C A R T I L H A

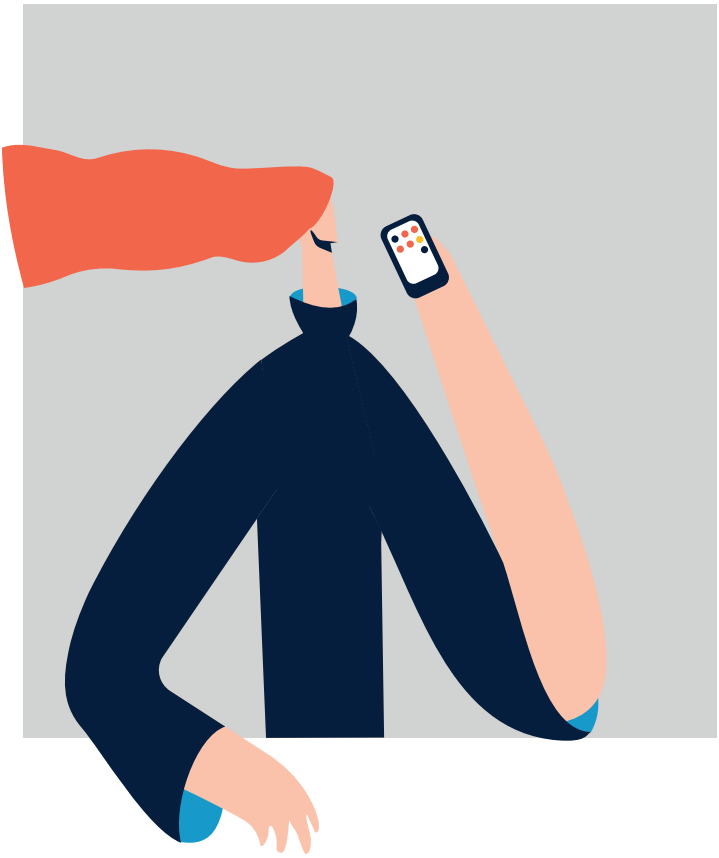
PROTEÇÃO DE DADOS PESSOAIS

abradi

ASSOCIAÇÃO BRASILEIRA DOS AGENTES DIGITAIS

C A R T I L H A

PROTEÇÃO DE DADOS PESSOAIS



SUMÁRIO

A ABRADi É UMA ENTIDADE QUE DEFENDE OS INTERESSES DOS AGENTES DIGITAIS NO BRASIL.

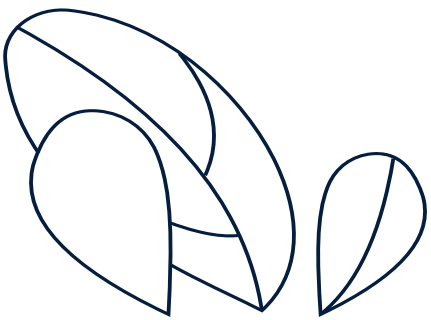
Reunindo cerca de 600 empresas por todo o país. Esta associação visa propiciar sempre um ambiente democrático e inclusivo aos Agentes Digitais, trazendo soluções e estimulando os associados a colaborarem ativamente na discussão de normas e a dialogar francamente com o mercado e os demais setores da sociedade. Imbuída desse espírito, a ABRADi criou a presente *Cartilha de Proteção de Dados Pessoais* com o intuito de esclarecer aos Agentes Digitais as obrigações legais criadas a estes pela Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), conscientizando-os acerca da mudança cultural proposta por essa nova legislação, bem como buscando auxiliá-los no processo de adequação à norma.

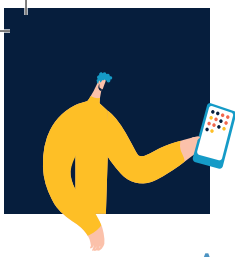
A ABRADi acredita que o Processo de Adequação à LGPD poderá criar diversas oportunidades de negócio e irá impulsionar os produtos e serviços ofertados pelos Agentes Digitais ao mercado, agregando a estes o diferencial do *compliance*: a privacidade.

Nesse sentido, a ABRADi pretende trazer, nas próximas páginas, os pontos da LGPD de maior relevância e impacto aos Agentes Digitais, de forma a auxiliá-los no Processo de Adequação, e colocar-se à disposição para eventuais dúvidas, já que o tema é demasiadamente complexo para ser esgotado neste documento.

Marcelo Sousa
Presidente da ABRADi

Vitor Morais de Andrade
Sócio LTSA Advogados





INTRODUÇÃO

APÓS ANOS DE DISCUSSÕES,

a Lei Geral de Proteção de Dados Pessoais (LGPD) virou realidade em 2018 e passará a vigorar em agosto de 2020. Trata-se de uma lei construída em conjunto por governo, sociedade civil e setor empresarial, merecendo especial destaque a participação do Setor de Comunicação, no qual a ABRADi está inserida.

Embora ainda haja muitos pontos a serem regulamentados, a LGPD trará segurança jurídica não só aos consumidores e titulares de dados, mas também a todos que de alguma forma manipulam informações no desenvolvimento de suas atividades comerciais – incluindo nós, os Agentes Digitais.

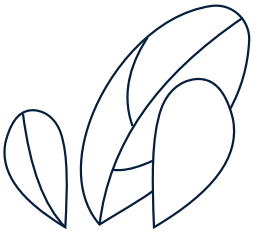
A lei concede aos Agentes Digitais parâmetros legais para desenvolverem suas atividades sem infringir a privacidade e a proteção de dados do titular, bem como impõe limites de atuação ao Poder Público, evitando, de certo modo, a aplicação de sanções de forma descabida.

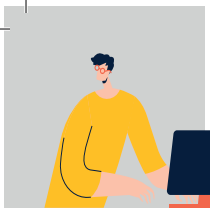
Imbuída neste espírito, a ABRADi criou, com o apoio da LTSA Advogados, a presente *Cartilha de Proteção de Dados Pessoais* com o intuito de esclarecer aos Agentes Digitais as obrigações legais criadas a estes pela Lei.

Nesse contexto, a presente cartilha visa trazer, de modo objetivo e sem a pretensão de esgotar os temas tratados na LGPD, orientações aos Agentes Digitais sobre essa nova legislação, para que todos estejamos devidamente preparados.

São fundamentos da LGPD:

- Respeito à privacidade;
- Inviolabilidade da intimidade, da honra e da imagem;
- Autodeterminação informativa;
- A liberdade de expressão, de informação, de comunicação e de opinião;
- Desenvolvimento econômico e tecnológico, e inovação;
- Livre-iniciativa, livre concorrência e a defesa do consumidor;
- Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.



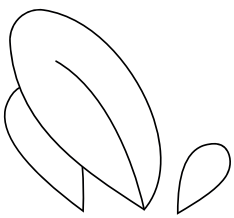


OPORTUNIDADE DE NEGÓCIOS PARA OS AGENTES

O AGENTE DIGITAL TEM UMA OPORTUNIDADE PRECIOSA À SUA FRENTE:

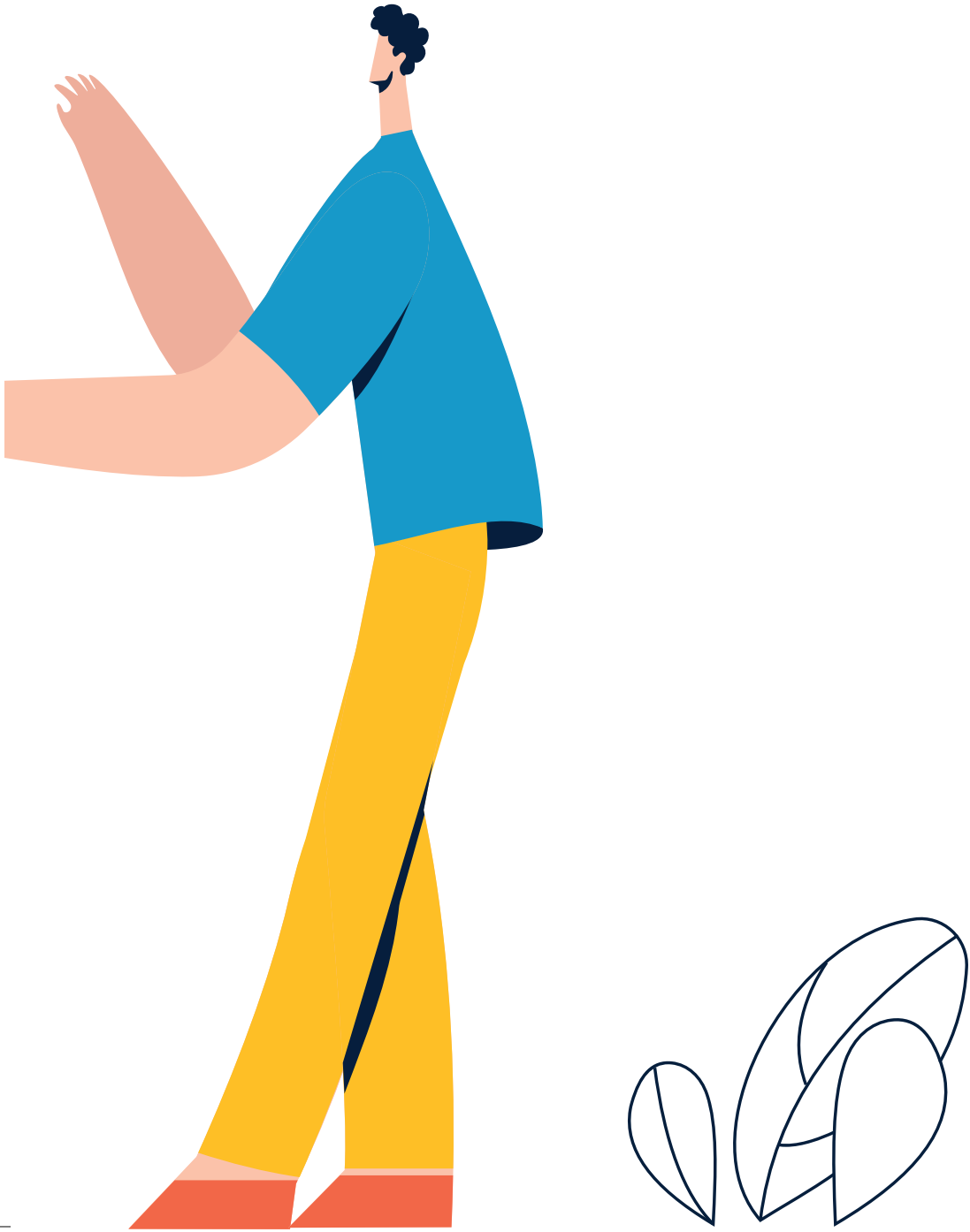
tempo para se adaptar e obter vantagem econômica pela oferta de produtos e serviços diferenciados em razão da adequação à LGPD – que é uma demanda de todos os anunciantes.

Em outras palavras, a regulamentação possibilitará aos Agentes Digitais assumir um compromisso definitivo com a privacidade dos titulares de dados, o que trará a estes e aos clientes confiança e transparência.



QUAIS SÃO OS BENEFÍCIOS PARA OS AGENTES DIGITAIS?

- A oportunidade de oferecer produtos diferenciados, pois as empresas que se adaptarem primeiro estarão à frente no mercado;
- O valor agregado aos dados coletados de forma regular e com origem definida torna-se maior no mercado;
- A possibilidade de participar do mercado internacional em países que possuem leis de proteção de dados; e
- A possibilidade de empresas ingressarem no mercado digital de forma responsável.



PRINCÍPIOS DA LGPD

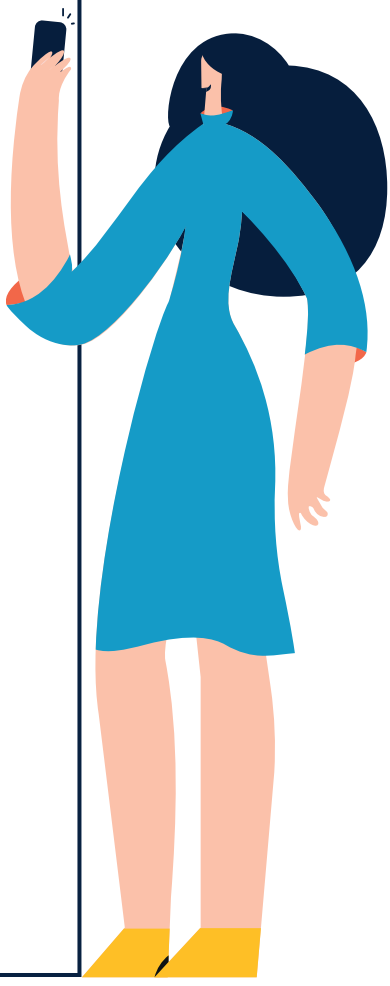
A LGPD APRESENTA UM ROL DE 10 PRINCÍPIOS BASILARES PARA NORTEAR TODA A ATIVIDADE DE TRATAMENTO DE DADOS PESSOAIS. SÃO ELES:

1 **Finalidade:** realizar tratamento com fins legítimos, específicos, explícitos e informados ao titular, de modo que o tratamento não pode fugir à finalidade divulgada ao titular – caso destoe, será necessário, muitas vezes, colher novo consentimento, se o tratamento não puder ser enquadrado em outra base legal;

2 **Adequação:** ajustar a atividade de tratamento de acordo com a finalidade divulgada ao titular de dados pessoais;

3 **Necessidade:** tratar somente os dados pessoais que forem necessários à persecução da finalidade informada – não se deve coletar ou manter dados pessoais que não possuam destinação certa, finalidade definida;

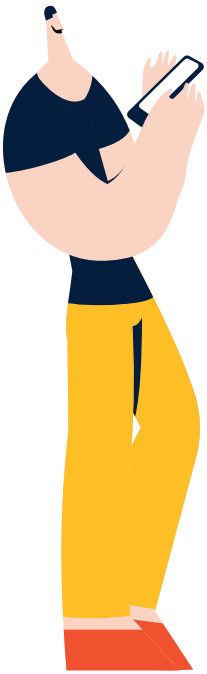
4 **Livre acesso:** possibilitar aos titulares consulta acessível e sem custo sobre a forma e a duração do tratamento, assim como sobre a integralidade de seus dados pessoais;



5 **Qualidade dos dados:** garantir aos titulares correção, clareza e atualização de seus dados pessoais em posse do agente de tratamento, considerando os princípios da necessidade e finalidade do tratamento de dados;

6 **Transparência:** garantir aos titulares de dados pessoais informações relevantes claras, precisas e de fácil acesso a respeito do tratamento de seus dados, resguardados segredos comerciais e industriais dos agentes de tratamento envolvidos;

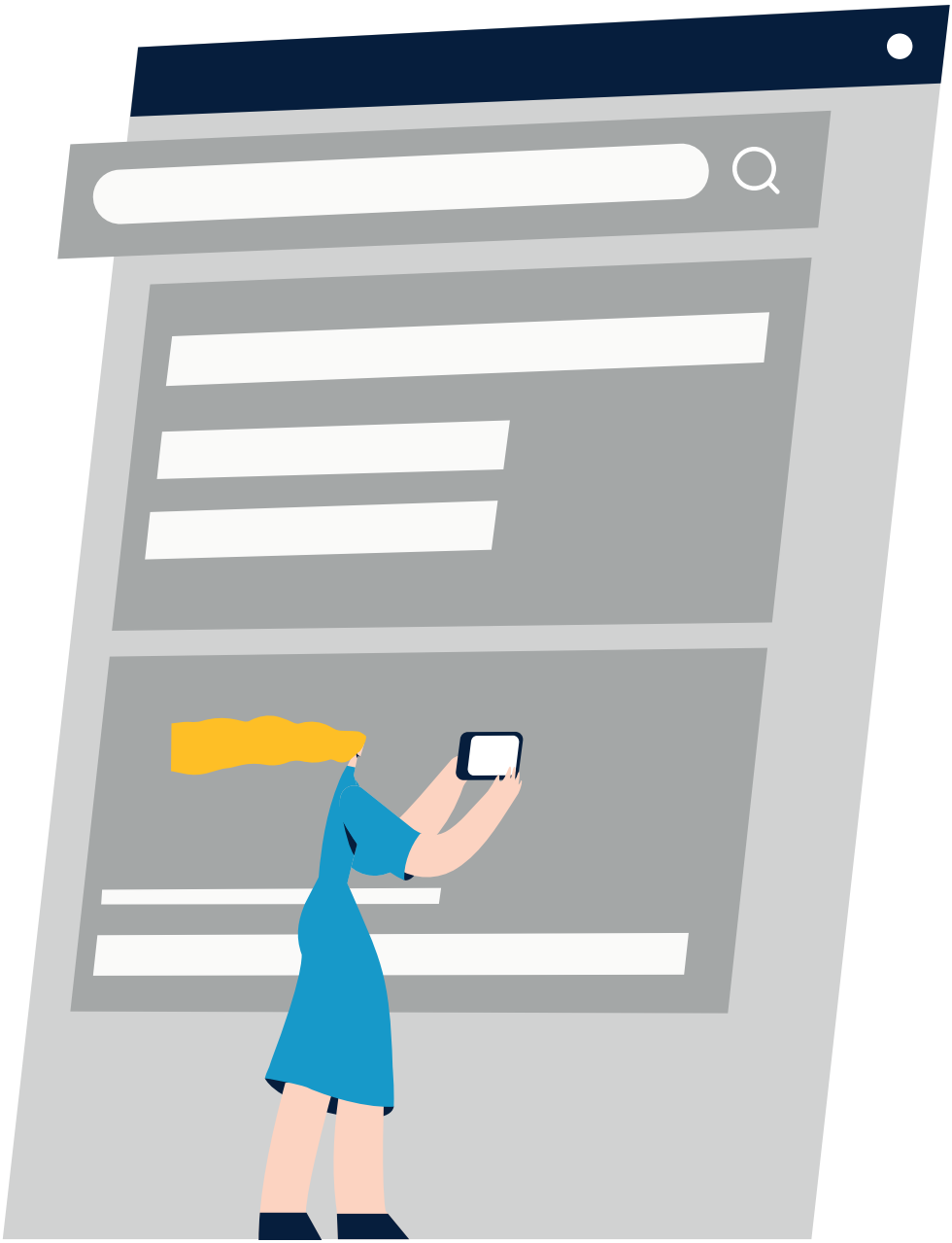
7 **Segurança:** adoção de medidas suficientemente aptas a assegurar os dados pessoais de acessos desautorizados, ocorrências acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;



8 **Prevenção:** adoção de medidas aptas à prevenção de danos, decorrentes do tratamento de dados pessoais;

9 **Não discriminação:** não realização de tratamento de dados pessoais com propósitos discriminatórios, ilícitos ou abusivos; e

10 **Responsabilização e prestação de contas:** capacidade do agente em demonstrar a adoção de medidas eficazes e suficientes para comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

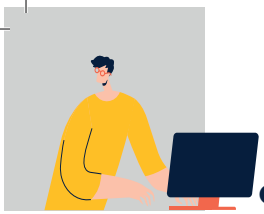


O TITULAR DOS DADOS É A PESSOA

a quem as informações tratadas se referem, e a este a LGPD elencou um rol de direitos, visando a transparência do tratamento de dados e o controle do titular sobre este. Nesse sentido, a LGPD coloca como obrigação do controlador – quem decide a respeito da utilização dos dados, geralmente o anunciante – garantir ao titular de dados:

- Confirmação da existência do tratamento;
- Acesso aos dados;
- Correção de dados;
- Anonimização, bloqueio e eliminação de dados;
- Portabilidade de dados;

- Informação sobre compartilhamento de dados pessoais;
- Informação sobre a possibilidade de não consentir o tratamento e as consequências da negativa; e
- Possibilidade de revogar o consentimento.



OS AGENTES DIGITAIS PRECISARÃO ESTAR EM *COMPLIANCE*,

ou seja, estar de acordo com a LGPD quando a lei entrar em vigor em agosto de 2020. Por isso, é preciso estabelecer um cronograma prévio de adequação, para que seja possível cumprir a legislação com tranquilidade. Nesse sentido, a ABRADi enumera alguns dos principais pontos de observância para um Agente Digital no desenvolvimento de seu Programa *Compliance* com a LGPD:

1° – No tratamento dos dados, respeitar sempre a **finalidade para a qual o dado foi compartilhado, além de observar, no momento da coleta, as bases legais instituídas pela LGPD**;

2° – Manter os registros das operações de tratamento de dados pessoais que realizar, a fim de cumprir com o princípio da **prestação de contas**;

3° – Adoção de medidas suficientemente aptas a assegurar os dados pessoais de acessos desautorizados, ocorrências acidentais ou ilícitas, garantindo a **segurança** de todo o fluxo de dados pessoais;

4° – Escolher **parceiros com nível adequado de proteção de dados**;

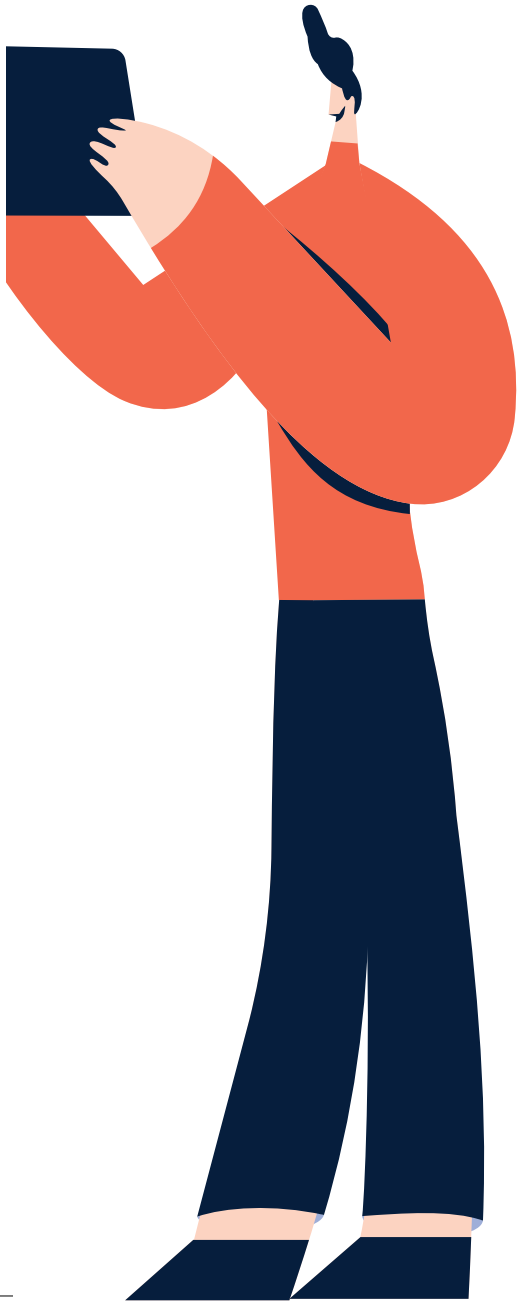
5° – Caso, em algumas das atividades, sua agência possa ser classificada como "controladora", sugere-se nomear um **encarregado** pelo tratamento de dados pessoais[1];

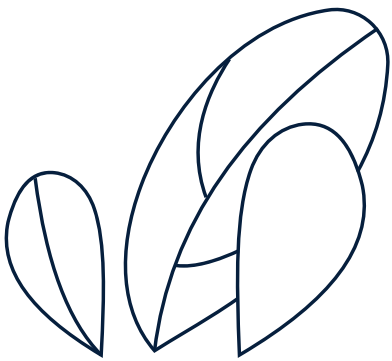
6° – Se atuar como um controlador, deve conceder ao titular o **direito de acesso, retificação, cancelamento e portabilidade dos dados pessoais**, disponibilizando um canal próprio para isso, e exigir que eventuais retificações/cancelamentos dos dados sejam replicadas(os) ao longo da cadeia de tratamento;

7° – Avaliar, mapear os fluxos de dados, fazer inventário de dados e Relatório de Impacto à Proteção de Dados Pessoais, de forma a apurar os potenciais riscos à privacidade dos titulares e estabelecer medidas de solução; e

8° – Estabelecer uma **política corporativa de privacidade, regras de boas práticas e governança sobre proteção de dados pessoais e revisar cláusulas contratuais e demais documentos** que envolvam a temática de tratamento de dados pessoais.

1 Devido às alterações promovidas pela Lei nº 13.853/2019, proveniente da Medida Provisória nº 869/2018, publicada em 09 de julho de 2019, o encarregado poderá ser necessário para empresa classificada como "operador" em hipóteses a serem reguladas pela Autoridade Nacional de Proteção de Dados (ANPD).





A) O QUE SÃO DADOS PESSOAIS?

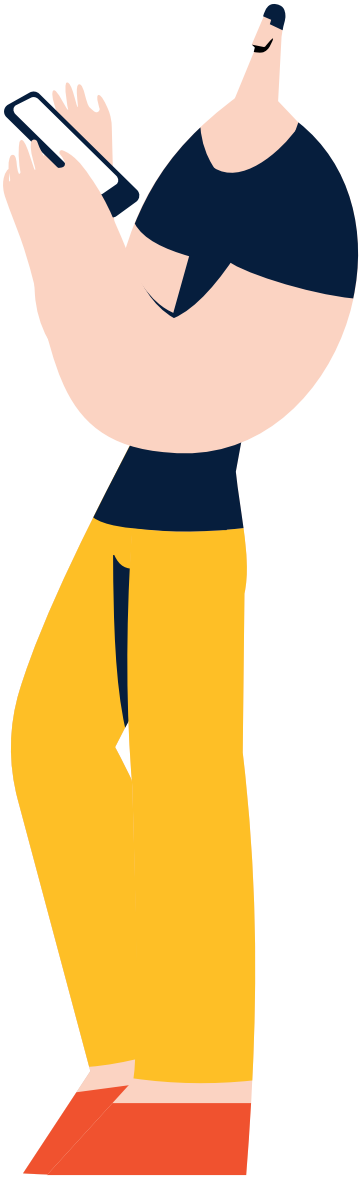
A LGPD, à luz do que já havia sedimentado o GDPR (Regulamento europeu de proteção de dados), definiu dados pessoais como informações relacionadas à pessoa natural, que possibilitam sua identificação, direta ou indiretamente. Assim, podemos entender como exemplos de dados pessoais: CPF, RG, profissão, IP, entre outros dados que nos permitam identificar alguém. Sendo assim, dados anonimizados não são considerados dados pessoais, não sendo estes sujeitos às aplicações da lei.

B) O QUE SÃO DADOS PESSOAIS SENSÍVEIS?

Dados pessoais sensíveis são considerados uma categoria especial de dados pela LGPD, que atribui ao tratamento dela algumas particularidades, bem como a define como todo dado pessoal que se refira a: origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou à 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. Note, que, muitas vezes, apesar de o dado pessoal demandar certa confidencialidade e dever de sigilo, como é o caso dos dados bancários e perfis de compras, ele nem sempre será tratado como sensível pela LGPD.

C) *COOKIES* E IPS DE MÁQUINA SÃO CONSIDERADOS DADOS PESSOAIS PERANTE A LEI?

Conforme definido acima, dados pessoais são informações que possibilitam a identificação de um indivíduo. Assim, pensando nesse conceito – embora a LGPD não defina expressamente o número do IP e do *cookie* como dado pessoal –, o GDPR traz a interpretação de que, pela natureza identificadora do IP e do *cookie*, eles podem ser usados como ferramentas para definição de perfis e identificação de pessoas – o que se encaixa no conceito de dado pessoal. Sobre o IP dinâmico, existem entre os pareceres emitidos pelo Grupo de Trabalho de Proteção de Dados Pessoais do artigo 29 e o Parecer nº 4/2007, que, em resumo, define: ao registrar sistematicamente data, hora, duração e IP, mesmo que dinâmico, é possível identificar o usuário, utilizando meios razoáveis. Por isso, também é enquadrado como dado pessoal.



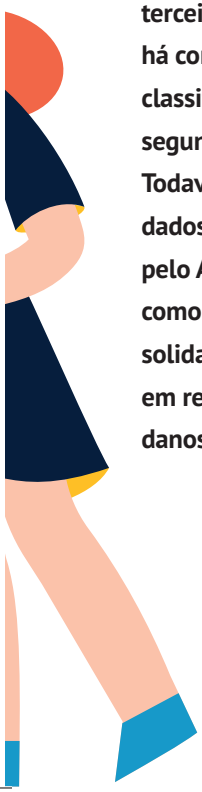
D) COMO AS AGÊNCIAS DIGITAIS PODEM SER CLASSIFICADAS: SÃO OPERADORES DE DADOS OU CONTROLADORES? QUAL É A RELEVÂNCIA DESSA DIFERENCIAÇÃO?

A LGPD classifica os agentes de tratamento de dados em controlador e operador. Controlador de dados é o responsável por tomar decisões acerca do tratamento de dados; o operador de dados segue as instruções daquele, operacionalizando tão somente o tratamento dos dados pessoais.

O mais comum seria classificar os Agentes Digitais como operadores, vez em que normalmente executam os tratamentos de dados seguindo a determinação de seus clientes, os controladores. Quando realizamos uma campanha de *e-mail marketing*, por exemplo, embora sejamos responsáveis pela criação do HTML e pelo disparo, estamos seguindo recomendações específicas do anunciante, que também foi o responsável pela captura do *mailing* do cliente. Essa diferenciação é essencial, pois a LGPD distribui de forma distinta as obrigações e as responsabilidades dos agentes. Se a Agência Digital for entendida como controladora com o seu cliente, eventual violação à legislação de proteção de dados gerará corresponsabilidade em reparar o dano.

E) SE, AO TRANSFERIR DADOS PESSOAIS ORIGINADOS DE BANCOS DE DADOS DE CLIENTES PARA UMA EMPRESA TERCEIRA, QUE REALIZA DISPAROS DE E-MAIL, OCORRER UM VAZAMENTO DE DADOS, A MINHA AGÊNCIA SERÁ CORRESPONSÁVEL?

Se o Agente Digital em questão transferir dados pessoais do banco de dados de seu cliente para a empresa terceira por determinação do cliente, em razão de a terceira ser sua parceira, nesse caso, não há corresponsabilidade, pois o agente será classificado como operador e terá agido segundo as instruções do controlador. Todavia, se a decisão de compartilhar os dados com empresa terceira for tomada pelo Agente Digital, ele será classificado como controlador e responderá solidariamente, isto é, será corresponsável em relação à reparação de eventuais danos sofridos pelos titulares dos dados.

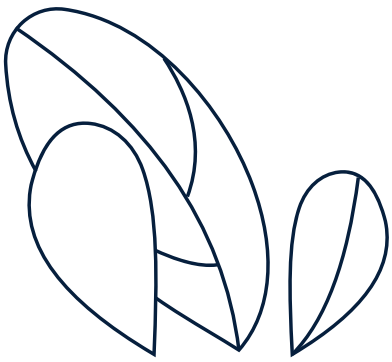


F) QUAL É O JEITO CORRETO DE CAPTURAR DADOS?

Como ponto de partida, é necessário entender que, segundo a LGPD, os dados coletados pertencem ao indivíduo ao qual dizem respeito, de forma que qualquer tipo de tratamento de dados realizado está condicionado aos requisitos impostos pela lei e pelas demais legislações que tratam do tema. Dessa forma, o tratamento de dados pessoais deve se restringir a propósitos legítimos e à finalidade específica informada ao titular de dados pessoais, no momento da coleta.

Além disso, o tratamento de dados pelos Agentes Digitais deve sempre estar fundamentado em uma das seguintes hipóteses enumeradas pela LGPD – do contrário, será ilegal:

- **Consentimento (escrito ou por meio que demonstre a vontade do titular);**
- **Cumprimento de obrigação legal;**
- **Necessidade para execução contratual;**
- **Exercício regular de direitos em processo judicial, administrativo ou arbitral;**
- **Proteção à vida ou incolumidade física do titular ou de terceiro;**
- **Tutela da saúde;**
- **Atendimento de legítimo interesse do controlador (quem exerce poder de decisão sobre o tratamento dos dados) ou terceiro;**
- **Proteção de crédito; e,**
- **Em razão da publicidade dada aos dados por seu titular ou do acesso público irrestrito a este, desde que observados a finalidade com que o dado foi disponibilizado, a boa-fé e se não fere direitos e garantias fundamentais.**



G) QUANDO É NECESSÁRIO OBTER O CONSENTIMENTO DO TITULAR DE DADOS PESSOAIS?

O consentimento, como visto no questionamento anterior, é apenas uma das bases legais a fundamentar o tratamento de dados pessoais; sendo assim, é necessário coletar e guardar o registro do consentimento quando o tratamento não se encaixar em nenhuma das demais bases legais de tratamento. Por exemplo, uma empresa que capture dados para fins de prevenção a fraudes não necessitaria da coleta do consentimento, visto que "proteção ao crédito" é uma das bases legais.

H) DADOS CAPTURADOS EM REDES SOCIAIS, COMO WHATSAPP E FACEBOOK, SÃO CONSIDERADOS PESSOAIS?

Dados pessoais são informações relacionadas à pessoa natural identificada ou identificável; assim, o meio pelo qual são capturados não altera a sua natureza, pois os dados continuam sendo pessoais e de titularidade da pessoa a que se referem.

No caso do WhatsApp, os dados são veiculados em conversas privadas ou para grupos de pessoas; ainda que se verifique certa publicidade dos dados, ela é limitada. Assim, uma eventual utilização desses dados deve enquadrar-se em uma das bases legais; do contrário, será indevida.

Em relação ao Facebook, se os dados estiverem abertos a todos e a informação tiver sido publicada pelo titular, configurará a hipótese da coleta de dados tornados manifestamente públicos pelo titular, sendo possível a sua utilização para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento de dados, e desde que preservados os direitos do titular.

Se os dados não foram divulgados com esse intuito, esse tipo de tratamento não estaria sob o manto da boa-fé.

I) QUAIS SÃO AS INFORMAÇÕES OBRIGATÓRIAS QUE DEVEM CONSTAR DOS TERMOS DE CONSENTIMENTO DO USUÁRIO?

Deste termo deverão constar: a finalidade específica do tratamento; com quem eventualmente aquele dado pessoal será compartilhado; qual será o período de duração do tratamento; a informação da possibilidade de não fornecer o consentimento; e quais seriam as consequências da negativa. Além disso, o termo deverá consistir em manifestação livre (verdadeira escolha, decisão voluntária), informada (informação completa, exata, disponibilizada de forma clara e compreensível) e inequívoca (o procedimento para a obtenção do consentimento não pode dar margem à dúvida quanto à intenção da pessoa em dar o seu consentimento).

Diante disso, não são mais aceitos ou vistos como manifestação de consentimento válido comportamentos de omissão (*opt-out*), como caixas previamente assinaladas.

J) O QUE PODE SER ENTENDIDO COMO TRATAMENTO DE DADOS?

A LGPD conceitua o tratamento de dados como 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.
Assim, toda operação que envolva informações capazes de identificar alguém direta ou

indiretamente é considerada tratamento de dados pessoais, podendo encontrar-se entre os exemplos práticos o serviço de tratamento e de duplicação de dados *(data quality)*, a seleção de públicos para audiência para campanhas, o desenvolvimento de modelos e algoritmos com dados de cliente, o enriquecimento de banco de dados com listas externas e os serviços de geolocalização.

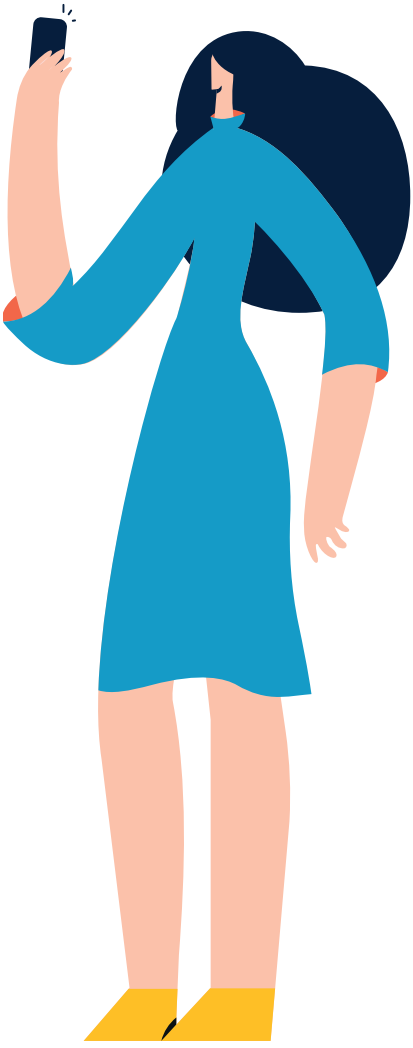
K) POSSO CONTINUAR A COMPRAR DADOS EXTERNOS PARA ENRIQUECIMENTO?

A LGPD não faz nenhuma restrição expressa no tocante à utilização de bancos de dados externos; entretanto, caso se opte por esta possibilidade, deve-se tomar alguns cuidados: certificar-se de que a coleta dos dados externos esteja fundamentada em uma das bases legais previstas na LGPD; exigir do fornecedor os registros de coleta; averiguar se a finalidade divulgada ao titular de dados é compatível com o tratamento que será destinado aos dados; certificar-se de que o compartilhamento dos dados foi devidamente informado e consentido (caso essa seja a base legal utilizada) pelo titular de dados pessoais.

L) AINDA POSSO FAZER MÍDIA PROGRAMÁTICA UTILIZANDO DMPS (*DATA MANAGEMENT PLATFORM*)?

A LGPD não veio para pôr fim às ferramentas de marketing digital, mas será necessário que os Agentes Digitais, ao utilizá-las, tomem algumas precauções e respeitem os limites legais. Dessa forma, como as DMPs envolvem coleta e tratamento de dados pessoais, elas deverão respeitar o *privacy by design*, consistindo em plataformas que cumpram os requisitos legais impostos pela LGPD para tratamento de dados pessoais. É necessário sempre questionar e exigir comprovações acerca da origem dos dados coletados e oferecidos.

M) SERÁ POSSÍVEL USAR DADOS DE GEOLOCALIZAÇÃO DENTRO DOS CRITÉRIOS DA LEI PARA REALIZAR CAMPANHAS DE MARKETING DIGITAL?



Da mesma forma como as demais práticas, a realização de campanhas por dados de geolocalização não foi inviabilizada pela LGPD. Se os dados estiverem anonimizados, ou seja, se o seu titular não puder ser identificado por esforços técnicos razoáveis, não há impedimento, visto que dados anonimizados não são considerados dados pessoais, de forma que a LGPD não se aplica a eles.

Por outro lado, caso seja possível a identificação do indivíduo, os dados de geolocalização estarão sob o manto da LGPD e a eles deverão ser destinados os mesmos cuidados que aos demais dados pessoais.

N) QUAIS SÃO AS CERTIFICAÇÕES DE SEGURANÇA QUE ATENDEM À LEI?

Em relação à temática da segurança, a LGPD exige que os Agentes Digitais façam uso 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. Isso significa que, em todo o fluxo de dados pessoais, não pode haver falhas de segurança que possibilitem acesso não autorizado. As licenças devem ser válidas, os softwares devem ser atualizados, os funcionários devem ser conscientizados acerca das medidas de segurança etc.

Apesar de a legislação não exigir certificações, a ISO 27001 – padrão para gestão da segurança da informação – tem sido em muito utilizada para o cumprimento deste requisito da LGPD.

O) O QUE SIGNIFICA *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*?

O *privacy by design* visa a utilização de mecanismos de privacidade em todo o ciclo do dado a ser tratado. A privacidade deve ser incorporada ao desenho do produto ou serviço, de modo a assegurar todo o fluxo do dado, desde a coleta até o término do tratamento.

O *privacy by default*, por sua vez, introduz a privacidade como modelo de conduta, de modo a minimizar o processamento de dados pessoais, pela adoção de técnicas como a pseudononimização e a criptografia. São modelos que devem ser adotados pelos Agentes Digitais com o objetivo de propiciar o cumprimento dos demais requisitos legais para o atingimento de um tratamento de dados que respeite efetivamente a privacidade.

P) QUAIS SÃO AS PENALIDADES PREVISTAS NA LEI PARA QUEM NÃO ESTIVER EM *COMPLIANCE*?

Quem não se adequar estará sujeito à fiscalização da Autoridade de Proteção de Dados Pessoais e às seguintes penas:

- **Advertência: com indicação de prazo para adoção de medidas corretivas;**
- **Multa: simples ou diária de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício – limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais), por infração;**
- **Publicização: após sua apuração e confirmação de ocorrência, com possibilidade de sanção em caso de vazamento de dados pessoais;**
- **Bloqueio dos dados: a que se refere a infração até a sua regularização; e**
- **Eliminação dos dados: a que se refere a infração.**

A aplicação das sanções será precedida de procedimento administrativo que possibilite a oportunidade de ampla defesa, de acordo com as peculiaridades do caso concreto.

Q) O QUE ACONTECE DIANTE DA OCORRÊNCIA DE UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO?

Em caso de ocorrência de qualquer incidente de segurança, o Agente Digital, caso opere como controlador, deverá notificar a Autoridade Nacional de Proteção de Dados, em tempo razoável. A LGPD não determina prazo certo – diferentemente do GDPR, que fixou o parâmetro de 72 horas, o qual poderá ser utilizado como orientador diante da atual lacuna de regulamentação nesse sentido.

Caso o Agente Digital atue como operador e detecte um incidente de segurança, deverá notificar o controlador a respeito, documentando devidamente essa notificação para eventual prestação de contas à Autoridade Nacional de Proteção de Dados.

A Autoridade Nacional de Proteção de Dados averiguará a gravidade do incidente, podendo determinar ao controlador a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

R) QUEM É RESPONSÁVEL PELO MONITORAMENTO DO CUMPRIMENTO DA LEI?

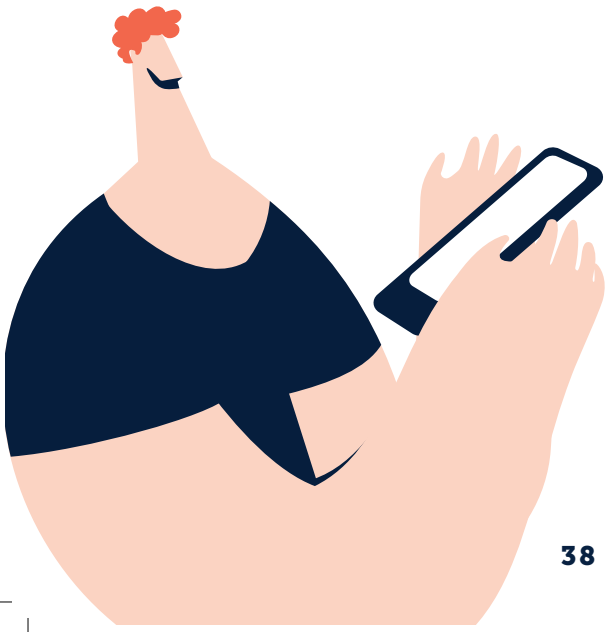
Em 09 de julho de 2019, foi publicada a Lei nº 13.853, proveniente da Medida Provisória nº 869/2018, que criou a Autoridade de Proteção de Dados (ANPD). Ela foi instituída como órgão da administração pública federal, integrante da Presidência da República, e possui a competência para fiscalizar e monitorar o cumprimento da LGPD, cabendo a esta a aplicação de sanções.

SERVIÇOS DE APOIO

Se esta cartilha ainda não foi suficiente para esclarecer as suas dúvidas, destacamos que o **associado ABRADi** possui **canais exclusivos** de apoio à implementação da LGPD. Envie sua dúvida pontual para o e-mail **lgpd@abradi.com.br** ou solicite um atendimento on-line em **http://bit.ly/atendimentoabradi**

CERTIFICAÇÃO

A **ABRADi** desenvolveu, em parceria com o Bureau Veritas e o escritório LTSA, uma **certificação exclusiva** para os Agentes Digitais, e um programa de *Compliance* e Adequação à Lei Geral de Proteção de Dados Pessoais exclusivo para associados. Para obter **mais informações**, envie uma mensagem para **lgpd@abradi.com.br**.



REFERÊNCIAS

GDPR. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679.

LGPD. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

Parecer nº 4/2007 do Grupo de Trabalho de Proteção de Dados do artigo 29, sobre o conceito de dados pessoais, 01248/07/PT, WP 136. Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf.

Parecer nº 15/2011, sobre a definição de consentimento. Disponível em: https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf.

Requisitos de Segurança enumerados pela ICO (Autoridade de Proteção de Dados Pessoais do Reino Unido). Disponível em: https://ico.org.uk/for-organisations/the-guide-to-nis/security-requirements/.
Medida Provisória nº 869/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm.

DIRETORIA ABRADi

Marcelo Sousa
Presidente ABRADi
Marketdata

Carolina Morales
Vice-Presidente Executiva
IComunicação

Flávio Horta
2º Vice-Presidente
Digitalks

Paulo H. Ferreira
3º Vice-Presidente
Clickweb

Daltro Martins
4º Vice-Presidente
RPMA Comunicação

Miguel Taino
Diretor
E/OU MRM

Carlos Paulo Jr.
Diretor
Umbrella

Daniel Rimoli
Diretor
Burson Cohn & Wolfe

Juan Carlos Gozzer
Diretor
Llorente Y Cuenca

Sandro A. Fernandes
Diretor
Área Local

Ricardo Abel
Diretor
RCA

Erick Formaggio
Diretor
Whip

Fábio Trindade
Diretor de Comitês
Grupo Digital Business

Beatriz Ayrosa
Diretora
Becabiz

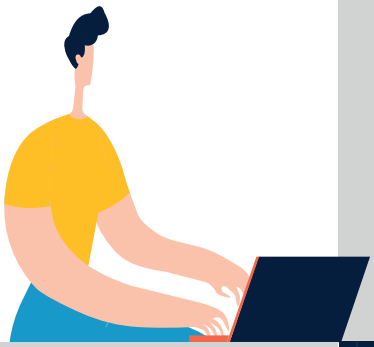
APOIO

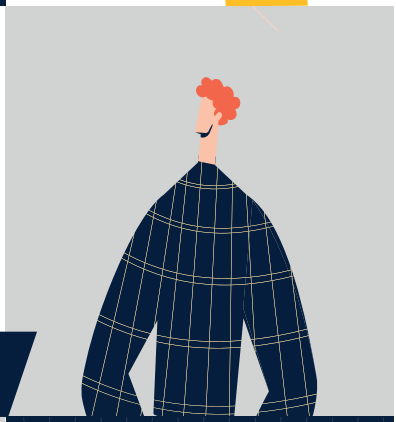
LTSA advogados

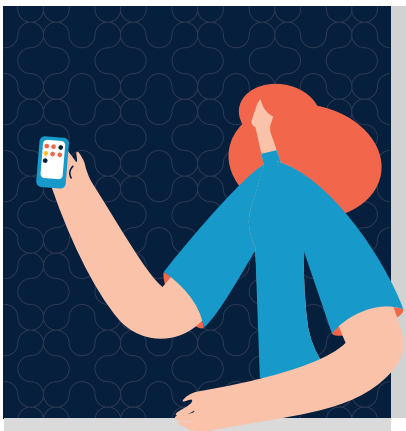
/ABRADiNACIONAL

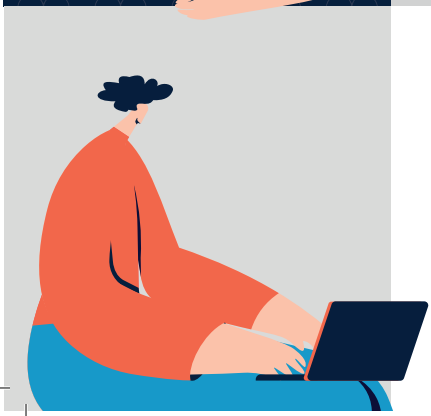
/ABRADi1

/ABRADi_NACIONAL









abradi

ASSOCIAÇÃO BRASILEIRA DOS AGENTES DIGITAIS