualizadas para se adequar aos novéis da sociedade da informação, acabando por influenciar diretamente a redação de leis em inúmeros países - até mesmo a antiga diretiva europeia de proteção de dados e o futuro regulamento. Apesar de os seus guidelines não terem força de lei, para que os países possam fazer parte da organização, eles devem se obrigar a cumprir com as regras estabelecidas pela OCDE, inclusive no tocante à proteção de dados. Entretanto, o Brasil, por carecer de uma lei geral ou de normas robustas, estava longe de cumprir com tais obrigações. Essa lacuna compeliu o Governo Federal e o Ministério das Relações Exteriores, por meio do seu chanceler, Senador Aloysio Nunes, que também fora relator do PL de Dados do Senado, o antigo PL 330/2013,

a apoiarem a aprovação da LGPD, como forma de facilitar a entrada do Brasil na OCDE.

Lei do Cadastro Positivo

Um outro ponto que foi essencial para a aprovação da LGPD no Congresso Nacional foi a tentativa de alteração da Lei do Cadastro Positivo, que regulamenta o banco de dados de adimplentes (bons pagadores, em conjunto com o Código de Defesa do Consumidor, que lida com o de mal pagadores), relatórios de crédito e algoritmos de risco de crédito. A lei atualmente em vigência determina que os dados de consumidores somente podem ser adicionados a tais bases com o seu consentimento, prática esta conhecida como opt-in. A alteração pretendia, entre outros pontos, mudar essa lógica para permitir que os dados pessoais pudessem ser coletados, utilizados e compartilhados sem o consentimento do titular, permitindo a este, apenas, requisitar o cancelamento dos seus dados posteriormente, prática conhecida como opt-out. Essa alteração automaticamente incluiria os dados de mais de 30 milhões de brasileiros em sistemas geridos por empresas, o que poderia, alguns defendiam, alavancar a concessão de crédito no País, pois seria possível, em tese, efetivamente distinguir os bons pagadores dos maus.

Todavia, essa vantagem não viria sem riscos. Numa era de grandes vazamentos de dados e incontáveis casos de usos indevidos destes, permitir a aglomeração de dados pessoais de toda a população brasileira economicamente ativa sem que haja regras claras, transparentes, robustas e harmônicas que regulem tais usos pode ser uma prática indesejada e temerária. Esse cenário deu ensejo a toda uma leva de negociações políticas que culminaram na aprovação de um texto base alterando a Lei do Cadastro Positivo, mas bem diferente do original, com bem mais garantias, e a concordância do Presidente da Câmara dos Deputados, Rodrigo Maia, da necessidade de se ter uma lei geral de proteção de dados antes das alterações pretendidas no cadastro positivo. Esse acordo político foi um dos principais fatores

que permitiram a aceleração do trâmite do PL 5276/2016 na Câmara, que recebeu a numeração de PLC 53/2018 após ser aprovado nesta casa e enviado para o Senado.

O que a lei diz

A LGPD tem aplicação transversal e multissetorial, tanto no âmbito público e privado, online e offline. Ela versa sobre o conceito de dados pessoais, lista as bases legais que autorizam o seu uso – e o consentimento é apenas uma delas, dando destaque para a permissão do uso de dados com base no legítimos interesse do controlador do dados -, além de tratar de princípios gerais, direitos básicos do titular - como acesso, exclusão dos dados e explicação sobre uso - obrigações e limites que devem ser aplicadas a toda entidade que se vale do uso de dados pessoais, seja como insumo do seu modelo de negócio, seja para a atividade de seus colaboradores. Estes são os principais pontos da nova lei:

- **Escopo de aplicação**: a LGPD de dados terá aplicação transversal, multissetorial, a todos os setores da economia, tanto no âmbito público quanto no privado, online e offline. Com poucas exceções, toda e qualquer prática que se valer do uso de dados pessoais estará sujeita à lei.

- **Aplicação extraterritorial**: em moldes similares à regulamentação europeia, a GDPR, a Lei Geral terá aplicação extraterritorial, ou seja, o dever de conformidade superará os limites geográficos do País. Toda empresa estrangeira que, pelo menos, tiver filial no Brasil, ou oferecer serviços ao mercado nacional e coletar e tratar dados de pessoais naturais localizadas no território brasileiro, estará sujeita à nova lei.

- **Conceito de dados pessoais**: a LGPD traz um conceito amplo do que deve ser considerado dado pessoal – trata-se da informação relacionada a uma pessoa natural identificada ou identificável. Ou seja, qualquer dado que, isoladamente ou agregado a outro, possa permitir

a identificação de uma pessoa natural, ou sujeitá-la a um determinado comportamento (interpretação esta oriunda de uma leitura integrativa do texto). Em tempos de big data, onde é possível a correlação rápida de grandes bases de dados, praticamente qualquer dado pode, eventualmente, vir a ser considerado pessoal - portanto, sujeito aos ditames da lei.

- **Conceito de dados pessoais sensíveis**: dados pessoais sensíveis são aqueles que pela sua própria natureza podem sujeitar o seu titular a práticas discriminatórias, tais como dados sobre a origem racial ou étnica, a convicção religiosa, a opinião política, ou dados referentes à saúde ou à vida sexual; ou permitir a sua identificação de forma inequívoca e persistente, tais como dado genético (este com ambas as facetas) ou biométrico. Tais dados devem ser tratados de forma diferenciada, com camadas de segurança adicionais, e com bases legais distintas e mais restritivas do que as que autorizam o tratamento de dados pessoais não sensíveis – sendo a principal delas, também, o consentimento expresso do titular.

- **Dados anonimizados**: dados anonimizados seriam os relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Desta forma, estariam fora do escopo de aplicação da lei, à exceção de quando o processo de anonimização puder ser revertido ou se estes forem utilizados na formação de perfis comportamentais. Dados efetivamente anonimizados são essenciais para o funcionamento de tecnologias na seara da internet das coisas, inteligência artificial, machine learning, smart cities e análise de grandes contextos comportamentais.

- **Dados públicos**: existem hoje grandes discussões sobre os limites no uso de dados pessoais publicamente acessíveis, tais como os constantes de bases geridas por órgãos públicos, publicações oficiais e cartórios, ou os expressamente tornados públicos pelos seus titulares, como em perfis públicos em redes sociais. A LGPD não define ou

delimita o conceito do que seriam "dados públicos", mas versa sobre situações que envolve os seus possíveis processamentos, tratando-as de formas distintas, e impondo determinadas limitações, como o uso limitado às finalidades que ensejaram a publicização dos dados pessoais.

- **Bases legais para o tratamento dos dados - consentimento e legítimos interesses**: para se tratar dados pessoais, o que inclui a prática da coleta, sempre é necessário ter um fundamento legal. A LGPD enumera 10 hipóteses que autorizam o uso dos dados, sendo o consentimento inequívoco apenas uma delas. Destaca-se a positivação da base legal conhecida como "legítimo interesse", que permitiria o uso dos dados para finalidades além daquelas originalmente autorizadas pelos seus titulares ou as que ensejaram a sua criação. Por meio de um teste de proporcionalidade que leva em consideração os interesses dos responsáveis pelo tratamento e os direitos dos titulares, essa hipótese permitiria novos usos, o que a torna essencial em tempos de big data, inteligência artificial, machine learning e modelos de negócio inovadores baseados no uso de dados pessoais.

- **Princípios gerais de proteção de dados**: a LGPD lista 10 princípios que devem ser levados em consideração no tratamento de dados pessoais, tais como o da finalidade, necessidade, transparência, segurança, não discriminação e o - novo - princípio da responsabilização e prestação de contas, que obriga o responsável pelo tratamento dos dados pessoais a demonstrar de forma cabal e transparente a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, algo que pode ser feito por meio dos assessments, metodologias de análise também previstas na lei.

- **Direitos básicos dos titulares**: os titulares dos dados pessoais tiveram seus direitos ampliados, que devem ser garantidos de forma acessível e eficaz. Dentre os direitos listados, destaca-se o de acesso aos dados, retificação, cancelamento ou exclusão, oposição ao

tratamento, de informação e explicação sobre o uso dos dados. A grande novidade é o direito à portabilidade dos dados, que, similar ao o que pode ser feito entre diferentes empresas de telefonia e bancos, permite ao titular não só requisitar uma cópia da integralidade dos seus dados, mas também que estes sejam fornecidos em um formato interoperável, que facilite a transferência destes para outros serviços, mesmo para concorrentes. Devido a sua natureza, este novo direito tem sido encarado como um forte elemento de competição entre diferentes empresas que oferecem serviços similares baseados no uso de dados pessoais.

- **Autoridade Nacional de Proteção de Dados**: um dos pontos mais relevantes estabelecidos pela lei é a criação de uma autoridade pública autônoma e independente para a supervisão da aplicação de lei – no projeto, nomeada como Autoridade Nacional de Proteção de Dados – a ANPD. O seu real formato ainda não foi definido, mas deve funcionar em moldes similares a uma agência reguladora, ou órgãos de fiscalização, como o CADE. A Autoridade poderá estabelecer diretrizes para a promoção da proteção de dados pessoais no Brasil. Em resumo, esta deverá zelar pela proteção dos dados pessoais, elaborar a "Política Nacional de Proteção de Dados e da Privacidade", como definida pela lei, fiscalizar e aplicar sanções em caso de violação às leis pertinentes, atender petições de titulares de dados contra os responsáveis pelo seu tratamento, regulamentar as matérias sobre proteção de dados, entre outras atividades. A LGPD prevê também a criação do Conselho Nacional de Proteção de Dados, órgão consultivo, com composição multissetorial, que pode propor diretrizes e estratégias, realizar estudos e disseminar conhecimento sobre proteção de dados no Brasil.

- **Data Protection Officer (DPO)**: o DPO foi traduzido pela LGPD como o "encarregado", e é a pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a Autoridade Nacional. Ademais, deve ser o responsável dentro da instituição pela supervisão do cumprimento das regras previstas na lei e orientar os funcionários e os contratados da entidade a respeito das

práticas a serem tomadas em relação à proteção de dados pessoais. Uma leitura inicial da LGPD permite concluir que toda e qualquer entidade que trate dados pessoais deve indicar um DPO, mas a Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa.

- **Relatório de impacto à privacidade - Data Protético Impact Assessment (DPIA)**: conceituado como o "relatório de impacto à proteção de dados pessoais", refere-se à documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos direitos dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos. Esta poderá ser obrigatória em situações já caracterizadas como de risco ou, a pedido da Autoridade, quando o tratamento de dados for baseado no legítimo interesse. A metodologia do DPIA é amplamente adotada pela GDPR e permite, além do mapeamento dos riscos, uma efetiva fotografia do status da conformidade regulatória da entidade.

- **Registro das atividades de tratamento**: 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.

- **Padrões de Segurança da Informação**: os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. A Autoridade Nacional poderá dispor sobre padrões técnicos mínimos, considerando a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia.

- **Privacy by Design e by Default**: torna-se obrigatório adotar desde a concepção de serviços, produtos e modelos de negócio a prática de se garantir direitos de proteção à privacidade e aos dados pessoais. Os princípios gerais da LGPD e os padrões de segurança devem, portanto, ser observados desde a concepção até a execução e oferecimento do produto e serviço. Ainda, os controles de privacidade, popularmente acessíveis por meio de dashboards em plataformas online, devem ser por padrão os mais protetivos, cabendo aos titulares flexibilizá-los, caso assim deseje.

- **Códigos de Conduta e Certificação**: a LGPD claramente incentiva a adoção de códigos de conduta setoriais e de certificações que possam garantir a observância das regras da norma. Determinados setores da sociedade podem criar seus próprios padrões de conduta no uso de dados, que podem até mesmo ser superiores à lei. Estes devem ser previamente autorizados pela Autoridade e conferir métodos que demonstrem o aferimento das condutas. Ainda, entidades podem se qualificar perante a Autoridade para certificar que outras instituições estão em conformidade com a lei geral.

- **Transferência internacional de dados**: a LGPD traz uma série de hipóteses que permitem a transferência internacional de dados pessoais, até mesmo para países não considerados como dotados de um nível adequado de proteção. Destaca-se a possibilidade de transferência baseada no consentimento específico do titular para a transferência, que deve ser prévio e separado das demais finalidades e requisições de consentimento. É possível, ainda, realizar a transferência caso haja a garantia, por meio de instrumentos contratuais, do controlador no cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na lei. Em moldes similares à GDPR, a lei permite a transferência por meio de adoção de selos, certificados e códigos de conduta regularmente emitidos e autorizados pela Autoridade Nacional.

- **Responsabilidade dos agentes de tratamento**: os diferentes agentes envolvidos no tratamento de dados - o controlador e o operador - podem ser solidariamente responsabilizados por incidentes de segurança da informação e/ou o uso indevido e não autorizado dos dados, ou pela não conformidade com a lei. Todavia, a responsabilidade do operador, aquele que pratica o tratamento de dados em nome e a mando do controlador, pode ser limitada às suas obrigações contratuais e de segurança da informação, caso não viole as regras que lhe são impostas pela LGPD. Importante, portanto, definir se uma empresa deve ser encarada como um controlador ou um operador, ou ambos, para definir os limites da sua responsabilidade.

- **Notificação obrigatória de incidentes**: a notificação sobre a ocorrência de incidentes de segurança da informação para a Autoridade Nacional de Proteção de Dados passa a ser mandatória, e deve ser feita em prazo razoável, podendo ainda a ANPD, com base na gravidade do caso, determinar a notificação dos titulares envolvidos e também a ampla publicização do incidente, o que pode ter um enorme impacto reputacional na imagem da instituição, e até mesmo ensejar a sua desvalorização no mercado e perda de confiança dos consumidores.

- **Penalidades**: sanções administrativas podem ser aplicadas pela ANPD em caso de infração à LGPD. Entre as sanções, há possibilidade de aplicação de advertências, multas, ou até mesmo a proibição total ou parcial de atividades relacionadas ao tratamento de dados. As multas podem variar entre 2% do faturamento da empresa, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Há ainda a possibilidade de multa diária para compelir a entidade a cessar as violações.

- **Período de transição e adaptação**: a LGPD entrará em vigor 18 meses após a sua publicação. Ou seja, entidades públicas e privadas

terão esse período para se adaptar. Ademais, A Autoridade Nacional poderá estabelecer normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor da Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Próximos passos

A LGPD vai agora para sanção presidencial. A Presidência pode acatar a lei como um todo, negá-la completamente ou vetar determinadas partes. Muito se discute sobre a possibilidade de veto do trecho que cria a Autoridade Nacional de Proteção de Dados, com base em uma série de argumentos jurídicos, políticos e orçamentários. Todavia, a entregada em vigor de uma lei geral de proteção de dados sem uma autoridade autônoma e independente pode ter um impacto indesejado na sua eficácia, e até mesmo tornar a lei incompleta, uma vez que o seu texto faz menção à autoridade 56 vezes, e determinadas partes simplesmente não farão sentido sem a sua existência.

Após a publicação da lei, as entidades terão 18 meses para se adaptar. Poderá ser uma tarefa árdua e custosa, principalmente para aquelas que deixarem para fazê-lo no final do período de transição, o que foi amplamente visto no contexto da GDPR.

Em suma, a LGPD terá um impacto na sociedade como poucas leis antes tiveram, uma vez que, hoje, praticamente toda e qualquer prática se vale do uso de dados pessoais. Empresas de todos os setores terão que se adaptar e uma nova cultura sobre o uso adequado de dados deverá ser formada, algo de difícil atingimento levando em consideração que o Brasil, diferente de outras regiões do mundo,

principalmente da Europa, ainda está na sua infância com relação a esse tema.

Nesse sentido, portanto, empresas precisam se adequar às regras de hoje e compreender que se antever à futura regulamentação é, também um investimento e uma vantagem competitiva.