

comércio & serviços

CADASTRO DE CONSUMIDORES

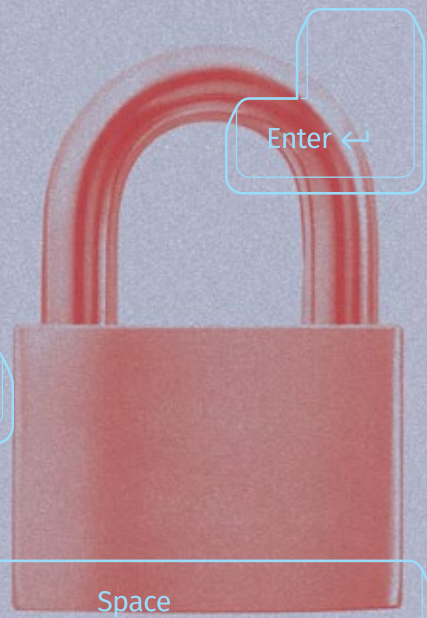
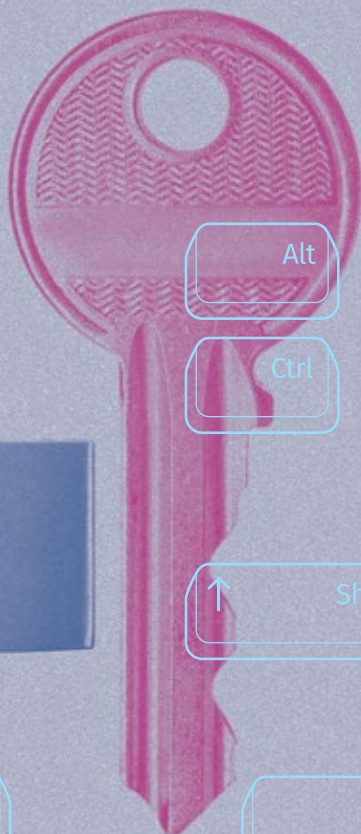
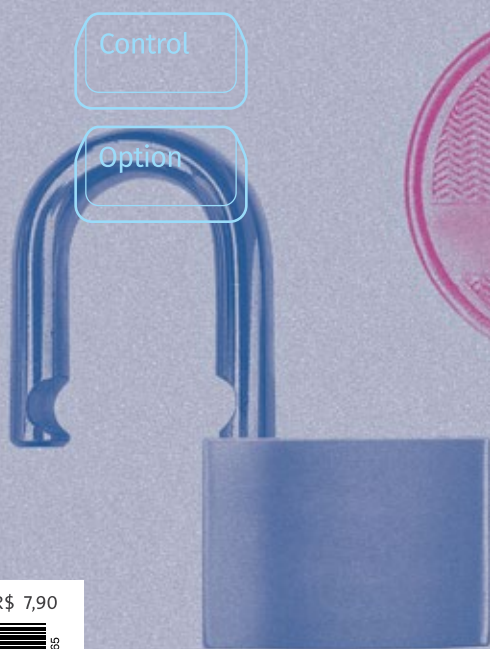
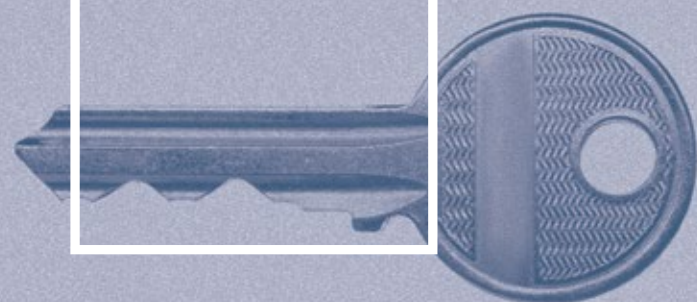
Passo a passo para
agir de acordo com
as novas regras

NO PRAZO E SEM MULTAS

Como se adaptar à
legislação, que passa
a valer em agosto

Lei Geral de Proteção de Dados

ENTENDA AS
EXIGÊNCIAS
OBRIGATÓRIAS
DE PRIVACIDADE.
SUA EMPRESA ESTÁ
PREPARADA?



Control

Option

Alt

Ctrl

Enter ←

↑ Shift

Command ⌘

Space

R\$ 7,90



PREPARADO PARA A NOVA LEI DE PROTEÇÃO DE DADOS?

Ponha a mão na massa e saia pronto para iniciar o seu processo de adequação.

Participe do evento feito para você ganhar tempo!
Trabalhe junto com profissionais que já estão coordenando os preparativos de grandes empresas.
Acelere sua adaptação com autoridades, consultores e empresários que são verdadeiras referências na LGPD.
Tenha um dia de imersão total, com muitas orientações práticas, e confira tudo o que precisa para aplicar na sua empresa.

Aprenda na prática com os maiores especialistas!

LGPD NA PRÁTICA

Coordenação

Renato Opice Blum

Fundador do escritório Opice Blum, Bruno, Abrusio, e Vainzof Advogados Associados; Mestre pela Florida Christian University; Coordenador do curso de Direito Digital do INSPER e do MBA em Direito Eletrônico da EPD; Presidente do Conselho de Comércio Eletrônico da FecomercioSP.

Rony Vainzof

Sócio do Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados; Coordenador e Professor do MBA em Direito Eletrônico da Escola Paulista de Direito; Vice-Presidente do Conselho de Comércio Eletrônico da FecomercioSP.



DO QUE VAMOS FALAR?

- LGPD no governo e a estruturação da ANPD
- Aspectos jurídicos e trabalhistas da LGPD
- Compliance digital e segurança da informação
- LGPD e GDPR – cases de sucesso na implantação da lei
- LGPD na prática: as mudanças necessárias no seu negócio
- Data Protection Officer (DPO)

24 DE ABRIL DAS 9H ÀS 16H

Descontos exclusivos para associados!

Mais informações e inscrições, acesse:
representa.fecomercio.com.br/eventos



FECOMERCIOSP
REPRESENTA MUITO PARA VOCÊ

SIGILO E SEGURANÇA: VALORES INEGOCIÁVEIS

O CONCEITO DE “PRIVACIDADE” nunca ocupou de forma tão intensa as discussões relacionadas à revolução tecnológica da última década. Com o incremento das ferramentas virtuais, o armazenamento de dados e sua interpretação pelas empresas têm despertado a preocupação do Poder Público e da sociedade.

Tema desta edição, a Lei Geral de Proteção de Dados (LGPD), prevista para entrar em vigor em agosto, exigirá conhecimento de profissionais de tecnologia e do Direito para que os sistemas digitais sejam aperfeiçoados de acordo com as novas regras de segurança da informação – que prezam, acima de tudo, pelo sigilo de dados pessoais.

Este número de **C&S** reúne vasto conteúdo sobre a LGPD, com orientações da assessoria técnica da FecomercioSP a respeito da implantação de programas de governança. Traz também a impressão de empresários sobre como eles estão encarando as adaptações à legislação em suas empresas. Nesse sentido, os setores de comércio e serviços devem lidar com essas adaptações como um diferencial competitivo no relacionamento com os clientes. Quem agir com transparência e responsabilidade será exemplo para o mercado.

Nesse contexto, ganha importância o papel da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e orientar a atuação das empresas públicas ou privadas – e com a qual a FecomercioSP, por meio do seu Conselho de Comércio Eletrônico, está mantendo constante diálogo. A Entidade entende que regulamentação é necessária. Mas deve ocorrer em sintonia com os pleitos do setor privado e sem comprometer a fluência do já intrincado ambiente de negócios brasileiro.

Esta revista integra um material multimídia preparado pela Federação para garantir ao leitor informações práticas acerca das mudanças que deverão ocorrer no cotidiano de seus negócios.

A todos, um bom proveito.

ABRAM SZAJMAN, presidente da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP), entidade que administra o Sesc e o Senac no Estado

Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo

PRESIDENTE Abram Szajman

SUPERINTENDENTE Antonio Carlos Borges

CONSELHO EDITORIAL

Antonio Carlos Borges, Ives Gandra Martins, José Goldemberg, José Pastore

ASSESSORIA TÉCNICA

Juliana Motta, Kelly Carvalho, Renato Opice Blum e Rony Vainzof

EDITORA



ESTRATÉGIA DE COMUNICAÇÃO INTEGRADA

Demian Russo

GERENTE DE CONTEÚDO

Elisa Klabunde

EDITOR E JORNALISTA RESPONSÁVEL

Lucas Mota MTB 46597/SP

EDITORA ASSISTENTE

Lúcia Helena de Camargo

REPÓRTER

Filipe Lopes

FOTÓGRAFO

Chistian Parente

ESTAGIÁRIA

Gabriela Henrique

DIRETORES DE ARTE

Clara Voegeli e Demian Russo

EDITORA DE ARTE

Carolina Lusser

DESIGNERS

Cintia Funchal, Daniel Monteiro, Joelson Buggilla, Paula Seco, Pedro Vó e Tiago Araujo

CAPA

Joelson Buggilla

REVISÃO

Bruna Baldini e Flávia Marques

COLABORAM NESTA EDIÇÃO

Aline Carvalho, Barbara Oliveira, Camila Silveira, Leda Rosa e Rafza Dias

REDAÇÃO

Rua Santa Cruz, 722, 5º andar
Vila Mariana – CEP 04122-000
São Paulo/SP | Tel.: (11) 3170 1571
Fale com a gente
publicacoes@fecomercio.com.br

IMPRESSÃO

Gráfica Eskenazi

TIRAGEM 10.000 exemplares



REPRESENTA MUITO PARA VOCÊ



C&S | EDIÇÃO 65 – MAR/ABR 2020

8 Entrevista

José Antônio Ziebarth, diretor no Ministério da Economia

14 O que é a LGPD

Conheça a lei que vai mudar tudo sobre dados pessoais

22 Onde o “bicho pega”?

Dicas dos especialistas de Tecnologia da Informação

26 Penalidades

Confira as punições para os infratores

28 Como se faz

Passo a passo para pequenas e médias empresas

30 Impacto geral

Legislação impacta corporações de todos os portes

38 Compliance

A diferença que faz ter um plano de conformidade

44 Artigo

Andrea Willemin

46 Setor privado

FecomercioSP defende atuação em parceria com ANPD

50 Glossário

Entenda as expressões mais usadas

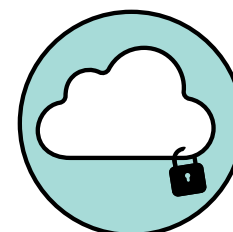


A LGPD TRAZ SEGURANÇA JURÍDICA, NA MEDIDA EM QUE HARMONIZA TODOS OS CONCEITOS ENVOLVIDOS NAS LEIS JÁ EXISTENTES SOBRE PROTEÇÃO DE DADOS.”

RENATO OPICE BLUM,
presidente do Conselho de Comércio Eletrônico da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP)



Assista ao webinar sobre LGPD



SIGILO

REPRESENTATIVIDADE

O Conselho de Comércio Eletrônico da FecomercioSP enviou ao Banco Central (BC) sugestões para a implementação do sistema financeiro aberto, o Open Banking – que modificará a relação entre os clientes e o setor financeiro, uma vez que o correntista será o “dono” de seus dados e decidirá se quer compartilhá-los ou não. Saiba mais sobre as atividades de advocacy da Entidade. Escreva para ri@fecomercio.com.br.

VIDA DIGITAL

BANCO DE BOLSO

“Hoje, nós consumimos produtos e serviços de forma digital. Por que não levar isso para a vida financeira das pessoas?”, reflete a diretora-executiva do banco digital BS2, Juliana Guimarães, em entrevista ao UM BRASIL, uma realização da FecomercioSP. Educação financeira e desburocratização do ambiente de negócios são outros assuntos no bate-papo. Acesse www.umbrasil.com.

GUIA

COMBATE À PIRATARIA

A FecomercioSP, em conjunto com a Secretaria Nacional do Consumidor, o Ministério da Justiça e Segurança Pública e a Subsecretaria de Desenvolvimento de Comércio e Serviços do Ministério da Economia, vem desenvolvendo um guia de boas práticas e orientações para a implementação de medidas de combate à pirataria nas plataformas de comércio online. O guia, que está sob consulta pública, traz normas e termos legais para o desenvolvimento dos marketplaces (plataformas que aglutinam diversas lojas online) que incluem educação digital, tanto para o consumidor quanto para o empresário. **Mais informações em:**





ENTREVISTA • com José Antônio Ziebarth

Aposta na cultura da privacidade

Com a LGPD, que entra em vigor em agosto, e a criação da Autoridade Nacional de Proteção de Dados (ANPD) sobre o tema, haverá maior clareza para o cidadão sobre os usos público e privado de suas informações pessoais e mais segurança jurídica para as empresas

texto BARBARA OLIVEIRA • fotos PAULO NEGREIROS

José Antonio Ziebarth

José Antonio Ziebarth, diretor do Ministério da Economia, fez carreira como professor, advogado e consultor, com experiência no setor privado, na academia e no serviço público federal em América Latina, América do Norte e Ásia-Pacífico. Foi docente da Faculdade de Direito da Universidade de Melbourne, considerada uma das dez melhores do mundo, segundo o ranking internacional Times Higher Education. Realizou análises das melhores práticas internacionais e estudos comparados com mais de 45 países sobre gestão e governança de autoridades de proteção de dados, além de avaliação de impacto regulatório e inteligência artificial. Premiado autor e palestrante em relevantes eventos internacionais. A convite da Comissão Europeia, proferiu palestra na 41ª Conferência Internacional de Proteção de Dados e Privacidade, que reuniu mais de 115 países. Nesta entrevista à **C&S**, Ziebarth fala sobre a importância da LGPD no Brasil e o papel reservado à Autoridade Nacional de Proteção de Dados (ANPD) na aplicação da lei.



Qual é a importância da Lei Geral de Proteção de Dados (LGPD) para o Brasil?

É importante porque disciplina os dados pessoais do cidadão. A lei vai introduzir uma nova cultura e novos procedimentos, além de rever procedimentos existentes – como as empresas e o setor público coletam e tratam os dados. E [servirá] para que o cidadão tenha conhecimento de como suas informações pessoais são utilizadas por empresas e pela administração pública, por exemplo, para a formulação do planejamento de determinada política pública.

Esse tipo de legislação é uma tendência internacional?

Sim, hoje já existem mais de 130 países com legislação de proteção de dados. A lei brasileira foi largamente influenciada pelo regulamento europeu – General Data Protection Regulation (GDPR) –, marco fundamental na legislação de proteção e que inspirou outras iniciativas que vieram depois.

Essa importância se dá, também, na relação mais transparente entre os setores público e privado com o titular?

Exatamente. Essa busca pelo consentimento do titular dos dados é o grande elemento de transparência dessa legislação. Temos trabalhado, neste momento que o Brasil passa por período de renovação e mudanças de políticas econômicas, para unir as

“

A LGPD estabeleceu princípios. Os grandes desafios para saber se ela vai ser pesada (ou não) serão as resoluções que a ANPD vai emitir.

melhores práticas internacionais. O Brasil pode aproveitar esse atraso [na lei] para aprender sobre as práticas internacionais, inclusive com os nossos vizinhos México, Argentina e Uruguai, que já têm experiência nessa área. No Ministério da Economia, fizemos um largo estudo comparado com 45 países, olhando os principais elementos de como a lei foi aplicada e como a Autoridade Nacional de Proteção de Dados (ANPD) é estruturada. É importante que comecemos o ano com a criação do órgão e com a vigência da lei [a partir de agosto], fornecendo ao cidadão maior conhecimento e mais clareza, além de segurança jurídica às empresas

brasileiras. Nossa batalha no Ministério da Economia é para simplificar a legislação, seja para o aplicador da lei, seja para quem está sendo analisado por ela.

O que o senhor destaca como muito positivo na lei? E em quais pontos mais penaliza as empresas?

A LGPD estabeleceu princípios. Os grandes desafios para saber se ela vai ser pesada (ou não) serão as resoluções que a ANPD vai emitir. A lei fala de legítimo interesse e de finalidade pública. Por exemplo, o Ministério da Saúde vai construir um hospital numa região onde é necessário, mas, para isso, precisará pesquisar os prontuários médicos dos pacientes e descobrir a especialidade mais exigida. O gestor público usará esses dados de acordo com os parâmetros estabelecidos pela lei. Baseado nessa finalidade pública, verá quais são esses dados, como são tratados e que tipo de informação é necessária. Isso quem vai definir é a ANPD, por meio de uma resolução específica. Se vai ser ruim ou boa, dependerá da especificação da Autoridade.

Qual a relevância do Conselho Nacional de Proteção de Dados Pessoais?

É um elemento importante definido pela ANPD. Junto com o Conselho Diretor, composto por cinco diretores, fará a execução de políticas públicas. Neste momento de

difusão da cultura de proteção, de criação de um regime jurídico, o conselho vai levar para o cidadão e para o pequeno empresário esse conhecimento. O empresário estará representado no Conselho Nacional: dos 23 assentos, 14 serão da sociedade civil e do setor produtivo para que se manifestem sobre as políticas públicas. O conselho será regulamentado por um decreto federal que detalhará o seu funcionamento.

A lei deve ser rígida na implantação ou permitir um prazo para as empresas se adequarem melhor?

Uma tendência que muitos países seguiram é de, no primeiro estágio da aplicação, a lei ser mais educativa. Olhamos para a experiência internacional e também para o que aconteceu no Brasil quando foram criadas as agências reguladoras. O Conselho Administrativo de Defesa Econômica (Cade), de 1994, começou com muito trabalho de formação e educação. Nos primeiros anos, os empresários recebiam ofício do órgão com uma nota de jornal falando: “Essa empresa ‘X’, noticiada na mídia impressa, pretende realizar uma operação de fusão e aquisição, e, a partir de junho de 1994, essa operação deve ser notificada ao Cade”. Pode ser uma linha a ser adotada pela Autoridade na LGPD. Falo como Ministério da Economia, mas a ANPD terá independências técnica e decisória.

“

Nossa batalha no Ministério da Economia é para simplificar a legislação, seja para o aplicador da lei, seja para quem está sendo analisado por ela.

E qual será o principal papel da Autoridade? Assumirá posicionamento normativo, fiscalizatório ou punitivo?

O Brasil não tem cultura de proteção de dados. O importante é que a nova entidade reguladora esclareça esses rumos. A ANPD terá três grandes esferas de atuação: normativa, educativa e institucional. A normativa virá com a emissão de resoluções e orientações públicas para os setores da economia, porque a lei é transversal, vai afetar todos os segmentos, e o tratamento é diferente em cada setor, pois o financeiro trata de uma forma, e o setor de saúde, de outra. Essa especificidade garante segurança jurídica. A educativa será explicar para o cidadão e empresários quais são as disciplinas que a sua atuação no mercado possibilita; e a terceira atuação é o diálogo institucional, porque um dos desafios será, justamente, como os outros órgãos com competências concorrentes ou similares – Secretaria Nacional do Consumidor (Senacon), Ministério Público Federal, ministérios públicos estaduais –, atuar em conjunto com a ANPD. Deve haver diálogo institucional para que a gente não caia num ambiente de insegurança, onde o empresário acata uma decisão, da Autoridade e, no dia seguinte, a Senacon emite outra decisão e o MPF, outra.

Novo jeito de lidar com informações

A grande maioria das empresas ainda precisa se preparar para a Lei Geral de Proteção de Dados (n.º 13.709/2018), que começa a vigorar em agosto e poderá render multas de até R\$ 50 milhões. Conheça mais sobre a legislação que traz desafios (e oportunidades de melhoria) para as empresas, colocando o Brasil num patamar de proteção de dados compatível com a maior parte dos países da Europa e da América Latina

texto LÚCIA HELENA DE CAMARGO

A LGPD FOI BASEADA NA GENERAL DATA Protection Regulation (GDPR), em vigor na União Europeia. Com o planeta interligado pela internet e a crescente utilização dos dados pessoais como ativos pelas empresas de todo o mundo, os governos viram a necessidade de adotar normas para garantir mais proteção e direitos aos titulares dos dados pessoais. Por isso, no contexto global, a implantação da lei por aqui será importante para os negócios, na medida em que facilita o trânsito de informações entre organismos internacionais, podendo trazer mais investimentos

e facilitando a celebração de acordos internacionais com outros países.

A nova legislação se aplica no território nacional, mas pode alcançar organizações sediadas no exterior que efetuarem qualquer etapa do tratamento de dados de brasileiros em território nacional. Esse é um ponto de atenção também para as empresas de turismo, como agências e companhias aéreas.

Trazemos, agora, algumas das dúvidas mais comuns para os empreendedores começarem a entender como implementar a legislação na sua empresa e manter a conformidade.

VOCÊ PRECISA SABER

PRECISO FAZER ALGO NESSE MOMENTO? OU POSSO DEIXAR PARA DEPOIS?

A LGPD passa a vigorar em agosto de 2020, e o processo de adaptação envolve a implementação de um projeto de governança nas empresas, revisão de processos e procedimentos, implantação de sistemas de segurança da informação, treinamentos e outras medidas. Mas o mais importante é a implementação da cultura de proteção de dados nas empresas e na sociedade. Um projeto completo de implementação da LGPD pode levar meses – ou até anos, dependendo da quantidade de dados tratados. Estima-se que o tempo médio varie de seis meses a um ano. No entanto, após a implementação, é crucial manter o processo de conformidade continuamente. Por isso, as empresas devem começar o quanto antes.

SOU UM PEQUENO COMERCIANTE, COM APENAS UMA LOJA. TAMBÉM PRECISO SEGUIR AS NORMAS?

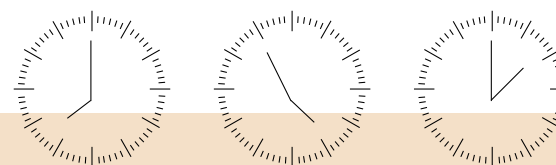
Embora exista previsão legal de que haverá uma regulamentação pela Agência Nacional de Proteção de Dados (ANPD) para interpretação e eventual flexibilização de determinadas regras a pequenas empresas, a instrução neste primeiro momento é que todas devem se adaptar, porque a legislação não distingue as empresas pelo porte, portanto, as normas valem para todas. A Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP)

trabalha ativamente com o Poder Público para obter condições diferenciadas de aplicação das normas para as corporações de pequeno porte.

NA PRÁTICA, COMO VAI FUNCIONAR?

O primeiro passo é fazer um mapeamento na empresa, uma espécie de diagnóstico para identificar toda a forma de coleta de dados e identificar como ela ocorre, se há dados pessoais com terceiros, se existe compartilhamento e transferência de dados, para qual finalidade eles estão sendo utilizados e quem tem acesso a eles. Dado pessoal é todo dado capaz de identificar diretamente uma pessoa ou torná-la, de alguma forma, identificável. Tais como nome completo, CPF, RG, IP (*internet protocol*, na sigla em inglês, ou a “identidade do computador”) em determinados casos, entre outros.

Nem sempre é exigível o consentimento do cliente, porém, em alguns casos é recomendável. Se, por exemplo, um cliente faz uma compra e o lojista deseja capturar certos dados e armazená-los para fins de fidelização, a empresa deve informar de maneira clara e objetiva no ato da



coleta, ou em momento anterior, quais são os dados, qual a finalidade da utilização e como e por quanto tempo serão armazenadas. Se a finalidade de uso dos dados for alterada, é necessário que o titular tenha conhecimento e consinta. Em resumo, não é mais permitida a coleta massiva de dados pessoais, mas somente os dados necessários e justificáveis à finalidade para a qual eles foram coletados. Se não há como justificar o uso dos dados, é necessário descartá-los dos bancos de dados!

ENTÃO, POSSO CONTINUAR COLETANDO OS DADOS DO CONSUMIDOR?

Sim, é possível, desde que a empresa se ajuste às novas normas trazidas pela LGPD. Importante lembrar que não importa a forma – física- ou eletronicamente, em uma ficha preenchida online ou manualmente. O consentimento dos titulares dos dados é recomendado nesses casos, embora nem sempre exigível por lei. Uma forma de fazê-lo é pedir que os clientes leiam os termos e assinem autorizando a utilização dos dados – de forma física ou eletrônica. Um cuidado fundamental a tomar: os termos de uso e as políticas de privacidade devem ser revistas – nada de letras pequenas e textos longos recheados de termos jurídicos. As informações devem ser prestadas de forma clara e objetiva. Transparência é um dos principais princípios trazidos pela LGPD

QUAL O VALOR MÁXIMO DAS MULTAS?

A lei prevê algumas penalidades administrativas pelo descumprimento das normas, tais como advertência, bloqueio ou eliminação dos dados pessoais a que se refere a infração e multa de até 2% do faturamento anual das empresas por infração, podendo chegar a até R\$ 50 milhões, quando se tratar de grandes empresas ou grupos empresariais. Cabe esclarecer, entretanto, que a aplicação das sanções será efetuada após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades de cada caso concreto, observando alguns fatores como a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, a reincidência e o grau do dano.

QUEM VAI FISCALIZAR?

A fiscalização, assim como a regulamentação e a interpretação da lei, será efetivada pela Autoridade Nacional de Proteção de Dados (ANPD), órgão estatal a ser criado pelo governo federal especificamente para essa finalidade. No entanto, outros órgãos, como os órgãos do Procon e o Ministério Público, também poderão, dentro das suas respectivas competências, fiscalizar a aplicação da lei. A assessoria técnica da FecomercioSP entende que a ANPD terá um papel fundamental para



estabelecer o equilíbrio das obrigações impostas pela lei e regulamentar as questões que precisam de especificações técnicas e mais flexibilidade para adaptação ao dia a dia das empresas, especialmente das micros e pequenas. Nesse sentido, a ANPD deve manter um diálogo aberto e permanente com a iniciativa privada na sua atuação, priorizando ações educativas em vez de punitivas.

QUAL O OBJETIVO DESSA LEI?

Um dos principais objetivos da LGPD é a proteção dos direitos fundamentais de liberdade e de privacidade dos cidadãos brasileiros. A autodeterminação informativa é justamente um dos principais princípios que balizam a legislação, colocando o titular dos dados no centro – como protagonista das decisões relacionadas aos seus dados, concedendo-lhe o poder de gerir as suas próprias informações. Em grande escala, a lei também terá a tarefa de trazer à sociedade brasileira a cultura de proteção de dados. Às organizações, cabe um olhar mais delicado para a legislação, entendendo a sua importância. A implementação da LGPD pode ser um grande desafio, que pode ser visto como um investimento pelas empresas, podendo gerar oportunidades de fidelização dos clientes e melhorias da reputação e da imagem das corporações. O uso dos dados dos clientes com transparência e segurança é primordial.

Informar como os dados serão utilizados, para qual finalidade e por quanto tempo serão armazenados é uma das medidas necessárias. A assessoria técnica da FecomercioSP alerta: daqui para a frente, a tendência é que as pessoas busquem se relacionar apenas com corporações nas quais confiem. Portanto, esta é uma grande oportunidade de estabelecer uma relação sólida de confiança com os clientes e fornecedores com quem a empresa se relaciona, assegurando que os dados pessoais serão tratados com ética, segurança e responsabilidade.

O CONSENTIMENTO DO TITULAR DOS DADOS PODE SER REVOGADO?

Sim, a pessoa pode revogar a qualquer momento o consentimento fornecido e também fazer portabilidade dos seus dados, ou seja, transferi-los para outra organização. Mas a boa notícia é que nem sempre será exigido o consentimento para realização do tratamento de dados. As empresas também poderão coletar e utilizar dados pessoais por outras razões, sem necessidade da autorização do titular – como ocorre no caso das empresas com empregados, que são obrigadas por lei a enviar determinadas informações ao INSS e outros órgãos governamentais.



PEQUENAS EMPRESAS, GRANDES DESAFIOS

Pesquisa do site *Reclame Aqui*, feita em 2019, mostra que 41,6% dos dirigentes corporativos do Brasil ainda não sabem o que significa a sigla “LGPD”. Outros 26,4% buscam informações para se adaptar às novidades e 19,9% dizem já ter boas práticas no tratamento de dados da clientela.

Uma sondagem da ICTS Protiviti, consultoria de gestão de riscos e *compliance*, realizada com 104 organizações entre agosto e novembro de 2019, apontou que 58,3% não haviam iniciado as ações necessárias para o cumprimento da nova lei.

O mapeamento de dados pessoais e dados sensíveis é o ponto no qual as participantes declaram ter mais dificuldade. O desafio foi apontado por 71,9%, que afirmam a falta de domínio sobre informações como nome, telefone e endereço residencial dos clientes. Esse mesmo percentual indica não ter um programa de segurança da informação estruturado.

A revelação mais alarmante é que 85% das organizações ainda não capacitaram seus funcionários para lidar com as novas normas. O levantamento mapeou micros e pequenas companhias dos segmentos de tecnologia da informação, serviços profissionais diversos, saúde, educação, agropecuária e construção civil.

LGPD NA PRÁTICA: 7 DICAS DA FECOMERCIO-SP

A assessoria técnica da Entidade detalha os pontos mais relevantes da nova legislação para quem pretende organizar a empresa o mais rápido possível

#1 MÍNIMO NECESSÁRIO

Avalie os dados que a sua empresa realmente precisa utilizar para atingir a finalidade desejada na sua operação. Os que não tiverem uma finalidade justificável devem ser descartados. Só capte e armazene aqueles dados que realmente vai precisar. É uma das formas de mitigar riscos.

#2 CUIDADO REDOBRADO

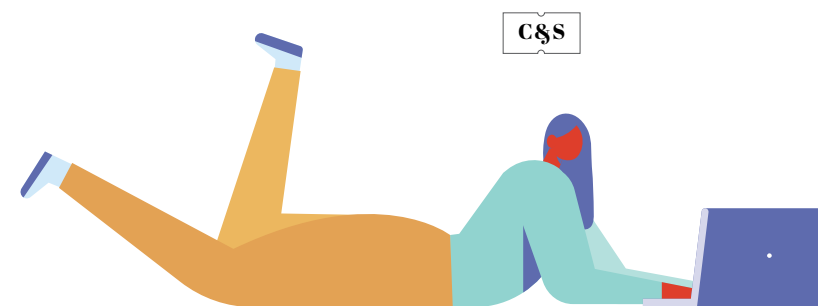
A coleta dos chamados “dados sensíveis” inclui um requisito adicional: o consentimento específico do titular daquelas informações. Dados sensíveis são aqueles relacionados às características da pessoa referentes a saúde, orientação sexual, cor, raça e preferências político-partidárias e ideológicas.

#3 QUEM É RESPONSÁVEL POR MANTER A CONFORMIDADE?

A implementação da LGPD é um projeto de toda a empresa, não apenas de determinadas áreas ou pessoas. É recomendável que seja formada uma equipe multidisciplinar para atuar nesse projeto, formada por uma ou mais pessoas de cada uma das áreas existentes na empresa. O líder desse projeto pode ser o encarregado de proteção de dados, o Data Protection Officer (DPO), função criada pela nova lei que poderá ser exercida por um funcionário contratado ou por empresas terceirizadas e terá a principal função de fiscalizar a aplicação da lei dentro da organização e atuar como ponte entre os titulares de dados, a ANPD e a empresa.

#4 DADOS TRABALHISTAS

O departamento de Recursos Humanos (RH) tem obrigação legal de requisitar dados de funcionários, inclusive os sensíveis (como os de saúde, para planos coletivos) em alguns casos. Nesse caso, não é necessário obter o consentimento do empregado, porque a legislação brasileira exige das empresas determinadas obrigações que só podem ser cumpridas com a coleta e a utilização dos dados pessoais dos empregados. No entanto, a obrigação de transparência para com os funcionários é exigida. A empresa deve implementar uma política interna de proteção de dados para informar aos trabalhadores quais dados são utilizados, por que e como isso ocorre.



#5 COMÉRCIO ELETRÔNICO

Em determinados casos, os dados pessoais serão necessários para a prestação de um serviço ou venda de um produto, como é o caso do e-commerce. Não é possível fazer a entrega de produtos, por exemplo, sem o endereço do cliente e outros dados necessários para emissão da nota fiscal e para o faturamento. Se o dado pessoal é essencial para a execução desse serviço – que o cliente solicitou –, o consentimento não é exigível, desde que exista clareza na prestação das informações pela empresa.

#6 TRANSFORMAÇÕES CULTURAL E ESTRUTURAL

A Entidade lembra que a lei vai gerar um impacto social à medida que as pessoas passem a se importar mais com a utilização dos seus dados, ao se darem conta de que elas podem ter o controle sobre eles, e as empresas também passarão a agir com mais transparência e responsabilidade. A partir de agora, deve-se incorporar a cultura de proteção de dados e as normas da LGPD em qualquer estágio da operação das empresas, desde a concepção de novos produtos e serviços, gerando um padrão de segurança, bem como no relacionamento com clientes, fornecedores, funcionários e parceiros.

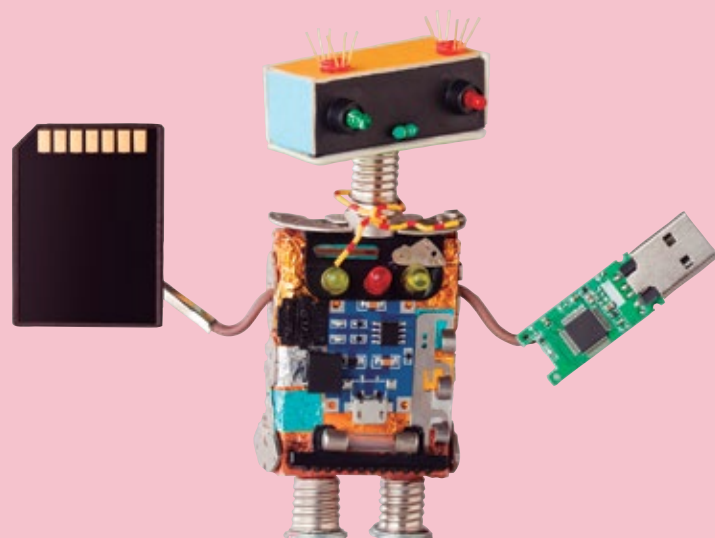
#7 PLANO DE AÇÃO

A assessoria técnica da FecomercioSP recomenda que os empreendedores comecem logo a implementar o plano de adequação, que deve ser implementado por uma equipe formada por funcionários de diversas áreas, envolvendo toda a empresa no processo. É fundamental que se crie a cultura de proteção de dados na organização, mediante treinamentos e ações que privilegiem a transparência e a segurança das informações. É fundamental estabelecer procedimentos operacionais na empresa que possibilitem o exercício dos direitos dos titulares dos dados pessoais – por exemplo, no caso de uma requisição de informações sobre seus dados ou de revogação de consentimento. Além disso, é preciso estabelecer procedimentos também nos casos de crises, por exemplo, um episódio de vazamento de dados. Assim, a empresa deve ter mapeadas quais as medidas técnicas necessárias para conter os prejuízos, além de comunicar imediatamente à ANPD e ao titular dos dados envolvido quando esse fato possa pôr em risco sua segurança ou gerar algum dano à sua imagem. Dependendo da quantidade de dados manipulados pela empresa e a importância desses dados para o negócio, é recomendável recorrer a uma ajuda profissional – como consultorias especializadas na implantação de um processo de conformidade com a LGPD.

Onde o “bicho pega”?

Para quem está na correria do dia a dia dos negócios, as dúvidas sobre a nova legislação se acumulam e envolvem fatores como custos, prazos e sistemas tecnológicos essenciais para encarar o desafio. Acostumados com tais demandas, especialistas dão dicas de como se adaptar

texto **FILIPE LOPES** • ilustração **DANIEL MONTEIRO**



QUANDO ENTRAR EM VIGOR, em agosto de 2020, a Lei Geral de Proteção de Dados (LGPD) vai alterar a rotina das empresas que terão que enquadrar processos, sistemas e soluções às novas obrigações legais. Com a proximidade do início da vigência da lei, as dúvidas se avolumam. Afinal, qual tecnologia deve ser implantada e quais são os custos, os prazos e os impactos técnicos dessa adaptação para a empresa?

No caso da BlueShift Brasil, a saída foi criar um comitê jurídico que aconselha os clientes na escolha de melhores soluções. “Também trouxemos organizações de fora do País para contarem suas experiências, já que estão em conformidade com a GDPR – norma europeia sobre proteção de dados”, afirma o fundador e CEO, Alan Camilo.

Basicamente há dois tipos de soluções tecnológicas para garantir a conformidade: um filtro para proteção dos dados existentes e um software para gestão da privacidade. Ambos são contratados por empresas de TI e podem custar de US\$ 6 mil a US\$ 800 mil anuais, dependendo do volume de dados, que também determina o tempo de migração. Nos grandes varejistas, o processo pode levar até dois anos.

De acordo com o *executive officer* da Privacy Solutions, Laércio Sousa, esse tempo envolve toda a implementação de um programa de governança em privacidade, que é totalmente exclusivo de cada companhia, pois considera o ciclo de vida dos dados pessoais internos e de terceiros. “As organizações B2C [*Business to Consumer* ou *empresa para consumidor*],

“

AS EMPRESAS QUE TRATARAM O CÓDIGO DE DEFESA DO CONSUMIDOR COMO INIMIGO PERDERAM PONTOS COM OS SEUS CLIENTES.

Rony Vainzof

vice-presidente do Conselho de Comércio Eletrônico da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP)

como as grandes varejistas, precisam de um escopo de medidas bastante amplo, o que implica prazo de 12 a 24 meses.”

No caso da pequena e média empresa, Sousa acredita que agosto seja um prazo viável. Dependendo do volume das operações, indica que elas organizem os dados em planilhas, listando os momentos em que essas informações são utilizadas e apontando quais medidas administrativas [escolha das pessoas que as acessam e manuseiam] e de segurança estão em curso para garantir a proteção.

A revisão de processos e o treinamento frequente também são fundamentais, segundo ele, na dinâmica de mudança de cultura para conferir mais transparência às corporações.

MÃO NA MASSA

Entre os segmentos que, desde já, avançam na adaptação à LGPD, as varejistas se destacam, investindo em processos que pretendem conceder mais segurança aos procedimentos de coleta, aceite do cliente e cuidados para proteger esses dados. “Assim como vemos em aplicativos ‘gratuitos’, com os termos de aceite, as empresas terão de formular esses documentos explicando como serão utilizados os dados”, afirma o CEO da startup Refinaria de Dados, Rafael Zenorini. O cliente também pode solicitar a exclusão dos seus dados do seu registro, e a empresa deve atendê-lo prontamente.

“Hoje, todo mundo é dado – e ele vale muito. Se você não paga por um serviço, é porque você é o produto”, destaca Camilo. Para suprir o receio dos consumidores em conceder informações estratégicas, empresários investem em recompensas, como acesso a conteúdos exclusivos.

Para baratear o processo, está se popularizando o conceito da anonimização dos dados. A anonimização é uma técnica aplicada de processamento de dados que impossibilita a identificação das pessoas. Assim, um grande varejista, que conta com vendas físicas e online para todo o Brasil, pode tornar todos os arquivos anônimos e usá-los no conjunto para identificar padrões de consumo por produtos, regiões, gênero, faixa etária, poder

aquisitivo, tempo de permanência na loja ou no site, entre muitos outros. A assessoria técnica da FecomercioSP lembra, no entanto, que essa “solução” é indicada somente em casos específicos. O mais aconselhável seria a implementação de um processo de governança para controle dos dados pessoais.

FORNECIMENTO DOS DADOS

A LGPD prevê como princípio a transparência com os titulares dos dados, ou seja, as organizações devem informar aos seus clientes e fornecedores sobre a forma e a finalidade do tratamento de dados.

Segundo o CEO da BlueShift, Alan Camilo, a dinâmica deve ser parecida com a do *Portal da Transparência*, do governo federal, no qual todo cidadão tem direito a requisitar informações da administração pública e receber os esclarecimentos em prazos determinados.

Alguns empresários trabalham com a hipótese de adiamento da vigência da lei. Mesmo sem descartar essa possibilidade, o vice-presidente do Conselho de Comércio Eletrônico da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP), Rony Vainzof, acredita que as corporações deveriam lidar com a LGPD com base nas lições deixadas pela adoção, em 1991, do Código de Defesa do Consumidor: “Naquela ocasião, as que trataram a legislação como inimiga, perderam pontos com seus clientes, que preferiram companhias éticas e responsáveis. A LGPD atende a uma realidade e deve ser vista como oportunidade para boas práticas de gestão de dados.”

PARA SABER COMO IMPLANTAR AS DIRETRIZES DA LGPD EM SUA EMPRESA, ASSOCIE-SE À FECOMERCIO-SP E TENHA ACESSO AO E-BOOK:



BANCO DE CURRÍCULOS

De acordo com a LGPD, dado pessoal é toda e qualquer informação que possibilite identificar um indivíduo ou que o torne identificável, como nome, RG, CPF, data de nascimento e nacionalidade. As empresas devem ajustar a forma de coleta dos dados na seleção, mantendo somente os dados necessários para os processos de contratação. Para a formação de bancos de currículos, a empresa deve informar sobre a forma de utilização dos dados e pedir o aceite do candidato no ato da coleta das informações. Para o CEO da Refinaria de Dados, Rafael Zenorini: “Isso não deve ser difícil, pois é de interesse do desempregado manter a chance da contratação”.



SANÇÕES ADMINISTRATIVAS NA LGPD

O QUE SERÁ LEVADO EM CONTA

REINCIDÊNCIA

BOA-FÉ

CONDIÇÃO ECONÔMICA

PROPORCIONALIDADE

PRONTA ADOÇÃO DE
MEDIDAS CORRETIVAS

IMPLANTAÇÃO DE PROCEDIMENTOS
INTERNOS DE PROTEÇÃO DE DADOS

POLÍTICA DE BOAS PRÁTICAS
E GOVERNANÇA

COOPERAÇÃO DO INFRATOR

GRAU DO DANO, GRAVIDADE

VANTAGEM OBTIDA OU PRETENDIDA

PENALIDADES PREVISTAS

ADVERTÊNCIA

MULTA DE ATÉ 2% DO FATURAMENTO
DO GRUPO NO BRASIL (TETO DE
R\$ 50 MILHÕES/INFRAÇÃO)

MULTA DIÁRIA COM O TETO MENCIONADO

DIVULGAÇÃO DA INFRAÇÃO

BLOQUEIO DOS DADOS PESSOAIS ENVOLVIDOS

ELIMINAÇÃO DOS DADOS
PESSOAIS ENVOLVIDOS

SUSPENSÃO PARCIAL DO FUNCIONAMENTO
DO BANCO DE DADOS ENVOLVIDO

SUSPENSÃO DO EXERCÍCIO DA
ATIVIDADE DE TRATAMENTO DOS
DADOS PESSOAIS ENVOLVIDOS



AFINAL, VOCÊ ESTÁ PREPARADO PARA A LGPD?
FAÇA O TESTE E CONFIRA A SITUAÇÃO DA SUA
EMPRESA. ACESSE [LAB.FECOMERCIO.COM.BR/LGPD/](https://lab.fecomercio.com.br/lgpd/)
OU USE O CÓDIGO QR

“BEABÁ” PARA PEQUENAS E MÉDIAS

Calma! Começar a adaptação de sua empresa à Lei Geral de Proteção de Dados (LGPD) pode parecer complicado, mas, utilizando o passo a passo a seguir, você vai ver que o processo é viável para todos

texto **FILIFE LOPES**

#1 MAPEAMENTO

A primeira ação a fazer é um levantamento de todos os dados pessoais tratados pela empresa, desde a coleta até o descarte. Avalie como e por que eles são utilizados nas empresas, distinguindo aqueles que são efetivamente importantes para o negócio. Posteriormente, é indicado separá-los de acordo com o tipo de dado (lembrando que a lei exige consentimento específico para os dados pessoais sensíveis). Por fim, a empresa deve ser capaz de identificar quais os tipos de dados coletados e com qual finalidade, quem tem acesso a eles e se existe (ou não) um procedimento de segurança dessas informações. A coleta massiva de dados deve ser substituída pela mínima coleta justificável.

#2 PROGRAMA DE GOVERNANÇA

A lei não define essa etapa como obrigatória, mas é fundamental que a empresa implemente um programa de *compliance* para estabelecer normas e políticas de boas práticas sobre os dados e fazer uma gestão contínua para manter a conformidade com a nova lei.

#3 DEFINA QUEM TRATA OS DADOS

Nomeie os agentes de tratamento: o controlador é a própria empresa responsável pelas decisões sobre o tratamento dos dados; e o operador é aquele que manipula essas informações, seguindo as orientações do controlador. Ambos devem indicar o encarregado pela proteção de dados da empresa, que atua como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

#4 ADAPTAÇÃO DE PROCESSOS E MAIS SEGURANÇA

Estabeleça medidas técnicas e administrativas para garantir a segurança dos dados e evitar acessos não autorizados, perda, destruição ou vazamentos. Para isso, recomenda-se a instalação de softwares e sistemas de segurança. Caso haja dificuldade nesse processo, é indicado procurar uma consultoria especializada, que apontará quais os melhores caminhos a seguir. É imprescindível que os sistemas implementados permitam fácil acesso aos titulares dos dados quando solicitados, além de gestão e registro do tratamento dos dados.



Reestruturação de porte

Dos grandes bancos à farmácia da esquina, todos que capturam dados pessoais sofrerão os impactos da LGPD. A diferença será na gradação dessas consequências, diretamente ligadas aos processos envolvidos e à quantidade de informações armazenadas. No caso de grandes empresas, o planejamento e a execução da conformidade já estão a pleno vapor

texto BARBARA OLIVEIRA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) vai alcançar praticamente todos os setores da economia: dos aplicativos de entrega e de mobilidade, passando pelas empresas de inovação tecnológica e negócios digitais, pelos setores de turismo, comércio (on e offline), financeiro, saúde (farmácias, hospitais e clínicas), educação, logística e serviços públicos. Até uma prosaica portaria de prédio, que pede RG ou CPF do visitante, estará sujeita à nova regulação.

Isso porque quem usa ou armazena alguma informação pessoal de terceiros terá que se adaptar à LGPD, em maior ou menor grau. O tamanho das mudanças vai depender do tipo de coleta, se envolve tratamento automatizado de dados pessoais que afetem os interesses dos usuários, da quantidade coletada, entre outras definições previstas na lei. Empresas que só fazem cadastros de funcionários, por exemplo, terão exposição menor e aquelas que



capturam e tratam informações sensíveis (relacionadas a raça, convicção religiosa, orientação sexual, etc.) terão risco maior e mais etapas a cumprir.

Grandes corporações com estruturas jurídicas e de Tecnologia da Informação (TI), bancos, multinacionais e redes de varejo online não terão muita dificuldade nesse caminho de ajustes, especialmente as que operam com parceiros do exterior. Muitas começaram esse processo ainda em 2018, quando entrou em vigor o marco regulatório europeu, a General Data Protection Regulation (GDPR), que serviu de modelo à LGPD.

PEQUENOS E MÉDIOS

Mas essa preparação pode ser feita sem traumas pelos pequenos e médios empresários, e haverá um prazo para isso, mesmo depois do regulamento aprovado pela Autoridade Nacional de Proteção de Dados (ANPD) – o que deve acontecer nas próximas semanas. “A maioria dos dados tratados (como a captura de informações previstas em contratos) já tem uma base legal, e basta aparar arestas e avaliar se há excessos e justificativas”, tranquiliza o especialista em proteção de dados e vice-presidente do Conselho de Comércio Eletrônico da FecomercioSP, Rony Vainzof.

É o caso, por exemplo, de um e-commerce que precisa de informações pessoais para emissão da nota fiscal, pagamento e envio do produto ao endereço do comprador. Já

uma farmácia que queira cadastrar o consumidor para marketing ou programa de fidelização e concessão de descontos deverá ser mais transparente e revisar esses procedimentos na hora de pedir o consentimento do titular. A partir de agora, deve-se levar em conta o princípio da necessidade com o *data minimization*, ou seja, utilizar a menor quantidade possível de informações para atingir a finalidade do modelo de negócios.

O iFood é uma organização bastante impactada pela LGPD. Com 131,3 mil restaurantes cadastrados no Brasil, o aplicativo atua com entregadores, clientes (restaurantes e lanchonetes), funcionários e parceiros, e todos estão sujeitos ao regulamento, afirma a coordenadora de privacidade para a América Latina, Camila Nagano. “Temos como prioridades a proteção e a privacidade das informações desde a GDPR, que obrigou as empresas a adaptar suas políticas internas e a de parceiros”, conta. “Estamos revisando os contratos já prevendo as cláusulas de proteção, fazendo treinamento dos funcionários e melhorando os controles.”

DESAFIOS JURÍDICO E TECNOLÓGICO

O conceito de *data minimization* no iFood ganhou força diante das exigências de marcos regulatórios e das pressões do mercado internacional para a cibersegurança. Camila detalha que uma das mudanças foi o ras-

tratamento do caminho percorrido pelos dados – devidamente autorizados pelo titular –, desde o cadastro do usuário no aplicativo até os pedidos, que, com o tempo, permitem à empresa compor um perfil baseado em seus hábitos de comportamento. Com isso, “completamos a atividade do tratamento e identificamos se existe o amparo legal para cada uma dessas etapas”. São procedimentos que constarão de relatórios de impacto para mitigação de possíveis riscos.

Segundo a executiva, o iFood exige dos parceiros essa mesma postura, não exatamente no cumprimento da LGPD, porque ainda não está em vigor, mas a de usar somente os dados necessários à finalidade específica e com os mesmos níveis de segurança do aplicativo. E isso fica registrado em contrato.

Outra novidade trazida pela lei é a nomeação de um responsável pela segurança dos dados, o DPO (Data Protection Officer, na sigla em inglês, ou “encarregado de proteção dos dados”). No caso de um hipotético vazamento de dados dos funcionários do iFood, cuja fonte fosse o software de uma empresa parceira de recursos humanos, “esse profissional da terceirizada responderia por isso”, esclarece Camila.

Toda a rede de parcerias precisa entender os direitos do titular. Uma dessas prerrogativas é a de pedir a sua exclusão das plataformas na hora que desejar. O desafio não é só jurídico, mas também tecnológico

Foto: Divulgação



“**CONECTAMOS ATIVIDADES ON E OFFLINE, MAS NÃO COLETAMOS DADOS DIRETAMENTE DE CONSUMIDORES, APENAS INTEGRAMOS OS QUE RECEBEMOS PARA MELHORAR A EXPERIÊNCIA DIGITAL DO USUÁRIO.**”

Mateus Pestana,
CEO da SenseData

A ADAPTAÇÃO PODE SER FEITA SEM TRAUMAS PELOS PEQUENOS E MÉDIOS EMPRESÁRIOS. É IMPORTANTE CONHECER O REGULAMENTO APROVADO PELA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

com processos integrados, tanto para receber o consentimento do titular como para efetivar a exclusão.

MELHORAR A EXPERIÊNCIA

A SenseData é outra companhia que já lida com as novidades. A plataforma de gestão permite aos clientes uma experiência melhor com os consumidores no ambiente digital – por exemplo, em um serviço de *streaming*, no qual é preciso entender as preferências do usuário para personalizar o atendimento. “Conectamos atividades on e offline, mas não coletamos dados diretamente de consumidores, apenas integramos o que recebemos para melhorar a experiência digital do usuário”, informa Mateus Pestana, CEO da SenseData, cuja clientela abrange healthtechs, fintechs, e-commerces, edutechs e startups. Na prática, é o caso de uma operadora de saúde, cujo portal permite que o beneficiário pague boletos ou agen-

de sozinho as consultas ou via call center. “Quando alio tudo isso, tenho um termômetro da experiência do cliente.”

A empresa diz estar alinhada à tendência global de proteção e ter investido, em 2019, 5% de seu faturamento anual (não revelado) em cibersegurança. Mudou processos, contratou profissionais e ajustou contratos e questões jurídicas. O mais relevante para as atividades da SenseData são os arquivos que contêm nome, telefone, e-mail e CEP; e, para isso, já deve haver o consentimento do titular. Segundo Camila, todas as informações coletadas nesse tráfego (de envio e recebimento) entre a plataforma e o cliente são criptografadas para evitar interceptação. A imagem é de uma cadeia de suprimentos na qual dados pessoais e sensíveis terão camadas de segurança em todas as etapas: coleta, transporte e armazenamento (no banco de dados), rastreando quem acessou e quem está operando.

NOVIDADES TRAZEM VANTAGENS COMPETITIVAS

A privacidade e a proteção são princípios que ganham destaque neste mundo conectado no qual os dados são cobiçados como moedas valiosas. Por isso, a LGPD chega em boa hora no Brasil, segundo especialistas. Apesar dos desafios para a conformidade, os profissionais desse mercado apontam que começa a se criar uma nova mentalidade sobre ambos os temas, que enfatiza a importância da transparência e da segurança jurídica. Tornou-se central o questionamento sobre a necessidade e a relevância de tantas informações para o modelo de negócio, quais devem ser protegidas e os controles a serem aplicados nos bancos de dados e na nuvem e quem vai ter acesso. Além disso, como o mercado já vem observando, a remodelagem pode render melhores posições diante da concorrência. Estudo da Cisco, realizado em janeiro deste ano, avaliou as práticas de privacidade de dados em empresas de médio e grande portes espalhadas por 13 países europeus e constatou que, um ano e meio após a entrada em vigor do marco regulatório GDPR, a maioria obteve resultados positivos. Em média, as corporações que investiram na adaptação receberam 2,7 vezes mais sobre esses montantes. E 40% das companhias relataram ter ganhado o dobro dos recursos aplicados melhorando a segurança e reduzindo as violações de dados. Mais de 70% dos profissionais participantes disseram ter obtido resultados comerciais significativos que vão além da conformidade, incluindo mais agilidade, atração de investidores e confiança dos clientes. A conclusão do estudo da Cisco é que aportes em privacidade valem a pena e geram melhor relacionamento entre empresas, consumidores e parceiros e impacto positivo nas receitas.



No caso da Doctoralia Brasil, portal de agendamento de consultas de origem espanhola, a captura de informações é consentida pelos pacientes e profissionais, estes com perfis disponíveis no site, observa o CEO, Cadu Lopes. A Doctoralia segue o conceito da minimização dessa coleta para atender aos princípios da GDPR europeia. Lopes informa que os dados são armazenados em nuvem “somente o tempo necessário para o cumprimento das obrigações contratuais” e com padrões de segurança.

O executivo prevê que até abril estarão concluídas todas as revisões contratuais, políticas internas de segurança e relatórios de impacto à proteção de dados. “Queremos também facilitar a compreensão desses requisitos a todos os usuários da plataforma.” Para cumprir essas etapas, a Doctoralia nomeou um DPO e criou um grupo interdisciplinar para trabalhar em conjunto com advogados especialistas no mapeamento das capturas.

O Mercado Livre, cujos dados de usuários e clientes são ativos essenciais ao modelo de negócios do marketplace, e a Followize, plataforma de gestão de vendas, que atende basicamente a concessionárias de veículos, estão na mesma corrida contra o tempo para o ajuste à legislação até agosto.

Em entrevista por e-mail à **C&S**, a responsável pelo projeto de adaptação e gerente sênior do jurídico do Mercado Livre, Cybelle Fernandes, informa que são realizadas “reuniões periódicas de conscientização dos funcionários e parceiros sobre a impor-

Foto: Divulgação



tância das boas práticas de segurança”. No ano passado, foram contratados mais profissionais das áreas jurídicas e cibersegurança, que, com parceiros externos, formam a equipe multidisciplinar de condução do projeto.

Cybelle destaca a segurança jurídica garantida pela LGPD para a revisão de fluxos internos em relação às diferentes unidades de negócio, e que sempre se preocupou com a proteção dos dados pessoais dos usuários e funcionários nos 18 países de operação. “Essas práticas também ajudam no convencimento de investidores estrangeiros sobre um nível adequado de proteção de dados adotado no Brasil”, afirma a gerente jurídica do Mercado Livre.

“

PREPARAMOS AÇÕES DE CONSCIENTIZAÇÃO COM ESSES PARCEIROS E ESTAMOS AMPLIANDO AS CAMADAS DE PROTEÇÃO E CRIPTOGRAFANDO O QUE CHEGA À PLATAFORMA.”

André Gil,
fundador e diretor de tecnologia
da informação da Followize

CRIPTOGRAFIA E CONSCIENTIZAÇÃO

A maioria dos clientes da plataforma de gestão de vendas da Followize (cerca de 200 concessionárias) ainda tem pouco ou nenhum conhecimento da LGPD, lembra o fundador e diretor de TI, André Gil. “Preparamos ações de conscientização com esses parceiros e, de nossa parte, estamos ampliando as camadas de proteção e criptografando o que chega.”

Trata-se de formulários de interessados na compra de moto ou carro que são enviados pela concessionária à Followize para as ações de venda e marketing. Os dados pertencem ao contratante do serviço (a concessionária) e são armazenados em um data

center com acesso restrito. A criptografia do banco de dados e a contratação de um DPO serão os próximos passos da Followize. Gil deixa claro: “Não detemos nenhum direito sobre essas informações, todas são de propriedade do contratante”.

Cybelle Fernandes, do Mercado Livre, defende que todas as empresas tenham um período de adaptação em relação à aplicação e à fiscalização, ainda a serem regulamentadas. “Esperamos que, inicialmente, a atuação da ANPD seja mais consultiva e colaborativa para que todos possam se ajustar à sua postura, e as penalidades sejam justificáveis só nos casos evidentes de não adequação à LGPD.”

Foco na transparência

Estar ciente de que a LGPD vale para todos que coletam e armazenam dados pessoais é o primeiro passo para mudança e adaptação dentro das empresas

texto BARBARA OLIVEIRA

ATÉ AGOSTO, TODAS AS EMPRESAS DO PAÍS – pequenas, grandes, online, públicas e privadas – estão diante de um grande desafio: terem um bom plano de adaptação a regras e princípios da Lei n.º 13.709/18, de Proteção de Dados Pessoais. Mesmo que a Câmara Federal vote na proposta, em tramitação na Casa, para adiamento do marco regulatório em mais dois anos, não é possível ignorar o fato de que o caminho da proteção e privacidade é um caminho sem volta.

Por isso, iniciar um plano de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) – seus princípios, padrões éticos

e regulamentos (*compliance*) –, é essencial neste momento, principalmente para que, mais tarde, surpresas com possíveis punições de parte da Autoridade Nacional de Proteção de Dados (ANPD) sejam evitadas. Essa será a instância responsável por fiscalizar e regular a lei, mas, antes de punir, ela vai orientar preventivamente, advertir e esclarecer dúvidas. Só depois dessa etapa que virá a penalização. “Defendemos que a ANPD tenha uma construção colaborativa, avalie e escute muito bem a iniciativa privada antes de sair sancionando”, observa o coordenador do curso de Proteção de



“

O PENSAMENTO NÃO DEVERIA SER EM QUANTO E QUANDO VOU SER PUNIDO, MAS QUAL VANTAGEM COMPETITIVA EU POSSO TIRAR DISSO.

Jefferson Kiyohara,
diretor de *compliance* da
consultoria ICTS Protiviti

Dados da Fundação Instituto de Administração (FIA) e vice-presidente do Conselho de Comércio Eletrônico da FecomercioSP, o advogado Rony Vainzof.

A LGPD é válida para todos que colhem, compartilham e armazenam as informações pessoais de clientes, fornecedores ou parceiros, desde nome, endereço, CPF e RG, dados profissionais (local de trabalho e salário) e hábitos de compra até as mais sensíveis (etnia, convicção religiosa, doenças, orientação sexual). “Há uma categorização

para dados sensíveis a fim de evitar algum tipo de discriminação. O importante é que, além de responsabilização, transparência e prestação de contas, as empresas tenham uma base legal para todas as atividades relacionadas ao tratamento da informação do titular, lembra Vainzof.

MAPEAMENTO E RELATÓRIOS

Antes de começar o caminho da conformidade, é importante a conscientização de CEO, diretor, sócio ou dono da empresa sobre a importância da lei e do seu impacto no negócio. O mesmo aconteceu com outros marcos regulatórios no Brasil (defesas do consumidor e econômica, Marco Civil da Internet), e a adaptação veio – mesmo sob protestos iniciais.

“O pensamento não deveria ser em quanto e quando vou ser punido, mas qual vantagem competitiva posso tirar disso”, destaca o diretor de *compliance* da empresa de consultoria e auditoria ICTS Protiviti, Jefferson Kiyohara. Segundo ele, quem enxergar longe e tornar o seu perfil adequado a prestar o serviço ou vender o produto terá vantagens diante dos concorrentes. “É uma mudança cultural, o próprio mercado vai regular e exigir essa adaptação”, avalia a especialista em privacidade de dados e sócia da Demarest Advogados, Tatiana Campello.

No rol de decisões internas para cumprir o *compliance*, a primeira providência é saber onde estão e quais os dados pessoais colhidos e armazenados pela empresa. “Esse mapeamento é crucial para se entender a natureza das informações, quais envia e quais recebe de terceiros, e, a partir daí, teremos



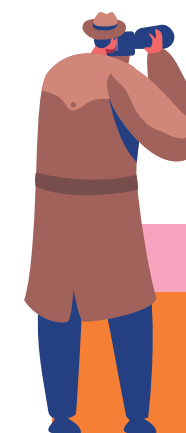
uma análise de onde estão as lacunas, se existe controle de acesso e se estamos obtendo esses dados de terceiros sem necessidade”, diz Campello. Assim, a empresa controladora terá como ajustar essas condutas e eliminar as fragilidades.

Para cada tipo de atividade de tratamento, é preciso uma base legal. As empresas avaliam o nível crítico das informações e sua quantidade, se existem justificativas para serem guardadas e qual o nível de segurança. Um pequeno e-commerce que precisa desses dados pessoais para executar um contrato está amparado pela lei. Também possui base legal uma empresa que faz essa coleta para cumprir legislação trabalhista e pagar o INSS. “Nesses casos, é só questão de aparar arestas e avaliar se não há quantidade excessiva de dados e se justificam”, explica Vainzof.

Mesmo assim, esse mapeamento é obrigatório, seguido da implementação e de suas complexidades. Por isso, é fundamental o treinamento interno de funcionários ou agentes de tratamento com base na nova legislação, tanto para o inventário como para o cumprimento do plano de governança –

mesmo que essas pessoas sejam recrutadas das áreas de TI, segurança ou jurídica. As empresas menores, cuja coleta de terceiros não é massiva nem muito crítica, podem recorrer a especialistas terceirizados de tecnologia e de cibersegurança para ajustar seus sistemas já existentes ou agregar ferramentas ao software, orienta Tatiana.

Treinamentos, relatório de impacto, revisão de políticas, reavaliação das informações colhidas e tratadas, transparência nos contratos, entre outras atribuições, integram as boas práticas e a governança da empresa. Está prevista, ainda, a existência de um profissional encarregado de proteção de dados, o Data Protection Officer (DPO), para atuar como elo de comunicação entre a empresa, o titular e a autoridade. Entre as exceções esperadas para serem definidas pela ANPD em normas complementares, é possível que esse cargo não seja necessário em alguns segmentos, ressaltam os especialistas. —



O OLHAR DO MERCADO



“

Um conselho que eu daria às empresas menores é que tentem engajar todos os dirigentes na aprovação do projeto de adaptação à lei, para entenderem que o investimento é necessário e vale a pena.

Camila Nagano,
coordenadora de privacidade da iFood para América Latina



“

ASSIM COMO VEMOS EM APLICATIVOS ‘GRATUITOS’, COM OS TERMOS DE ACEITE, AS EMPRESAS TERÃO DE FORMULAR ESSES DOCUMENTOS EXPLICANDO COMO SERÃO UTILIZADOS OS DADOS.

Rafael Zenorini,
CEO da startup Refinaria de Dados

“

Uma empresa só vai contratar outra se esta adotar práticas de compliance, o próprio mercado vai exigir que elas tomem essa atitude.



Tatiana Campello,
especialista em Data Protection e Privacidade, da Demarest Advogados



“

HOJE, TODO MUNDO É DADO, E ESTE DADO VALE MUITO. COSTUMO DIZER QUE SE VOCÊ NÃO PAGA POR UM SERVIÇO, É PORQUE VOCÊ É O PRODUTO.

Alan Camilo,
fundador e CEO da BlueShift

Responsabilidade com dados pessoais

ANDREA WILLEMEN,

Data Protection Officer (DPO), advogada com mais de 20 anos de experiência em proteção de dados no Brasil e Europa. Mestre em Direito da Sociedade de Informação pela UFSC (Santa Catarina); pós-graduada em Proteção de Dados e Segurança da Informação pela Universidade de Maastricht (Holanda).

A ERA DA SOCIEDADE DA INFORMAÇÃO e o desenvolvimento de novas tecnologias permitiram o avanço de um mercado baseado em dados dos quais se extraem valiosas informações. Quem detém a informação, detém o poder. Afinal, o dado é o novo petróleo. Com ele, são feitas análises e se extraem perfis, estatísticas e um mundo numérico que permite cruzamentos e identificação de tendências e comportamentos.

A análise de dados criou um fenômeno mundial de controle e vigilância explorado pelo mercado econômico e pelos governos. No entanto, a invisibilidade da tecnologia dificulta que o indivíduo se proteja de forma eficaz.

O tratamento de dados criou, desde a década de 1970, na Europa, a necessidade de regulamentação da privacidade de forma

a delimitar os direitos e regular a utilização das informações a fim de resguardar os indivíduos de manipulações indevidas. Hoje, na maioria dos países europeus, a proteção de dados pessoais é garantida constitucionalmente como direito fundamental. Em maio de 2018, a General Data Protection Regulation (GDPR), lei da União Europeia sobre a proteção de dados pessoais, passou a vigorar com aplicabilidade extraterritorial.

Com o escândalo de vazamento de informações de milhares de usuários da maior rede social do mundo no incidente da Cambridge Analytica, a discussão sobre proteção de dados gerou pressão internacional para que o Brasil também uniformizasse a questão, além de ser um dos requisitos para a vaga na Organização de Cooperação e Desenvolvimento Econômico (OCDE). Dessa forma, foi aprovada a Lei Geral de Proteção de Dados (LGPD). Em razão dessa lei, operadores e desenvolvedores de aplicações tecnológicas serão atores nessa nova economia e precisam dominar conceitos jurídicos que englobam direitos internacionais público e privado. O tempo é curto, e o engajamento, principalmente da direção, é crucial para essa reestruturação à qual o Brasil está sendo chamado a participar.

Multas altíssimas, suspensão da atividade comercial, apreensão do banco de dados e processos judiciais são algumas das consequências do desrespeito à LGPD. Na era da sociedade da informação, muito além de valores pecuniários, o maior dano será a quebra de reputação por violação dos direitos fundamentais da proteção de dados. Ao trabalho!

SAVE THE DATE

Congresso de Direito Digital, Tecnologia e Proteção de Dados

dias 21 e 22 de setembro de 2020

local: FecomercioSP

Visite
<https://opiceblumacademy.com.br/cddtgd/>
e registre-se para receber
mais informações por e-mail



promovido por



apoio





Pela participação do setor privado

A FecomercioSP defende que as empresas façam parte da regulamentação da LGPD, atuando em parceria com a ANPD a fim de evitar que as penalidades comprometam o ambiente favorável aos negócios na economia digital

texto BARBARA OLIVEIRA

EM NOVEMBRO DE 2019, a FecomercioSP comunicou ao governo federal a importância do marco jurídico da Lei n.º 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que entra em vigor em agosto, para atualizar conceitos e buscar o “equilíbrio para o uso ético, seguro e consciente de dados por entidades públicas e privadas”.

Nesse texto, a Entidade – que representa mais de 130 sindicatos patronais paulistas e mais de 80% do faturamento do varejo online brasileiro – sugere que a regulamentação da LGPD pela Autoridade Nacional de Proteção de Dados (ANPD) tenha a participação do setor privado visando à melhoria do ambiente de negócios. Conheça as principais recomendações nesta matéria.



MODELO TÉCNICO

Para evitar arbitrariedades em eventuais fiscalizações, a FecomercioSP e seu Conselho de Comércio Eletrônico entendem que o modelo ideal para a composição da ANPD é o técnico, pautado em conhecimentos tecnológicos, jurídicos, econômicos e de negócios.

AGENDA TRANSPARENTE

Quanto às funções da ANPD, é imprescindível que promova ações educativas referentes aos dados, incluindo a indicação das melhores práticas empresariais e a elaboração de uma agenda nacional com detalhamento transparente dos resultados esperados e das abordagens que serão realizadas.

HARMONIA ENTRE NAÇÕES

É necessário que a ANPD contribua para a conscientização e a aplicação dos termos da lei e que sua atuação leve em conta as especificidades de cada setor e relações entre segmentos. Ela deve ser o ponto único de contato entre organizações regionais e estrangeiras e autoridades internacionais, atuando para harmonizar o tema nas diversas nações.

CONFIANÇA DO MERCADO

Em um país no qual se intensifica a cultura da proteção de dados, são prioritárias as participações do setor privado e da administração pública, sob pena da ausência de confiança do mercado na referida ANPD.

PARTICIPAÇÃO DAS EMPRESAS

É importante que as empresas também possam participar do processo de regulamentação da lei, contribuindo para a elaboração de seus termos e evitando que a aplicação das penalidades comprometa a continuidade dos seus negócios.

ORIENTAÇÃO ANTES DA AUTUAÇÃO

Prioridade para o critério da dupla visita na fiscalização. Ou seja, a fiscalização orientadora deve preceder a autuação, que só deve ser efetivada caso a empresa não cumpra a adaptação solicitada pela ANPD.

PRESUNÇÃO DE BOA-FÉ

O Estado deve privilegiar o diálogo, a mútua cooperação, a orientação, a conscientização e a informação; além de estimular as relações abertas e construtivas com negócios que lidem com dados pessoais, primando pela presunção da boa-fé das empresas.

INOVAÇÃO NOS NEGÓCIOS

É primordial a criação de ambientes de experimentação, como os *regulatory sandboxes*, espaços nos quais novos projetos e modelos de negócios inovadores podem ser testados, sob a supervisão do regulador, sem que haja inicialmente qualquer punição legal.

RESPONSABILIDADE CERTIFICADA

Estímulo à responsabilidade e *accountability* (prestação de contas), demonstradas pelas corporações em programas de privacidade e segurança da informação e códigos de conduta e no gerenciamento de risco. A FecomercioSP defende essas boas práticas sejam reconhecidas com certificações.

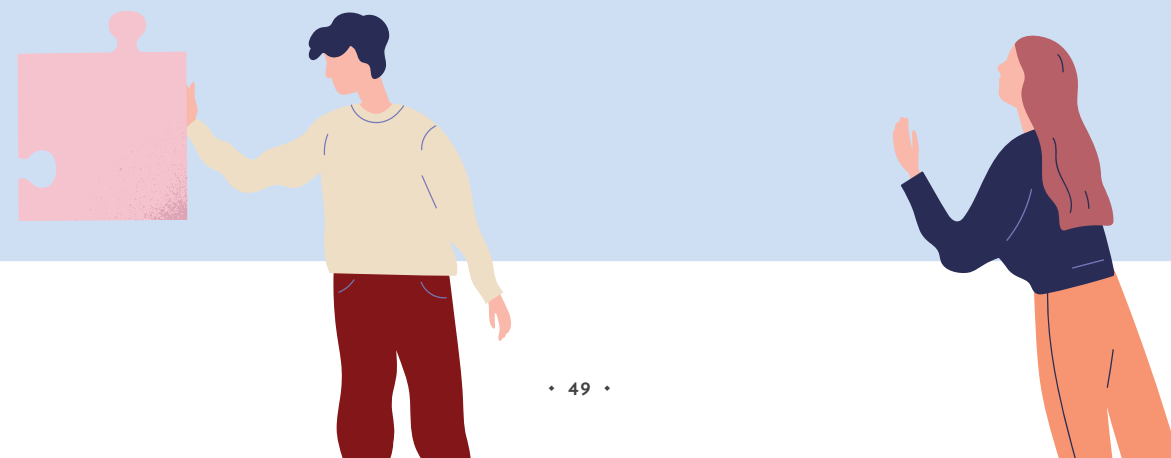
PUNIÇÕES JUSTAS

Sanções devem ser empregadas somente quando ocorrer violação dolosa, prática negligente, conduta reiterada ou extremamente grave. É importante frisar que tais punições não devem servir como principal fonte de recursos da ANPD, sob pena de legitimar contestações éticas, políticas e legais.

ENTIDADE DEMANDA QUE AS EMPRESAS PARTICIPEM DO PROCESSO DE REGULAMENTAÇÃO DA LEI, CONTRIBUINDO PARA A ELABORAÇÃO DE SEUS TERMOS

COOPERAÇÃO COM A ANPD

Por último, é fundamental a finalização do processo legislativo da LGPD para as empresas em geral, com foco no equilíbrio entre os interesses sociais e os econômicos, os setores público e privado e a liberdade, a proteção e a segurança. A FecomercioSP ressalta que as empresas terão papel relevante de cooperação com a ANPD para a efetiva manutenção da competitividade na economia digital.





GLOSSÁRIO

DADO PESSOAL – É toda e qualquer informação relativa a uma pessoa natural (física) que sirva para identificar ou tornar um indivíduo identificável, como nome, RG, CPF, data de nascimento, nacionalidade, entre outros.

TITULAR DOS DADOS – É a pessoa física detentora dos dados pessoais a quem se referem os dados tratados.

TRATAMENTO DE DADOS – Toda operação relacionada a 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.

AUTODETERMINAÇÃO INFORMATIVA –

Princípio que concede ao titular dos dados (pessoa física) o poder de controlar a utilização deles, nos termos da lei. Possibilita, por exemplo, questionar e solicitar informações sobre a existência e a forma de tratamento dos seus dados pelas empresas.

COMPLIANCE – Adotar as práticas de *compliance* significa manter políticas e diretrizes do negócio em conformidade com leis, regulamentos e normas internas e externas que regem a atividade. Esse conjunto de disciplinas no âmbito da LGPD significa implementar um programa de governança na empresa a fim de manter a conformidade contínua com a legislação em relação à privacidade e à segurança de dados.

CONTROLADOR – É a denominação utilizada pela lei para designar a pessoa (física ou jurídica) que detém o controle e o poder de decisão sobre os dados dos titulares.

Exemplificando, é a empresa que faz tratamento de dados dos seus clientes, empregados ou fornecedores.

OPERADOR – Empregado ou empresa especializada indicada pelo controlador para realizar o tratamento de dados em nome dele e seguindo as suas orientações. Pode responder em conjunto com o controlador em casos de descumprimento da legislação.

DADOS SENSÍVEIS – Toda informação que possa ser utilizada para identificar uma pessoa física de forma discriminatória, como dados sobre raça e etnia; orientação sexual; convicções religiosas, filosóficas ou políticas; saúde e dado genético ou biométrico.

DPO/ENCARREGADO – O encarregado – também conhecido em outros países como Data Protection Officer (DPO), – é a pessoa responsável pela proteção dos dados do titular na organização, servindo de elo na comunicação entre a empresa, os titulares e a Agência Nacional de Proteção de Dados (ANPD). Ele vai auxiliar ainda na adaptação, na estruturação e no monitoramento do programa de *compliance* com foco na proteção de dados.

DIVULGAÇÃO DA INFRAÇÃO – É uma das penalidades a serem aplicadas depois de apurada e confirmada a infração cometida pela empresa. É um tipo de propaganda negativa porque evidencia para o mercado e para as autoridades que existiu alguma infração à lei cometida pela empresa, como vazamento de dados ou desvio de finalidade no tratamento, por exemplo. A regulamentação pela ANPD ainda vai definir os detalhes da publicização e como será feita.

publicis

Delícias de Chocolate

Pitadas da Rita

for ever

Projeto Espaço

RAIZA COSTA

Imperador

MIRIAM GURGEL

A MISSÃO DO MESTRE-CERVEJEIRO

O que tem na geladeira?

Senac

Senac Panelinha

Senac Panelinha

MAIS DE 1.000 TÍTULOS PARA TODAS AS ÁREAS DE CONHECIMENTO.

Senac

LIVRARIA SENAC.COM.BR

COMPRA VIRTUAL, CONHECIMENTO REAL.

50% DE DESCONTO PARA ALUNO SENAC

É POSSÍVEL

ter um plano de saúde
que cabe no seu bolso.

Só com a Qualicorp e com a **FECOMERCIO-SP**
você, **Empregador do Comércio**, tem
condições especiais na adesão de um dos
melhores planos de saúde do Brasil.

A partir de:

R\$ 291¹



Ligue: 0800 799 3003

Se preferir, simule seu plano em qualicorp.com.br/anuncio

SulAmérica:

ANS nº 006246

Bradesco Saúde:

ANS nº 005711

Central

Nacional Unimed:

ANS nº 339679

Amil:

ANS nº 326305

Qualicorp

Adm. de Benefícios:

ANS nº 417173