VMCA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

PERGUNTAS E RESPOSTAS SOBRE OS IMPACTOS DA NOVA REGULAMENTAÇÃO **NO SETOR DE PUBLICIDADE**

Todas as empresas que atuam com publicidade, de todos os portes e operando *online* ou *offline*, serão afetadas pela LGPD.

COLABORAÇÃO TÉCNICA

CENP
Conselho Executivo das Normas-Padrão

AGOSTO DE 2019

As transformações digitais das últimas duas décadas mudaram profundamente a forma como empresas, consumidores e usuários se relacionam. *Smartphones*, aplicativos, *e-commerces* e mídias sociais tornaram as relações mais próximas e permitiram a empresas de todos os segmentos a coleta, a análise e o uso de dados dos consumidores (do nome ao endereço, da localização ao horário em que preferem comprar pela Internet) de maneira nunca imaginada.

Esse novo patamar de coleta e uso de dados pessoais — considerados o "novo ouro" da era digital — barateou campanhas e facilitou a tomada de decisões das empresas, permitindo ações de *marketing* mais assertivas. Também gerou benefícios aos consumidores, que passaram a contar com campanhas, promoções e ações customizadas.

No entanto, a enorme quantidade de dados que passou a ser coletada em anos recentes trouxe desafios sem precedentes quando o tema é a proteção da privacidade. Um exemplo corriqueiro é o uso dos dados pessoais por terceiros sem a ciência ou consentimento de seus titulares.

Um caso que ilustra os malefícios que o uso indiscriminado de dados pessoais pode gerar é o que envolveu a empresa britânica de análise de dados Cambridge Analytica. Em 2014, a empresa coletou dados de usuários do Facebook por meio de testes lúdicos de personalidade aplicados em um app nessa rede social. Estima-se que as informações foram usadas para traçar o perfil psicológico de 87 milhões de pessoas.

Em uma primeira análise, nada ilegal foi praticado. Afinal, a política de privacidade do Facebook permite a coleta de dados pelas empresas parceiras à medida que os usuários permitam tal acesso. Ainda que posteriormente os dados tenham sido utilizados pela consultoria para traçar o perfil psicológico dos usuários com o intuito de fazer marketing político, novamente não havia problema aparente: marketing político não é ilegal.

O que causou escândalo foi que em nenhum momento a empresa informou que os dados estavam sendo coletados para essa finalidade. Tampouco foi informado que a coleta incluía os dados não apenas das pessoas que fizeram os testes, como os de suas redes de contato na rede social (os "amigos" dos usuários).

Os usuários do app desconheciam que informações pessoais foram utilizadas para a produção de propaganda eleitoral altamente personalizada, que, especula-se, influenciou nos resultados da campanha presidencial dos Estados Unidos em 2016 e no plebiscito que marcou a saída do Reino Unido da União Europeia (o Brexit), no mesmo ano.

O exemplo deixa claro que existe uma zona cinzenta que separa a coleta e o uso legal de dados da invasão da privacidade. Que dados posso coletar, tratar e utilizar? Há regras para isso? O cenário exigiu respostas e obrigou governos mundo afora a regulamentar a matéria.

A Câmara dos Comuns inglesa, por exemplo, desenvolveu o relatório "Desinformação e fake news", complementado por um Comitê Internacional com participação de nove países — Brasil, França e Canadá entre eles — para apurar consequências prejudiciais à democracia decorrentes da realização de

campanhas políticas por meios digitais. O relatório aborda diversas questões nessa zona cinzenta, como o papel e a responsabilidade das redes sociais, o direcionamento de anúncios com teor político e a influência em campanhas eleitorais. No entanto, mesmo tendo avançado muito ao trazer a visão de múltiplos interessados sobre o tema, ainda se espera movimentação do governo inglês para que as recomendações adquiram caráter mais concreto.

Grande referência sobre o tema, o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation – GDPR*), da União Europeia, em vigor desde maio de 2018, estabeleceu novas regras de proteção a dados pessoais aplicáveis às empresas do mundo todo operando no ambiente europeu. Fruto de longo esforço de reflexão sobre o tema da proteção de dados, cuja elaboração contou com a participação de especialistas do mundo todo, considera-se o GDPR uma legislação protetiva e um grande avanço na regulamentação do tema. Vale lembrar que no segundo semestre de 2018, o estado da Califórnia aprovou a Lei de Privacidade dos Consumidores da Califórnia (C*alifornia Consumer Privacy Act – CCPA*), inspirada pelo GDPR. Trata-se da primeira legislação compreensiva de dados pessoais nos Estados Unidos.

Mesmo com o curto período em vigência, já foram identificados na Europa diversos casos de imposição de multas por descumprimento do GDPR[1]. Em julho de 2018, por exemplo, após notificação da Ordem dos Médicos de Portugal, a autoridade de proteção de dados portuguesa aplicou multa de € 400 mil a um hospital por não ter implantado medidas técnicas e organizacionais adequadas para a proteção de dados pessoais dos pacientes e a garantia de segurança e integridade do seu sistema interno. Em novembro, a autoridade do estado de Baden-Württemberg, na Alemanha, multou em € 20 mil uma plataforma de chats que não cumpriu o dever de desenvolver medidas de segurança suficientes para a proteção de senha dos usuários depois de sofrer um ataque de hackers dois meses antes, que resultou no vazamento de endereços de e-mail e senhas de cerca de 300 mil usuários. O valor da punição foi reduzido em razão da postura cooperativa da empresa nas investigações, notificando a autoridade de proteção de dados e informando os usuários sobre a falha no sistema.

No Brasil, o Congresso Nacional aprovou em agosto de 2018 a Lei Geral de Proteção de Dados (Lei nº 13.709/18, também conhecida como LGPD), que disciplina o tema "proteção de dados pessoais" nacionalmente.

A lei surge em um momento em que o setor de publicidade vive uma profunda transformação por conta das novas tecnologias. A crescente conectividade do brasileiro culminou em forte crescimento do comércio eletrônico e, consequentemente, das ações de *marketing* digital. Como no caso europeu, a lei brasileira foi desenhada para ser abrangente, portanto, é preciso estar atento: **todas as empresas que atuam com publicidade, de todos os portes e operando *online* ou *offline*, serão afetadas pela LGPD.**

---

1. O número indicado pela *International Association of Privacy Professionals* (IAPP) do total das multas aplicadas em decorrência do GDPR desde sua entrada em vigor é de 56 milhões de euros.

Assim, é fundamental entender os impactos da LGPD sobre o setor. Trazemos nesta *newsletter* perguntas e respostas relevantes sobre o tema. A ideia é abordar algumas das consequências da regulação para empresas e profissionais que atuam no ramo.

A LGPD entra em vigor em agosto de 2020. Até lá, muitas questões permanecem em aberto e exigem dos agentes do setor um acompanhamento contínuo para além dos apontamentos preliminares aqui trazidos.

1 Quais atores do setor de publicidade devem se preocupar com a LGPD?

Todas as empresas que atuam com publicidade, de todos os portes e que operam tanto *online* quanto *offline* serão afetadas pela LGPD. Isso porque a lei se aplica aos setores público e privado (incluindo o terceiro setor), abrangendo todas as organizações, independentemente de sua forma de constituição ou natureza jurídica, que realizem tratamento de "dados pessoais", definidos pela LGPD como qualquer "informação relacionada à pessoa natural identificada ou identificável".

> O que define se a lei é aplicável ou não é a existência de tratamento de dados pessoais pela entidade. Portanto, **com raríssimas exceções, todas as empresas que atuam com publicidade e marketing, de todos os portes, estão sujeitas à LGPD.**

Como a definição é baseada na forma de uso de dados, e não no elo da cadeia produtiva em que a empresa se encontra, há diversos impactos possíveis, diretos ou indiretos, sobre praticamente todas as empresas que atuam com publicidade e *marketing*, incluindo:

i. empresas de comércio eletrônico, principalmente das modalidades B2B (negócio-a-negócio) e B2C (negócio-a-consumidor), mas também *e-commerce* realizado em ambiente interno de organizações e aquele cujo foco são vendas entre pessoas físicas por meio de plataformas de vendas;
ii. agências de comunicação (clipping, assessoria de imprensa, criação de conteúdo etc.);
iii. agências de publicidade;
iv. agências de *marketing* digital;
v. agências de vendas;
vi. agências de SEO (*search engine optimization*);
vii. agências de branding e design;
viii. consultorias que atuem na área;
ix. agências de CRM ou DBM (*Customer Relationship Management, Database Marketing);*
x. empresas intermediárias, que colhem e vendem a terceiros informações de consumidores na internet (*data brokers*); e
xi. outras empresas que tratem dados para fins publicitários (*online* ou *offline*).

2 Como definir o que é o "tratamento de dados pessoais" para saber se minha empresa deve se preocupar com o tema?

A LGPD tem uma definição extremamente ampla do que considera "tratamento de dados pessoais". Diz expressamente que "coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" são todas modalidades de tratamento.

Na prática, isso quer dizer que **mesmo que a empresa não use os dados, se ela simplesmente os coletar de clientes e/ou tiver contato com essas informações por meio de algum um terceiro, deverá se adequar à lei.** Mais: até a eliminação de dados é considerada uma forma de tratamento.

Na área de publicidade, tratamentos de dados podem ocorrer especialmente em casos de:

i. coleta de dados de consumidores, seja para cadastro em banco de dados, seja para posterior contato via e-mail, telefone ou correio;
ii. práticas de individualização e direcionamento de anúncios baseados em informações de consumidores;
iii. compartilhamento e comercialização de dados pessoais de terceiros (como mailing lists);
iv. análises de dados pessoais feitas tanto com base em algoritmos como por pessoas físicas para segmentação de público-alvo e classificação de consumidores a partir de seus perfis de consumo e elaboração de *rankings* de clientes, entre outros.

3 O que é consentimento para tratamento de dados? O que é uma "base legal" de tratamento? Quais as implicações da exigência de consentimento pelo titular dos dados?

É importante ressaltar que o consentimento é a mais famosa, mas não a única, base legal para o tratamento de dados pessoais. As bases legais são aquelas justificativas que a legislação apresenta para que o tratamento possa ser realizado, e estão no artigo 7º da LGPD. São dez as bases existentes:

a. o consentimento
b. o cumprimento de obrigação legal (ou regulatória)
c. a execução de contrato ou de procedimentos preliminares a um contrato (desde que solicitado pelo titular)
d. a proteção da vida ou da incolumidade física do titular (ou de terceiro)
e. a tutela da saúde
f. o legítimo interesse
g. a proteção do crédito
h. o exercício regular de direitos
i. a realização de estudos e pesquisas
j. e, no caso do poder público, a execução de políticas públicas.

Se nenhuma das outras hipóteses de tratamento estiver presente — por exemplo, a retenção de dados para cumprimento de obrigações regulatórias ou para a execução de um contrato — a lei exige que o titular dos dados (o consumidor ou usuário, por exemplo) dê o seu aval, por escrito ou "por qualquer outro meio que demonstre a manifestação da vontade do titular", para que a coleta e o tratamento dos dados possa acontecer. **Ou seja, a regra é que o tratamento só é permitido depois do consentimento, a menos que outra base legal justifique o tratamento.**

Em situação ilustrativa dos efeitos da exigência de consentimento no dia-a-dia, executivos da empresa de transporte privado urbano norte-americana Uber revelaram, em 2014, a existência de uma ferramenta chamada "God View" ("Visão de Deus", em tradução livre). A ferramenta, de uso interno da empresa, mostraria a localização dos veículos dos motoristas vinculados à empresa e dos clientes que requisitaram um carro. Possibilitaria, assim, que a Uber rastreasse a viagem de seus clientes e que utilizasse tais informações privadas em benefício próprio e para qualquer outro fim, como a venda da informação a terceiros para fins de publicidade, sem prévio consentimento. Reter os dados da viagem para garantir que o passageiro seja de fato levado até seu destino é justificável do ponto de vista da legislação, já que poderia ser enquadrado como a execução de um contrato entre o aplicativo e o usuário, mas qualquer outro uso dos dados não se beneficia da mesma justificativa. É por isso que a obrigação geral de consentimento da LGPD, caso se aplicasse a este caso, poderia ter sido violada pela Uber.

Consumidores em potencial ou outros titulares de dados pessoais devem, expressamente, autorizar que seus dados sejam colhidos para cadastro e posterior utilização. Isto é, os consumidores devem ter ciência da finalidade da utilização de seu dado pessoal ao "consentir" com determinada prática. É importante também que as empresas sempre solicitem de seus clientes apenas as informações que sejam relevantes para o propósito almejado e que este propósito esteja claro para o titular dos dados, para evitar riscos desnecessários. É importante ressaltar que o consentimento deve sempre estar relacionado a finalidades determinadas. Isto é, ao consentir, o usuário deve compreender quais são o objetivo e contexto da guarda e utilização daquele dado pessoal. A LGPD expressamente afirma que as autorizações genéricas para o tratamento de dados pessoais serão nulas.

Técnicas de *e-mail marketing* também precisarão ser adaptadas à nova lei. É importante manter listas de *e-mails* atualizadas e precisas, além de assegurar que as pessoas (usuários e consumidores) que constem do banco de dados tenham autorizado ou solicitado o envio do *e-mail*. As empresas devem ainda tomar especial cuidado com sistemas de automação, como o envio automático de *e-mails*. O mesmo vale para empresas que ofertam e promovam produtos e serviços por telefone (*telemarketing*) ou por correio (mala direta postal).

Práticas de direcionamento de anúncios, baseadas na coleta de informações pessoais na Internet, como *cookies* e geolocalização (desde que individualizáveis), também serão afetadas. A recente polêmica envolvendo a instalação,

na Linha 4-Amarela do metrô da cidade de São Paulo, de equipamentos com câmeras de reconhecimento facial nas portas que dão acesso aos trens, ilustra a questão. As câmeras monitorariam o número de transeuntes em suas imediações e, também, as emoções por eles expressadas. Com base em tais informações, anunciantes poderiam categorizar os usuários do metrô e personalizar as propagandas exibidas a eles. Esta situação, em que câmeras possibilitam que os dados das pessoas sejam colhidos e utilizados sem seu prévio consentimento ou sequer ciência, e sem uma justificativa alternativa, exemplifica violação à necessidade de consentimento ou existência de base legal prevista na lei.

Como ainda é incerto o grau de exigência das autoridades e, também, diante da determinação da LGPD de que **a responsabilidade em comprovar que o titular dos dados pessoais consentiu com o tratamento é daquele que realiza o tratamento**, recomenda-se que as empresas sejam cautelosas. O consentimento do cliente deve ser claro, preciso e não deve se referir apenas a operações de exclusão de dados e alteração de preferências, como geralmente ocorre.

4 O titular dos dados pode mudar de ideia e "cancelar" seu consentimento?

Sim, a LGPD estabelece que o titular dos dados poderá, a qualquer momento, cancelar seu consentimento. Portanto, as empresas e demais agentes do setor deverão implementar mecanismos de monitoramento permanente e confiável que possibilitem o ágil cancelamento do consentimento e que impeçam o uso e tratamento de seus dados dali em diante. Assim, é importante que a gestão dos dados seja feita de forma organizada pelas empresas, para que o cancelamento possa acontecer a qualquer instante.

> O consentimento deve ser explícito e claro. Além disso, ele deve poder ser revogado a qualquer momento.

5 O que são "dados sensíveis"? Há alguma diferença entre o consentimento para o tratamento de dados em geral e o consentimento para dados sensíveis?

A lei define dado sensível como "dado pessoal sobre a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação, a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

É possível que empresas que atuem no setor de publicidade armazenem dados que se enquadrem nessa categoria**.** Cuidados especiais devem ser tomados em sua coleta e manuseio. **O consentimento deve ser colhido com o esclarecimento da finalidade específica do uso do dado, de forma destacada. Existe, portanto, um ônus maior de se comprovar que o titular de dados autoriza o tratamento para aquela determinada finalidade do que no caso dos**

outros dados pessoais. Em nenhuma circunstância, entretanto, cláusulas de autorização para tratamento de dados pessoais poderão ser genéricas.

Essa questão merece muita atenção, pois é comum que uma empresa colete dados, obtenha o aval do titular para o tratamento para determinada **finalidade** e, depois, utilize os dados para outras finalidades. Informações colhidas para cadastro podem ser úteis, por exemplo, para direcionamento de publicidade ou segmentação dos consumidores. No caso de dados sensíveis, sempre que houver alteração na finalidade de tratamento de dados, há necessidade de renovação do consentimento de forma expressa.

> O consentimento para dados sensíveis deve sempre explicitar a finalidade de seu uso, de forma destacada. Se houver alteração na finalidade, é preciso renovar o consentimento de forma expressa.

6 E o consentimento de menores de idade?

A LGPD estabelece um tratamento diferenciado para dados pessoais de crianças e adolescentes. Deverão ser tratados sempre no melhor interesse de seus titulares. Quando pertencerem a crianças (até 12 anos de idade), **o consentimento, além de ter que ser colhido de um dos pais ou responsável legal, deverá ser concedido de forma específica e destacada (ou seja, nunca embaralhado em outras cláusulas de um termo de uso ou escondido em letras pequenas num contrato).**

> O tratamento de dados de crianças sempre exige consentimento de um dos pais ou responsável legal.

Além disso, a proteção de dados de crianças e adolescentes deve considerar a legislação aplicável à publicidade infantil. Existem diversas normas que consideram abusiva toda publicidade que se "aproveite da deficiência de julgamento e experiência da criança". Da mesma forma, já há decisão do Superior Tribunal de Justiça (STJ) proibindo, por exemplo, o direcionamento de publicidade de alimentos a crianças, particularmente de venda de brinquedos junto com comidas calóricas. Apesar disso, a questão ainda gera muito debate e dúvidas tanto no meio jurídico como na sociedade civil. Recomenda-se cautela às empresas que façam tratamento de dados pessoais de adolescentes e, principalmente, crianças, para fins de direcionamento de publicidade.

7 Quais os impactos da LGPD sobre a comercialização e o compartilhamento de dados pessoais?

De acordo com a LGPD, o compartilhamento e a comercialização de dados pessoais só podem ocorrer em caso de consentimento expresso e específico do titular dos dados. *Data brokers* (como a Cambridge Analytica), que comercializam dados pessoais como atividade principal, devem se atentar a isso. Mais, a LGPD já determina que o compartilhamento de dados sensíveis "com o objetivo

de obter vantagem econômica" poderá ser vedado ou regulamentado pelas autoridades, e no caso específico de dados de saúde esclarece que a vedação já existe, a menos em casos de consentimento expresso ou para a adequada prestação de serviços de saúde suplementar. Assim, as empresas que desejam comprar dados de outras, como listas de e-mails (*mailing lists)* — ou que os obtenham por compartilhamento -, devem se assegurar de que o vendedor obteve consentimento expresso do titular dos dados para esse fim.

Importante atenção a este ponto, pois **empresas que compram de terceiros dados obtidos/transferidos em desacordo com as normas da LGPD** — obtidos sem o consentimento do titular dos dados ou para outra finalidade, por exemplo — **poderão ser também responsabilizadas pelas violações à lei por parte do vendedor**.

8 A LGPD restringe a tomada de decisões automatizadas baseadas no uso de algoritmos?

O uso de algoritmos não é vedado pela LGPD. No entanto, o artigo 20, que aborda decisões tomadas exclusivamente por meio de automação — ou seja, sem participação de seres humanos –, determina que o titular dos dados pode, sempre que desejar, requerer a revisão de decisão automatizada que afete seus interesses. Como a redação da lei é ampla, será inicialmente possível questionar, inclusive, anúncios específicos dirigidos às pessoas em redes sociais, em buscadores na Internet ou em outros sites. Ante a complexidade deste tema, trataremos do assunto de forma aprofundada e individual em uma nova *newsletter,* no próximo mês.

9 Quais os efeitos para o setor de publicidade das exigências de não-discriminação do titular dos dados?

A LGPD dá atenção especial à possível discriminação ilegal, por parte de empresas e demais responsáveis pelo tratamento de dados. A lei prevê o princípio da não-discriminação, que proíbe o "tratamento para fins discriminatórios ilícitos ou abusivos". Tal princípio pode gerar impactos consideráveis no setor de publicidade, especialmente considerando que qualquer prática de segmentação pode, no limite, ser considerada discriminatória.

Como se trata de disposição genérica, é difícil concluir como será sua aplicação pelas autoridades competentes quando a LGPD entrar em vigor. Mas é razoável assumir que amplo debate a respeito da aplicação de tal princípio será necessário. Por exemplo, práticas corriqueiras como classificação de consumidores segundo seu perfil e publicidade direcionada, atualmente corriqueiras, pressupõe a classificação de pessoas em categorias. Quais critérios serão considerados lícitos para a segmentação de consumidores, bem como para sua segregação em grupos de diferentes perfis? Em quais hipóteses o direcionamento de publicidade será permitido? Por exemplo, o direcionamento de anúncios de planos de saúde a pessoas de determinada faixa etária ou classe social, que se-

riam clientes com perfil mais interessante às operadoras, poderia representar discriminação ilícita?

> Práticas como classificação de consumidores segundo seu perfil e publicidade direcionada devem ser realizadas com cautela, pois podem representar violação ao princípio da não-discriminação.

Tais pontos só serão esclarecidos quando a LGPD for aplicada a casos concretos, ou se vier a ser regulamentada por outras normas. De todo modo**, o uso de dados sensíveis para a classificação de consumidores e o direcionamento de campanhas publicitárias com foco étnico-racial, na orientação sexual ou em convicções religiosas e políticas, por exemplo, deverá receber atenção especial do setor**. Até que se tenha maior clareza quanto aos limites da utilização dos dados, a recomendação às empresas é a cautela.

Aqui, práticas de determinação de preços de acordo com o perfil do consumidor ou sua localização geográfica também podem ser consideradas preocupantes, pois podem vir a contrariar determinações da LGPD que exigem igualdade de tratamento. Não se sabe ainda, por exemplo, se será permitido estipular preços diferentes de acordo com o poder aquisitivo ou a inclinação de uma pessoa a pagar um valor maior por um bem.

Em 2018, a Decolar.com, empresa de reservas *online* de viagens, foi multada com base no Código de Defesa do Consumidor (CDC) por órgão ligado ao Ministério da Justiça por, supostamente, discriminar preços de acomodações segundo a localização geográfica do usuário. Segundo a Secretaria Nacional do Consumidor, o *website* da empresa informava preços maiores aos clientes brasileiros do que aos de outros países, como da Argentina. As consequências de uma atitude equivalente no âmbito da LGPD ainda não estão claras, por não haver jurisprudência ou outras normas que forneçam maior segurança jurídica sobre práticas comerciais e sua aceitação perante a legislação.

Estas perguntas só poderão ser respondidas após a entrada em vigor da lei e depois de um certo período de adequação, tanto das empresas como do governo e órgãos reguladores. Além disso, as disposições do CDC deverão sempre ser consideradas em conjunto com a nova lei, por exemplo, para que os efeitos do princípio da não-discriminação sobre o setor de publicidade sejam completamente esclarecidos.

10 Quais as consequências do descumprimento da LGDP? Como diminuir os riscos?

A LGDP estabelece penalizações pelo descumprimento de suas determinações que vão de advertências com indicação de medidas corretivas e bloqueio dos dados pessoais relacionados à infração, até multas que podem chegar a 2% do faturamento do grupo econômico no Brasil no ano anterior à condenação, dentro do limite de R$ 50 milhões. Permite ainda que, confirmada, a infração seja divulgada amplamente ao público.

O titular de dados pessoais lesado também pode buscar reparação de danos no Poder Judiciário, o que resultaria, além dos custos com a própria reparação, em gastos com honorários de advogados e gerenciamento de processos. A reparação de danos, em especial, é tema que pode vir a gerar preocupações, dada a dificuldade em estimar o valor das indenizações que podem ser impostas, que pode variar bastante de acordo com a natureza do dano — moral ou material — e a sua extensão.

A redação ampla de diversos dispositivos da LGDP torna incerta a avaliação de como serão determinadas as sanções. Apesar disso, a própria lei afirma que serão levados em conta na aplicação de punições a existência de boas práticas e mecanismos e procedimentos internos sólidos de governança na empresa que garantam o tratamento seguro e adequado dos dados. Nesse contexto, destaca-se que antes mesmo da vigência da lei, autoridades brasileiras têm considerado a adoção de boas práticas de proteção de dados como critério relevante na celebração de acordos com empresas envolvidas em casos de vazamento de dados. O Termo de Ajuste de Conduta (TAC) assinado entre Unidade Especial de Proteção de Dados e Inteligência Artificial do Ministério Público do Distrito Federal e a empresa Netshoes, em razão do vazamento de informações de cerca de 2 milhões de clientes em 2018, é um exemplo. Na determinação do valor da indenização estabelecida no acordo, o Ministério Público considerou relevante o fato de que a empresa teve uma postura proativa na notificação de consumidores sobre o incidente e se comprometeu a implantar medidas adicionais ao seu programa de proteção de dados.

Assim, conclui-se que o desenvolvimento e a implementação de programas de *compliance* de dados pelos agentes do setor de publicidade não só é uma estratégia importante de prevenção e redução de riscos de infrações, mas também de redução de danos em eventuais punições. Considerando que existe um período razoável até que a lei entre em vigor (só em agosto de 2020), este é o momento ideal para adequação de práticas das empresas para evitar maiores problemas no futuro.

11 Como será a aplicação da LGPD na esfera administrativa?

A LGPD cria um órgão da administração pública que será responsável por implementar e fiscalizar o cumprimento da lei: a Autoridade Nacional de Proteção de Dados (ANPD). A ANPD terá um papel central no estabelecimento da política pública de proteção de dados pessoais, sendo responsável por guiar a interpretação da norma e regulamentar padrões e técnicas aplicáveis a questões de segurança da informação, interoperabilidade e processos de anonimização. Além disso, com o objetivo de fiscalizar o cumprimento da LGPD, a ANPD poderá requisitar informações sobre tratamentos de dados pessoais para agentes de tratamento e aplicar sanções administrativas em caso de descumprimento da norma (descumprimento este que só será identificado por meio de processo administrativo com contraditório, ampla defesa e possibilidade de recurso). Por fim, ANPD poderá criar normas, orientações.

12 De quem é a responsabilidade por eventuais infrações? A empresa pode responder por adquirir dados obtidos/transferidos em desacordo com as normas da LGPD?

As sanções discutidas acima podem ser aplicadas às empresas operadoras e controladoras quando o tratamento de dados causar dano patrimonial, moral, individual ou coletivo em violação à legislação de proteção de dados.

A diferença entre operador e controlador se dá no fato de que o controlador é aquele que toma as decisões sobre como os dados serão tratados, enquanto o operador é quem efetivamente realiza o tratamento, seguindo as orientações do controlador. Por exemplo, no caso de uma empresa que contrata agência de publicidade para realização de serviços de CRM, a empresa seria a controladora e a agência de CRM, que de fato realiza o tratamento dos dados, a operadora.

A regra geral é que o controlador é sempre responsável por qualquer dano causado, mas o operador será igualmente responsabilizado se (i) deixar de cumprir com as orientações do controlador sobre o tratamento dos dados, ou (ii) descumprir com as regras da LGPD. Nesses casos, ambas as empresas seriam responsabilizadas para fins de sanção administrativa.

Por exemplo, empresa que adquira dado sensível obtido sem o consentimento concedido de forma específica e destacada de seu detentor pode ser penalizada pelo descumprimento à LGDP, conjuntamente ao *data broker* que os vendeu, mesmo que não tenha feito a coleta ilícita das informações. Nesse caso, há **responsabilidade solidária pelas violações à lei de proteção de dados,** independentemente de qualquer disposição contratual em contrário acordada pelas partes. ■

Documento elaborado com a colaboração do **Cômite Técnico Digital do Cenp**. Tendo em vista que a LGPD ainda não se encontra em vigor e, como determinado pela própria lei, diversos temas dependem de regulamentação mais precisa da Autoridade, esse texto está sujeito à evolução do entendimento da doutrina e da jurisprudência.

VMCA

Vinicius Marques de Carvalho Advogados

Rua Doutor Rafael de Barros, 210 9º andar Paraíso 04003 041 São Paulo SP Brasil

+55 11 3939 0708 | contato@vmca.adv.br | www.vmca.adv.br