



E-BOOK

Privacidade e proteção de dados na era da inteligência artificial



Sumário

■ Introdução

CAPÍTULO 1

■ O dilema privacidade x uso de dados pessoais

CAPÍTULO 2

■ Regulamentação e proteção de dados na era da IA

- A regulamentação no Brasil e na Europa
- O que esperar do futuro da regulamentação?
- Os desafios dos dados


CAPÍTULO 3

■ Preocupação com segurança digital cresce entre consumidores

CAPÍTULO 4

■ Direitos digitais dos consumidores: transparência, consentimento e acesso

- Tendências e desafios futuros



Introdução

Nos últimos anos, a ascensão da inteligência artificial (IA) tem redefinido as estratégias de negócios e impulsionado uma transformação digital sem precedentes. Essa revolução tecnológica não apenas aumentou a competitividade no mercado, mas também elevou as expectativas dos consumidores, que agora esperam que as interações com as companhias sejam rápidas, inteligentes e integradas, independentemente do canal de comunicação utilizado. Um levantamento da Zendesk mostra, por exemplo, que 63% dos consumidores esperam que as marcas usem inteligência artificial para personalizar suas experiências.

Na outra ponta, as organizações têm acelerado o uso de ferramentas inteligentes para melhorar a experiência no curto prazo, como tecnologias que favoreçam a personalização, coleta de dados em tempo real, chatbot alimentado por inteligência artificial e experiências de omnichannel interligadas.

Ao mesmo tempo em que traz eficiência e agilidade, o avanço da IA trouxe à tona desafios complexos, especialmente no que diz respeito à privacidade e à segurança dos dados. Com a ampliação da coleta e do uso de informações pessoais para alimentar modelos preditivos e

soluções personalizadas, cresce a preocupação com a transparência e o consentimento no uso desses dados. Regulamentações como a LGPD no Brasil e o GDPR na União Europeia têm ganhado relevância nesse contexto, impondo diretrizes para garantir a proteção dos consumidores sem comprometer a inovação das empresas.

Nesse cenário de oportunidades e riscos, as organizações enfrentam um dilema estratégico: como equilibrar o uso inteligente de dados com o respeito à privacidade dos clientes? Neste e-book, uma coprodução **MIT Sloan Management Review Brasil** e Pinheiro Neto Advogados, que contou com a colaboração dos repórteres Daniel Navas e Sandra Regina da Silva, abordaremos os impactos da IA nas regulamentações de privacidade, as estratégias para garantir conformidade sem comprometer a inovação, e também como as empresas podem construir relações mais transparentes com os consumidores garantindo o equilíbrio entre tecnologia e segurança de dados.

Boa leitura!

Christye Cantero


Editora de conteúdos cobranded na
MIT Sloan Management Review Brasil

CAPÍTULO 1



O dilema privacidade x uso de dados pessoais

Em [artigo recente publicado na MIT SMR Brasil](#), Gregory Vial, professor-associado do Departamento de Tecnologias de Informação da HEC Montréal (Canadá); Julien Crowe, diretor sênior de inteligência artificial do National Bank of Canada; e Patrick Mesana, doutorando no Departamento de Ciências



Para a efetiva gestão da privacidade e do uso de dados, as empresas têm de investir no letramento dos colaboradores

da Decisão da HEC Montréal, afirmaram que as implicações da potencial exposição de dados pessoais estão apenas começando, “especialmente no caso das empresas que investem em IA e análise avançada para colher insights valiosos para o negócio a partir dos dados de seus clientes”.

Entre as abordagens sugeridas pelos autores para fazer da melhor forma a gestão da privacidade e do uso de dados estão o investimento no letramento dos colaboradores e também a visão de que privacidade de dados é uma questão de negócios. Segundo eles, essas são ações fundamentais para que toda a organização se conscientize dos riscos e entenda qual é a solução mais equilibrada para resguardar os dados dos clientes.

Os autores explicam que deve haver um entendimento generalizado de que o imperativo de gerenciar dados pessoais com cuidado está fundamentado na necessidade de manter a

confiança do cliente – e isso está diretamente relacionado ao resultado da empresa.

Para eles, um caminho para resolver o dilema entre privacidade e uso de dados pessoais é a colaboração entre as equipes de segurança cibernética e de IA. Quando há uma compreensão mútua das necessidades de cada área, é facilitada a adoção de técnicas que equilibram a privacidade e a utilidade dos dados.

Eles ressaltam ainda que a garantia da privacidade de dados envolve uma série de stakeholders com diferentes conhecimentos e preocupações, e todos eles devem ser capazes de se comunicar em uma linguagem comum e participar da discussão e do desenho de estratégias de privacidade de dados. A colaboração interdisciplinar é essencial: quando algo é visto como uma questão de negócios, passa a ser importante para todos na organização, principalmente num momento de evolução acelerada da ciência da privacidade de dados, aliada à modernização das exigências regulatórias.



CAPÍTULO 2

Regulamentação e proteção de dados na era da IA

Uma pesquisa realizada recentemente pelo Gartner revela que a adoção rápida da inteligência artificial generativa (IA gen) é a principal preocupação indicada por 70% dos líderes jurídicos, de compliance e de privacidade dos dados para os próximos dois anos.

O estudo mostra que um ponto de atenção é que, enquanto a regulamentação da IA ainda está sendo desenvolvida em muitos países, há diversas incertezas e riscos imprevisíveis com os quais as organizações terão de lidar para garantir o uso ético e legal dessa tecnologia.

Madalena Gomes Cruz, associada da área de comunicações, proteção de dados e tecnologia do escritório Vieira de Almeida, de Portugal, ressalta que, embora a tecnologia traga grandes oportunidades, a IA também representa uma série de desafios legais, que, segundo ela, se concentram em três eixos principais: as normas que regulam a própria IA, as questões relacionadas ao uso de dados, sejam eles pessoais ou não, e o contexto específico em que a IA é utilizada, como no relacionamento com colaboradores, clientes ou outros públicos. “É um cenário complexo, mas a identificação desses três eixos auxilia na compreensão dos principais pontos de atenção”, ressalta.

Ciro Torres Freitas, sócio da área de tecnologia de Pinheiro Neto Advogados, lembra que a IA é uma tecnologia cujos impactos ainda são, em grande medida, desconhecidos, e que o Brasil ainda não tem legislação específica sobre o tema. No entanto, ele aponta que leis já existentes, como as de proteção de dados e de direitos autorais, exercem um papel fundamental na regulação da IA.

Para ele, o primeiro passo para as empresas – e que também representa um desafio – é identificar a legislação aplicável a cada negócio para, então, implementar as medidas cabíveis visando ao seu cumprimento. “Isso se dá por meio do estabelecimento de medidas de governança, incluindo medidas técnicas de segurança, supervisão humana, transparência, registro e documentação de operações, auditorias”, detalha Freitas.

A regulamentação no Brasil e na Europa

Cruz explica que o regulamento já aprovado na União Europeia, cuja aplicação ainda está em andamento, divide os sistemas de IA por níveis de risco. “Vai desde sistemas proibidos, como os usados para social score [sistema que avalia o comportamento de indivíduos com base em suas ações e interações sociais, tanto online quanto offline, como o sistema de crédito social da China], aos que envolvem alto risco e demandam maior controle e transparência, até aos sistemas que não têm praticamente obrigações adicionais, pelo diminuído nível de risco que apresentam”, diz.

De acordo com ela, “o fato de haver um regulamento reduz a incerteza. Porém, o caminho ainda é longo, com adaptações esperadas pelas legislações locais e também no processo de aplicação



Da mesma forma que a IA oferece grandes oportunidades, também representa uma série de desafios legais

prática”. Cruz prevê que, assim como ocorreu com o Regulamento Geral sobre a Proteção de Dados (RGPD), a regulamentação da IA passará por anos de interpretações e ajustes.

Já no Brasil, “o panorama legislativo hoje é de ausência de uma lei específica de IA, mas com expectativa de aprovação em breve, e existência de normas legais que se aplicam ao tratamento de dados pessoais, inclusive no contexto da inteligência artificial”, resume Freitas. De acordo com o advogado, é esperada a aprovação de uma legislação específica para IA, como o Projeto de Lei 2.338, de 2023, que busca regulamentar o uso da tecnologia no País. “O PL, inspirado no modelo europeu, trata da concepção, desenvolvimento e adoção de sistemas de IA, com uma abordagem também baseada em risco”, comenta.

Segundo ele, o Brasil já está bastante engajado nesse processo legislativo e, embora a aprovação da lei possa levar tempo, o avanço é inevitável. Ele reforça que, enquanto isso, as empresas já precisam estar atentas à LGPD, que se aplica de forma ampla ao uso de dados pessoais, inclusive no contexto da IA.

O que esperar do futuro da regulamentação?

Em relação ao futuro da regulamentação da IA, Cruz destaca a importância de se criar certificações, standards e códigos de conduta que possam facilitar o cumprimento das obrigações legais, especialmente para pequenas empresas. Já Freitas, comenta que “o momento atual é de busca por equilíbrio entre proteção das pessoas afetadas pelo sistema de IA e a inovação”.

É certo que as ferramentas de IA criam riscos consideráveis, atesta ele, “mas essa mesma tecnologia já é aplicada com sucesso em áreas muito importantes, como na medicina, educação, agropecuária, e na própria acessibilidade”.

A expectativa é que a regulamentação caminhe lado a lado com o desenvolvimento tecnológico. Enquanto Cruz afirma que as empresas precisam estar atentas às mudanças legislativas para não se encontrarem despreparadas no futuro, Freitas enfatiza que as normas também podem, de fato, criar oportunidades para as companhias que queiram se destacar no mercado.

Com o crescimento rápido da IA, os debates sobre sua regulamentação se tornam cada vez mais urgentes. Apesar da complexidade desse cenário, é preciso ter uma abordagem equilibrada, que permita que a inovação continue avançando de maneira segura e ética.

Os desafios dos dados

Artigo publicado na **MIT SMR Brasil** aponta que as empresas, em nome da segurança cibernética, estão blindando informações dos clientes, o que acaba empobrecendo a análise avançada de dados, seja para oferecer produtos e serviços mais personalizados ou seja para estreitar a relação com os clientes. Uma das grandes questões para as organizações é saber como proteger a privacidade dos dados pessoais dos clientes e, ao mesmo tempo, usar essas informações para alimentar análises modeladas por IA.

De acordo com Freitas, o caminho para as empresas protegerem dados pessoais ao mesmo tempo em que utilizam essas informações para treinar sistemas de IA é seguir as diretrizes da LGPD, a qual funciona como um “manual de instruções” sobre como tratar dados pessoais. Segundo ele, é possível conciliar o uso desses dados com as exigências legais, desde que a empresa utilize ferramentas de segurança adequadas e esteja respaldada por uma base legal, como um interesse legítimo ou o consentimento dos titulares.

“A LGPD indica hipóteses em que o tratamento pode ser feito, condições para que isso seja feito, as obrigações impostas àqueles que tratam os dados pessoais, os direitos dos titulares desses da-



“O momento atual da regulamentação de IA é de busca por equilíbrio entre proteção das pessoas afetadas pelo sistema de IA e a inovação”

Ciro Freitas, de Pinheiro Neto Advogados

dos. E isso tudo pode ser aplicado no contexto do uso desses dados para alimentar análises modeladas por IA”, completa Freitas. Ele sugere ainda que, quando não for possível atender às exigências da LGPD, o uso de dados anonimizados poderá ser uma alternativa.

No mercado europeu, o regulamento permite a reutilização de dados desde que o novo objetivo seja compatível com o propósito inicial. Cruz menciona a importância de iniciativas europeias que incentivam a partilha de dados entre setores, além do crescente mercado de compra de dados. Contudo, “é preciso ter muito cuidado com esse tipo de mercado para garantir que a reutilização é possível de modo compatível com a lei”, aponta.



CAPÍTULO 3

Preocupação com segurança digital cresce entre consumidores


Conforme avançam os recursos tecnológicos, também aumenta a preocupação dos consumidores relacionada à segurança digital. [Estudo da Deloitte](#) aponta que quase seis em cada dez entrevistados temem que seus dispositivos sejam vul-

neráveis a ataques de hackers e violações de segurança. O mesmo percentual também se preocupa com a possibilidade de serem rastreados por empresas ou indivíduos por meio de seus aparelhos.

A preocupação é mais acentuada entre usuários de smartphones e dispositivos domésticos inteligentes. Sessenta e sete por cento dos donos de smartphones temem pela segurança de seus dados, enquanto, entre os usuários de casas inteligentes, 62% manifestam a mesma preocupação.

O levantamento também revela que mais da metade (52%) teme que hackers possam assumir o controle de dispositivos como fechaduras inteligentes. Os usuários de smartwatches e rastreadores de fitness também demonstram apreensão: 48% estão preocupados com a privacidade nesses aparelhos. O rastreamento de localização também é uma questão crítica, com mais de 60% dos entrevistados receosos de que seus hábitos e movimentações sejam monitorados.

E esses receios têm fundamento. Um terço dos entrevistados relatou ter sofrido pelo menos uma violação ou golpe no último ano, enquanto 16% foram vítimas de dois ou mais ataques. A vulnerabilidade cresce com o aumento do número de dispositivos conectados em uma residência. Famílias com até 15 dispositivos relataram um índice de 11% de múltiplas violações, número que



Estudo da Deloitte aponta que 6 em cada 10 entrevistados temem que seus dispositivos sejam vulneráveis a ataques de hackers e violações de segurança

sobe para 16% entre aquelas com 16 a 30 aparelhos e chega a 29% em lares com mais de 30 dispositivos. Em um experimento, pesquisadores constataram que uma casa equipada com dispositivos da internet das coisas (IoT) pode ser alvo de milhares de tentativas de invasão em apenas uma semana.

Diante desse cenário, mais consumidores estão adotando medidas de segurança. O estudo identificou 14 práticas que podem ser utilizadas para proteger dados, como autenticação em duas etapas, desativação de localização e conexões bluetooth, além da instalação de softwares de segurança. Em 2023, 79% dos entrevistados afirmaram ter tomado pelo menos uma dessas precauções, um aumento em relação aos 71% do ano anterior. No entanto, três em cada quatro consumidores acreditam que deveriam fazer mais para se proteger. Entre os principais obstáculos, 27% afirmam que as empresas conseguem rastreá-los independentemente das medidas adotadas, enquanto 17% acreditam que hackers sempre encontra-

rão uma forma de acessar seus dados. Além disso, um quarto dos entrevistados diz não saber quais ações tomar, e 18% relataram não querer pagar por serviços ou softwares de segurança.

A pesquisa ainda aponta que a grande maioria dos entrevistados deseja mais proteção e controle sobre como seus dados são usados. Quase nove em cada 10 concordam que devem ser capazes de visualizar e excluir os dados que as empresas coletam sobre eles, e 80% acham que merecem ser pagos por organizações que lucram com seus dados. Além disso, 85% consideram que os fabricantes de dispositivos devem fazer mais para proteger a privacidade e a segurança dos dados nos dispositivos que vendem, e 77% querem que o governo faça mais para regular a maneira como as empresas coletam e usam esses dados.

E o caminho para equilibrar o que os consumidores esperam e o que as empresas oferecem parece ser longo. O estudo revela que apenas 41% dos consumidores consideram ser mais fácil proteger os seus dados online e só 34% deles acham que as empresas são transparentes quanto à forma como utilizam os dados coletados em diversos serviços online. Garantir um ambiente digital mais seguro exige um esforço conjunto entre usuários, fabricantes e legisladores para equilibrar inovação, privacidade e proteção de dados.



CAPÍTULO 4

Direitos digitais dos consumidores: transparência, consentimento e acesso


O boom do comércio eletrônico nos últimos anos desencadeou não só o crescimento exponencial do volume de dados que circula pelas empresas como também provocou uma disrupção significativa no comportamento do consumidor, transformando a forma como as empresas interagem com seus clientes.

Nesse contexto, a instantaneidade e a personalização ganharam destaque, tornando-se premissas fundamentais na experiência do cliente.

Além disso, hoje o consumidor busca uma relação mais próxima com as marcas, desejando ser reconhecido individualmente, independentemente do ponto de contato pelo qual se comunica com as companhias. Nessa jornada, a tecnologia tem papel fundamental. Um levantamento da Zendesk, por exemplo, aponta que 63% dos consumidores esperam que as marcas utilizem inteligência artificial para personalizar suas experiências.

Por outro lado, para atender a essa expectativa, as organizações têm acelerado o uso de ferramentas inteligentes para aprimorar a interação, como tecnologias que favorecem a coleta de dados em tempo real, chatbots alimentados por inteligência artificial e integração de soluções omnichannel.

Nessa jornada, mesmo com a criação do Marco Civil da Internet (Lei 12.965, de 2014) - com o objetivo de estabelecer o direito ao exercício da cidadania nos meios digitais e garantir a liberdade de expressão na internet -, até hoje existe muita polêmica sobre os direitos digitais dos consumidores no Brasil. “Tanto que os órgãos de defesa do consumidor têm muita dificuldade de lidar com a regra de responsabilização”, afirma Pedro Barata, sócio do escritório Pinheiro Neto Advogados e especialista em relações de consumo.



Pesquisa da Zendesk mostra que 63% dos consumidores esperam que as marcas utilizem IA para personalizar suas experiências

Outro ponto que merece atenção envolve a transparência de dados. “Podemos dividir esse assunto em duas vertentes: a questão da transparência das regras da relação comercial de determinado consumidor com o site que é regulado por meio de termos de uso; e a transparência de como se usa os dados pessoais. E esses pontos se tornaram muito importantes também na relação de consumo”, argumenta Larissa Galimberti, sócia do escritório Pinheiro Neto Advogados e especialista em proteção de dados.

Ainda de acordo com a especialista, com a evolução das tecnologias, percebeu-se que os dados traziam informações relevantes, seja para manter o consumidor engajado, seja para conseguir ofertar melhores produtos e serviços. “Dessa forma, principalmente nos artigos 6 e 9 da [Lei Geral de Proteção de Dados \(LGPD\)](#), que abordam como a empresa tem de dar essa informação com transparência, as companhias precisam deixar bastante claras as

finalidades do uso dos dados por meio da política de privacidade”, exemplifica a advogada.

Por isso, de acordo com Barata, é importante que as empresas adotem uma comunicação transparente e informativa a respeito do tratamento dos dados dos usuários. Além disso, ele conta que existe uma proposta para a criação de um sistema de sinalização gráfica que chame a atenção do usuário sobre o uso consciente de dados. “Seria algo parecido com as informações nutricionais dos rótulos de alimentos. O usuário entra no site e já na página principal aparecem ícones que apontam que naquela hospedagem são usados cookies, que alguns dados são compartilhados, que coletam dados de geolocalização, entre outros pontos importantes”, comenta.

Tendências e desafios futuros

O que esperar para os próximos anos envolvendo os direitos digitais dos consumidores brasileiros? Para Barata, um grande desafio é como lidar com a inteligência artificial. “O uso da IA aumentou de uma forma exponencial. E aí, especificamente para compras pela internet, existe a questão da internacionalização do acesso. Hoje é muito fácil acessar um marketplace de fora do Brasil, e isso traz uma série de desafios”, afirma. Isso porque, se o usuário comprar produtos num

site internacional que não são aprovados no Brasil, por exemplo, é muito provável que esse objeto não vá funcionar ou que vá ter um funcionamento intermitente. “A questão é como educar o consumidor para evitar esse tipo de problema?”, questiona o especialista.

Relação consumidor versus empresas ao longo do tempo

A evolução dessa relação começou a partir do Marco Civil da Internet, projeto criado com a intenção de trazer uma regulação de direitos e obrigações na internet. “Logo de início, o Marco Civil trouxe a garantia de que na internet é necessário ter a proteção de dados dos usuários e, por outro lado, a liberdade de expressão”, esclarece Galimberti.

Paralelo a isso veio o Decreto do Comércio Eletrônico, que trata sobre os direitos digitais dos consumidores. “A ideia do decreto, portanto, era tentar dar um pouco de concretude para os princípios do Código de Defesa do Consumidor nas relações mantidas, principalmente, pela internet”, explica Barata.

Na sequência, em 2020, entra em vigor a Lei Geral de Proteção de Dados (LGPD). Nesse caso, não é aplicada ao consumidor em si, mas ajuda a manter uma relação mais transparente com qualquer pessoa física cujos dados estão sendo usados. “Afinal de contas, os dados pessoais dos usuários, como nome, CPF, endereço e e-mail, passaram a ser regulamentados”, comenta Galimberti.

Já em relação ao uso de dados especificamente, Barata comenta que um ponto primordial será o fortalecimento da cibersegurança. Uma ideia trazida pelo advogado seria um documento de identidade em formato de token anônimo. “Por exemplo, a plataforma onde estou comprando não precisa saber que sou eu, Pedro, mas por meio do token é possível entender que é um homem, de 43 anos, o que já garante o acesso ao site”, explica.

Em relação à proteção de dados, Galimberti destaca a importância da Autoridade Nacional de Proteção de Dados (ANPD) no cenário brasileiro, órgão responsável por fiscalizar e promover a educação em relação à proteção de dados pessoais. Segundo a advogada, esse marco regulatório encontra-se em constante evolução e a iminente publicação de um guia sobre a figura do encarregado de proteção de dados, responsável por garantir a conformidade do tratamento de dados pessoais nas empresas, demonstra esse dinamismo. “Esse profissional é o responsável por comunicações internas e externas sobre proteção de dados e por orientar funcionários sobre as práticas de proteção de dados. E isso é bem interessante porque as transformações ocorrem e vão moldando a regulamentação”, conclui.

Sobre MIT Sloan Management Review Brasil

A **MIT Sloan Management Review Brasil** explora as principais tendências globais em gestão, inovação e liderança, trazendo insights estratégicos para que os profissionais se adaptem a um mundo de negócios dinâmico. Agora, a MIT SMR Brasil faz parte do portfólio do CNEX, um centro de formação executiva que atua no desenvolvimento e capacitação de lideranças das principais indústrias e companhias do País. Com mais de 38 anos de história, o CNEX prepara executivos para enfrentar desafios cada vez mais complexos por meio de imersões internacionais, programas intensivos, curadoria e eventos de conteúdo, além de pesquisas e estudos aplicados.

MIT SloanReview Brasil

www.mitsloanreview.com.br



Sobre Pinheiro Neto Advogados

Pinheiro Neto Advogados possui uma história de mais de 80 anos na área jurídica. A equipe multidisciplinar do escritório é formada por advogados especializados em todas as áreas do direito e oferece suporte jurídico abrangente e personalizado para empresas brasileiras e estrangeiras, potencializando seus negócios. Comprometido com os mais elevados padrões éticos, Pinheiro Neto Advogados tem como pilares fundamentais a tradição, a inovação e a responsabilidade socioambiental. Com escritórios em São Paulo, Rio de Janeiro, Brasília, Palo Alto (EUA) e Tóquio (Japão), o escritório é reconhecido com destaque nos principais rankings jurídicos internacionais.

PINHEIRO NETO
ADVOGADOS

www.pinheironeto.com.br

