TEXTO DE CAROLINA TAVARES

De olho na segurança do seu cliente

Lei que regulamenta o tratamento de dados pessoais envolve empresas de todos os portes e segmentos. Saiba como adaptar o seu negócio para evitar multas já no próximo ano

Ter um banco de dados de clientes é imprescindível se a sua empresa lida com o público. Afinal, conhecê-los é importante para direcionar produtos e campanhas que realmente sejam do seu interesse. No entanto, com tanta onda de vazamentos de dados pessoais de clientes até por grandes empresas como Facebook, tornou-se cada vez mais essencial ter regras que digam até onde se pode usar as informações pessoais dos clientes com fins de vendas e poder.

Por isso, a Lei Geral de Proteção de Dados Pessoais (LGPD) 13.709, sancionada em 2018, sofreu diversas alterações e entrará em vigor em agosto de 2020. E não pense que o tamanho da companhia não é parâmetro de exclusão para a aplicabilidade das novas regras. Seja você micro, pequeno, médio ou grande, de qualquer segmento de atuação, se coleta e armazena dados pessoais, terá que atender às exigências da nova legislação.

O Brasil passou a fazer parte dos países com esta legislação específica para proteger a privacidade dos cidadãos, assim como o General Data Protection Regulation, da União Europeia, e o California Consumer Privacy Act of 2018, dos Estados Unidos. Mesmo assim, uma pesquisa do Serasa Experian mostrou que cerca de 85% das empresas brasileiras ainda não estão preparadas para atender às exigências da LGPD.

Qualquer dado pessoal em território brasileiro que envolva o objeto das atividades empresariais estará sujeito a penalidades caso não seja realizado o tra-

tamento correto. Será um momento de adaptação das empresas, cidadãos, órgãos públicos e autoridades regulatórias, como explica a sócia do L.O. Baptista Advogados, Esther Cunha. "A Lei dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa", afirma.

Situações como venda de cadastros, uso dos dados coletados sem autorização do titular e vazamento de informações são exemplo de violações da LGPD, completa o diretor de Segurança Cibernética da Service IT e professor da Unisinos, Leonardo Lemes.

DE ACORDO COM A LEI

Mas, afinal, o que minha empresa precisa fazer para se adequar aos novos procedimentos?

Primeiro, Esther conta que a nova lei exige uma mudança da cultura interna das empresas, passando a incorporar algumas práticas específicas de privacidade e segurança. Isso porque a LGPD é aplicável a qualquer operação de tratamento (coleta, produção, utilização, reprodução, eliminação) de dados pessoais que preencha um dos seguintes requisitos: A. Seja realizada no Brasil; B. Tenha por objetivo a oferta de bens ou serviços ou ainda o tratamento de dados de indivíduos no Brasil; C. Seja referente a dados pessoais coletados no Brasil. "A LGPD somente não é aplicável em situações excepcionais previstas no Art. 4º da mesma lei. Para adequação das empresas, é necessária a revisão, a adaptação e, possivelmente, a criação de novos procedimentos internos, além da conscientização de todos os colaboradores sobre a LGPD e seus impactos nas suas atividades, tanto por meio de políticas internas como através de treinamento dos colaboradores", explica.

Alguns pontos também merecem maior atenção. Caso a empresa trate dados pessoais de crianças e adolescentes (Art. 14, LGPD) ou dados sensíveis (Arts. 5º, II e 11, 12 e 13, LGPD), por exemplo, deverá garantir o cumprimento de requisitos ligados a essas categorias. A LGPD prevê responsabilidade solidária entre controladores e operadores (Art. 42 e ss., LGPD), significando que empresas não diretamente ligadas a uma violação da lei podem ser responsabilizadas e obrigadas a reparar danos causados por outra empresa da cadeia, em lógica semelhante à do Código de Defesa do Consumidor. "As legislações anteriores já tratavam do tema. Contudo, a LGPD é uma lei que zela pelo direito do titular dos dados, os cidadãos, independentemente do segmento de atuação da empresa e que não se restringe ao meio (digital ou impresso) em que esse dado esteja sendo tratado", acrescenta Lemes.

O primeiro passo da mudança seria mapear os dados pessoais e entender contexto e práticas de cada organização, implicando nesse processo questões jurídicas, de tecnologia da informação e de segurança, além de uma revisão dos aspectos do negócio. As penalidades previstas podem chegar a multas no valor de R$50 milhões por infração, quando for devidamente apurada e confirmada. "A Lei não impede que o dado seja utilizado para uma ou outra finalidade, ela apenas

ERROS MAIS COMUNS

- Imaginar que a LGPD se aplica apenas a dados no ambiente digital. A LGPD se aplica a dados pessoais em qualquer formato (Art. 1º, LGPD).
- Assumir que uma empresa que tem como clientes pessoas jurídicas, e não pessoas naturais, não está abrangida pela LGPD.
- Esquecer que no ambiente interno de toda empresa há, no mínimo, fluxo de dados pessoais dos colaboradores.
- Acreditar que sempre é necessário obter consentimento dos titulares para tratar seus dados pessoais. A LGPD estabelece dez bases legais diferentes e deve ser feita uma análise caso a caso para identificar qual a base legal mais adequada para cada finalidade de tratamento (Art. 7º, LGPD).
- Pensar que bastará incluir nos contratos, documentos e plataformas da empresa um parágrafo genérico dizendo que o titular consente com o tratamento de seus dados pela empresa para fins indeterminados. A LGPD estabelece requisitos de validade para o consentimento (deve ser livre, o controlador deve ser capaz de demonstrar a manifestação de vontade do titular, deve se referir a finalidades determinadas, deve ser revogável – Art. 8º, LGPD).
- Não lembrar que a lei determina que o controlador deve assegurar a segurança dos dados pessoais, e deixar de implementar políticas e sistemas próprios.
- Criar ferramentas e produtos que sejam ótimos sob perspectiva de vendas, mas que não necessariamente atendam às exigências da LGPD. É importante que os produtos e ferramentas das empresas sejam concebidos de forma a garantir a privacidade e segurança ("*privacy by design*").
- Esquecer que a empresa deve criar canais e mecanismos para que os titulares de dados pessoais possam exercer de forma efetiva os seus direitos quanto a dados pessoais.
- Atribuir a uma única área ou departamento a função de deixar a empresa em conformidade com a LGPD. O ideal é que se estabeleça um comitê composto por profissionais de diferentes áreas (jurídico, TI, RH, comercial, *compliance* e outros).

exige que o usuário seja informado dessa utilização e autorize. Acaba devolvendo para o usuário o controle de algo que sempre foi dele, possibilitando-lhe decidir se quer ou não fornecer o dado e, ainda, que saiba exatamente para que ele será utilizado", explica o diretor executivo da IT2S, Leonardo Goldim.

Ele conta ainda que há a possibilidade de a Autoridade Nacional simplificar procedimentos para que microempresas e empresas de pequeno porte possam adequar-se. Mesmo assim, não conte com a sorte! Comece desde já sua reorganização para evitar problemas futuros. Os maiores riscos envolvem incidentes como *ransonware* – um tipo de ameaça que criptografa os arquivos e pede um resgate para que sejam liberados novamente; vazamento de dados; invasão de dispositivos e outros.

Ou seja, não se trata apenas do que sua empresa faz com as informações, mas também da segurança delas em relação a ameaças externas, tornando você o responsável. A disciplina jurídica dos dados pessoais está espalhada em diversas leis, como o Marco Civil da Internet e seu decreto regulador, o Código de Defesa do Consumidor, o Estatuto da Criança e do Adolescente, a Lei do Cadastro Positivo, Lei do Sigilo Bancário, normas do CMN e do BACEN sobre Cibersegurança, a Lei de Acesso à Informação, entre outras. "A LGPD não afasta a aplicação das regras sobre proteção de dados pessoais já estabelecidas em outras leis, mas reúne os direitos dos titulares de dados pessoais e estabelece para as empresas a obrigação de garantir os direitos dos titulares e criar mecanismos para que isso ocorra de forma rápida e eficaz", adverte Esther.

ATENÇÃO REDOBRADA

Empresas que já possuem outras obrigações relacionadas permanecem obrigadas, segundo Esther, a menos que a LGPD disponha em contrário. Além disso, a LGPD estabelece uma autoridade fiscalizadora e sancionadora para prevenção e repressão de práticas abusivas, relativamente a dados pessoais, sendo também atribuição dessa Autoridade

© UNILEGIÃO / ACERVA

"A Lei não impede que o dado seja utilizado para uma ou outra finalidade, ela apenas exige que o usuário seja informado dessa utilização e autorize. Acaba devolvendo para o usuário o controle de algo que sempre foi dele, possibilitando-lhe decidir se quer ou não fornecer o dado e, ainda, que saiba exatamente para que ele será utilizado"

LEONARDO GOLDIM,
DIRETOR EXECUTIVO DA IT2S

BÊ-Á-BÁ DA LGPD

O QUE MUDA: as leis existentes hoje garantem o direito à intimidade e ao sigilo de comunicações, porém foram criadas e implementadas em um cenário que não contemplava soluções tecnológicas. A LGPD é uma legislação que disciplina como as empresas e os setores públicos podem coletar e tratar dados de pessoas, determinando direitos, exigências e procedimentos a serem seguidos.

A TRANSIÇÃO: o ideal é contar com um parceiro com *expertise* para ajudar na transição e com serviços que possam ser facilmente implementados. A adequação começa a valer em agosto de 2020, o que significa que as empresas têm menos de um ano para estar em conformidade.

PASSO A PASSO: desde o mapeamento de todos os dados que são coletados do usuário, onde esses dados estão sendo armazenados, quais dados o usuário consentiu que fossem coletados e qual o uso de cada dado, até processos de remoção completa dos dados por solicitação do usuário e a definição de um responsável pela proteção e privacidade de dados na empresa.

APLICABILIDADE DA LEI: atualmente, qualquer empresa, órgão ou pessoa física que não cumprir as orientações ditadas pela lei poderá pagar multas que variam entre R$50 milhões e 2% do faturamento total da empresa. Mas as penalizações ainda estão em avaliação pela Autoridade Nacional de Proteção de Dados (ANPD), responsável pelas diretrizes.

EXEMPLOS: diversas atividades comuns que vemos atualmente podem ser consideradas ilegais, desde atividades como a venda de dados até a simples coleta de dados sem consentimento do usuário (como dados coletados para *marketing* e outros).

© DIVULGAÇÃO / FOTÓTICA

“A LGPD não afasta a aplicação das regras sobre proteção de dados pessoais já estabelecidas em outras leis, mas reúne os direitos dos titulares de dados pessoais e estabelece para as empresas a obrigação de garantir os direitos dos titulares e criar mecanismos para que isso ocorra de forma rápida e eficaz”

ESTHER CUNHA, SÓCIA DO L.O. BAPTISTA ADVOGADOS

Nacional de Proteção de Dados (ANPD) educar a população sobre privacidade e proteção de dados pessoais.

Leonardo Lemes conta que uma coleta de dados realizada para uma finalidade específica não poderá ser usada para outra sem o devido consentimento. “Além disso, é preciso oferecer ferramentas que permitam ao usuário revogar esse consentimento quando quiser. A compra de base de dados de terceiros para envio de publicidade, por exemplo, pode ser um tiro no pé quando a empresa não documentar o ciclo de vida dos dados pessoais dentro da organização e indicar a finalidade deles”, afirma.

Um dos pilares da LGPD é a autodeterminação informativa, isto é, o titular dos dados pessoais deve ter controle sobre o fluxo. “A comercialização indeterminada de dados pessoais sem o conhecimento dos titulares vai em direção completamente oposta à autodeterminação informativa e com as exigências da LGPD”, completa Esther.

PROTEJA-SE!

Um bom *design* de PKI (*Public Key Infrastructure* ou chaves de segurança), usando certificados digitais, pode proteger organizações bem-sucedidas, com foco em uma abordagem de segurança por *design*. Isso é especialmente importante para os fabricantes de dispositivos de IoT (*Internet of Things - Internet* das Coisas) e as empresas que os utilizam, além de empresas com forte presença digital para lidar com comércio eletrônico, transações financeiras e informações privadas, como data de nascimento, endereço, ID do governo.

O uso de PKI reforça os princípios básicos de segurança – autenticação, criptografia, dados e integridade do sistema –, pode ajudar a proteger *sites* e aplicativos conectados à *internet*, bem como dispositivos de IoT na rede e à medida que são fabricados. “Os certificados digitais e PKI podem fornecer uma camada importante de defesa e prova de que você leva a sério a segurança de seus clientes e mantém os dados privados”, alerta o representante principal do DigiCert, Timothy Hollebeek. O profissional tem mais de 15 anos de experiência em segurança de computadores, incluindo oito

“Além disso, é preciso oferecer ferramentas que permitam ao usuário revogar esse consentimento quando quiser. A compra de base de dados de terceiros para envio de publicidade, por exemplo, pode ser um tiro no pé quando a empresa não documentar o ciclo de vida dos dados pessoais dentro da organização e indicar a finalidade deles”

LEONARDO LEMES, DIRETOR DE SEGURANÇA CIBERNÉTICA DA SERVICE IT E PROFESSOR DA UNISINOS

© DIVULGAÇÃO / RPNA

SELO DE QUALIDADE

A Associação Brasileira de Fintechs - ABFintechs, em parceria com a empresa de tecnologia IT2S Group, acaba de lançar um selo de qualidade voltado à segurança de dados. O Programa Fintech Segura é uma iniciativa para trazer mais transparência sobre a maturidade das *startups* do setor nos temas de proteção e privacidade de dados, além de fomentar as boas práticas de segurança da informação e proteção de dados pessoais, que é um dos requisitos da LGPD. As recomendações de segurança são práticas e objetivas, sendo aplicáveis a *startups* em qualquer fase operacional.

anos trabalhando em pesquisas inovadoras sobre segurança financiadas pela Agência de Projetos de Pesquisa Avançada de Defesa.

Ele ressalta também que uma boa higiene de segurança exige o uso de certificados digitais em todos os pontos de conexão – páginas da *web*, interna e externamente, para proteção de *e-mail*, acesso remoto, autenticação de dispositivos IoT e proteção dos dados compartilhados com criptografia e assinatura de código no *firmware* do dispositivo. "É aqui que entra o TLS - *Transport Layer Security*, conhecido como SSL para *Secure Socket Layer*, que foi substituído pelo TLS. Uma tecnologia de segurança padrão criada para proteger o tráfego na *internet* usando criptografia, também", acrescenta.

Além disso, todos os servidores *web* na *internet* precisam de certificados de segurança. Antes, eram projetados para comércio eletrônico e transações financeiras, para *sites* em que outras informações confidenciais eram inseridas, como informações de identidade pessoal ou *logins*. Atualmente, a necessidade de criptografar a *web* por padrão é motivada pela proteção da livre troca de ideias e pela privacidade dos usuários contra o governo, agências de espionagem ou pessoas com intenções criminais. "O Google deu aos *sites* HTTPS um valor extra em seus algoritmos de pesquisa há alguns anos. Todos os principais navegadores agora marcam *sites* HTTP que não usam certificados TLS como Não Seguro. As empresas não podem mais ignorar o uso de certificados TLS, não apenas em *sites* que realizam transações com informações valiosas, mas em todos os *sites* da *internet*", conclui. G&N

© DIVULGAÇÃO | SOURCE MARKETING

"Todos os principais navegadores agora marcam *sites* HTTP que não usam certificados TLS como Não Seguro. As empresas não podem mais ignorar o uso de certificados TLS, não apenas em *sites* que realizam transações com informações valiosas, mas em todos os sites da *internet*"

TIMOTHY HOLLEBEEK, REPRESENTANTE DO DIGICERT

DICAS DE SEGURANÇA

1. Crie modelos de ameaças: avalie o caso de uso dos *sites*, aplicativos e serviços conectados à *internet* durante sua fase de *design*. Avalie os vários riscos e crie planos de mitigação no *design* geral de seus aplicativos voltados para a *web*, incluindo servidores de preparação e produção.

2. Elabore casos de segurança e abuso: certifique-se de colocar sua equipe para trabalhar seu modelo de ameaça. Implemente uma avaliação contínua para garantir que o modelo de ameaça continue atendendo seus cenários de ameaça.

3. Gerencie chaves com segurança: integre seus processos gerando e armazenando suas chaves privadas com segurança, usando os módulos de segurança de *hardware* (HSM) ou uma das principais plataformas de IoT

4. Coloque certificados em uso: saiba onde sua organização pode usar certificados em vez de senhas para autenticação com integração ao Active Directory. Os certificados de infraestrutura de chave pública (PKI) desempenham um papel fundamental em sua solução, pois validam a identidade para que apenas usuários e servidores autorizados possam acessar um dispositivo ou