Genetec dispõe de especialista em segurança física, cibernética e privacidade preparado para ajudar as companhias a garantirem sua conformidade à nova lei, como cuidados com os dados coletados e tratados em diferentes processos, desde o os sistemas de acesso, de vendas e marketing até na captação de imagens pessoais

Ueric Melo, engenheiro de aplicação e gestor de privacidade e especialista em cibersegurança da Genetec

Mesmo tendo entrado em vigor há mais de um ano, as empresas ainda têm dúvidas sobre quais políticas e procedimentos adotar para estarem em conformidade com a Lei Geral de Proteção de Dados (LGPD) e precisam atualizar e adaptar todos os seus processos, sistemas físicos e cibernéticos para respeitar os novos parâmetros de privacidade e segurança definidos pela legislação. Ciente disto, Ueric Melo, especialista da Genetec, aponta cuidados fundamentais para garantir a compliance das empresas com a nova regulamentação.

“É uma lei absolutamente necessária, mas que demanda muita atenção à coleta, armazenamento,

tratamento e análise de todos os dados pessoais, pois quaisquer transgressões podem resultar em multas pesadas e em graves danos à reputação de empresas e marcas, por estar intrinsicamente vinculada às relações das empresas com seus clientes e demais públicos, além dos potenciais danos aos titulares de dados pessoais", explica Melo, que é engenheiro de aplicação, gestor de privacidade e especialista em cibersegurança da Genetec. Por isto, não é à toa, que a LGPD estabelece que as grandes e médias empresas, além daquelas que realizam tratamento de dados que tragam um alto risco para os titulares, devem contar com um Encarregado pelo Tratamento de Dados Pessoais (DPO) para fazer a gestão de compliance à LGPD, exigência recentemente atenuada através de resolução publicada pela NAPD, somente para pequenas e microempresas, que foram dispensadas de ter este profissional, mas estão sujeitas à todas as punições estabelecidas pela lei.

O especialista adverte que **o primeiro passo é ter uma definição clara do que são considerados "dados pessoais"**, um termo que não se restringe apenas a nome, telefone, endereço, documentos e fotos do indivíduo. Mas inclui também dados indiretos, que permitam a identificação da pessoa, como imagem do rosto, número de IP do computador, IMEI do Celular (identificação de cada aparelho), placas de carros e motos, cookies armazenados na máquina, que facilitam a navegação, mas também permitem identificar preferências e traçar o perfil dos clientes, entre outros. "É preciso ainda mais atenção aos dados pessoais considerados sensíveis, que podem identificar a pessoa e gerar algum tipo de desconforto, preconceito ou restrição, como aqueles referentes à saúde, raça ou religião da pessoa, e que, quando necessários, devem ter tratamento diferenciado para assegurar a privacidade", destaca Melo.

O segundo passo é estabelecer quais dados pessoais precisam ser tratados para garantir a operação e o sucesso dos negócios, ou seja, quais informações são realmente relevantes para a finalidade de um processo específico e da companhia, para que os profissionais de segurança da informação determinem as políticas e estratégias de proteção mais adequadas. "Para oferecer um desconto aos clientes, por exemplo, um varejista deve analisar a real necessidade de pedir o CPF do consumidor, e se existe uma forma menos intrusiva de atingir o mesmo objetivo ", explica o especialista da Genetec.

Com isto em mente, a empresa deve **adequar os seus sistemas tecnológicos para coletar o mínimo de dados pessoais possível** e descartar os desnecessários, reduzindo assim o volume de informações a ser armazenado e tratado diariamente. Isto porque é hora de considerar o tratamento destes dados de acordo com as bases legais da LGPD, que são monitoradas pela ANPD. "É preciso saber, por exemplo, os motivos que justificam a companhia ter e tratar cada tipo de dado", detalha o especialista da Genetec. **É fundamental também usar a tecnologia como aliada na proteção dos dados e da privacidade dos titulares**, com ferramentas que ajudem a anonimizar ou "pseudonimizar" os dados, que tenham recursos com criptografia em diversos níveis, ou, por exemplo, permitam distorcer as imagens faciais dos titulares em câmeras, como o Genetec Privace Protector, limitando o acesso a casos de extrema necessidade e a um número restrito de gestores.

Outro aspecto que exige atenção é o controle de acesso das pessoas às instalações das organizações, pois nestes sistemas é evidente a necessidade de coleta de dados pessoais, por tanto, é recomendado uma atenção especial na hora de escolher e gerenciar os sistemas de controle de acesso físico. "Hoje, é possível a utilização de recursos de pseudonimização, permitindo que dados as informações do o crachá ou credencial sejas armazenados em um banco de dados e que todos os demais dados pessoais fiquem armazenados em uma tabela separada", alerta Melo.

Em relação à contratação de produtos e serviços tecnológicos, como apps de entrega, de transporte etc., é essencial a correta gestão dos dados em relação à LGPD para **garantir que os dados dos usuários da empresa-cliente não são compartilhados com outras organizações**, sem a prévia autorização ou conhecimento dos titulares. Afinal, se houver qualquer vazamento ou se as informações forem armazenadas e tratadas de forma inadequada, a responsabilidade inicial é do fornecedor do produto ou serviço (controlador). Além disso, é preciso ter este controle do tratamento, porque o titular tem direitos previstos em lei, como o de solicitar

confirmação, acesso, correção, portabilidade e até mesmo a eliminação de seus dados, entre outros.

Outro cuidado consiste na necessidade de integração e atualização constante dos sistemas de TI de modo a permitir que caso o titular solicite acesso aos seus dados pessoais tratados pela empresa, ela consiga atender à solicitação dentro do prazo de 15 dias, estabelecido pela lei. “Isto porque em grandes empresas, com carteiras de clientes que incluem milhares ou milhões de pessoas, se 100, 200 ou 1.000 delas resolverem fazer este pedido no mesmo dia, a companhia precisa estar pronta para atender”, alerta o especialista da Genetec. **É essencial também assegurar que a empresa já adote boas práticas de governança e segurança física e cibernética**, que contribuam para a segurança geral dos dados e de sua privacidade. “O ideal é que a empresa utilize frameworks de governança e privacidade para proteger os dados, atenuando sanções previstas no artigo 52, mantendo um ciclo de melhoria contínua, que lhe permita avaliar de forma recorrente os processos de tratamento dos dados”, recomenda Melo.

E, por último, mas de extrema relevância está a **exigência de que as grandes e médias empresas contêm com os serviços de um DPO**, que é o profissional responsável por zelar pelo cumprimento de todas as exigências da LGPD e por responder pela empresa junto à ANPD. “Este profissional pode integrar os quadros da companhia ou pode-se optar por serviços terceirizados, mas sua escolha é de máxima importância, porque é necessário conhecer profundamente a lei e conceitos mais amplos de proteção de dados pessoais, além de possuir conhecimento sobre os negócios da companhia, contribuir para que as boas práticas sejam inseridas na cultura empresarial, fazer o enquadramento legal (compatibilizar as exigências da LGPD com as de outras leis que regem os seus negócios no Brasil e no exterior, como a GPDR), instruir e disseminar conhecimento em relação à privacidade e proteção de dados, entre outras atribuições.

Conheça as bases e princípios estabelecidos pela LGPD

As bases para coleta e tratamento de dados pessoais estabelecidas pela LGPD, de acordo com o artigo 7º são que o tratamento só poderá ser realizado com o prévio consentimento do titular, quando for necessário para o cumprimento de obrigação legal ou regulatória pelo controlador, ou caso o titular contrate um produto ou serviço. Eles podem ser tratados também pela administração pública com o intuito de balizar a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, assim como para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, sua anonimização.

O tratamento pode ocorrer ainda para o exercício regular de direitos em processo judicial, administrativo ou arbitral (Lei de Arbitragem), para a proteção da vida ou da incolumidade física do titular ou de terceiros, bem como para a tutela da saúde, em procedimentos realizados por profissionais da área ou por entidades sanitárias. Outras possibilidades são quando os dados forem necessários para atender aos interesses legítimos do controlador ou de terceiros - exceto no caso de prevalecerem direitos e liberdades fundamentais do titular; ou para a proteção do crédito, quanto ao disposto na legislação pertinente.

Entre os princípios norteadores da LGPD, presentes no artigo 6º da lei estão a boa-fé; a definição da finalidade - tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de uso em formas incompatíveis. Estão também incluídas a necessidade, que consiste na limitação de tratar o mínimo de dados necessário para a realização das finalidades empresariais; a qualidade e o livre acesso, que garantem aos titulares o direito de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais, que devem ter exatidão, clareza, relevância e atualização constantes.

A lei considera também imprescindível a transparência no uso de informações claras, precisas e facilmente acessíveis sobre o tratamento e os respectivos agentes, observados os segredos comercial e industrial, assim como a garantia de que as empresas adotam medidas de segurança técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. “A lei inclui

também dois princípios que deveriam ser óbvios: de não discriminação, ou seja, a garantia de impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e exigência de responsabilização e prestação de contas em relação a qualquer falha no tratamento ou vazamento dos dados pessoais", acrescenta o especialista da Genetec.

Sobre a Genetec

A Genetec Inc. é uma empresa global de tecnologia que vem transformando o setor de segurança física há mais de 25 anos. Hoje, a empresa desenvolve soluções projetadas para melhorar a segurança, a inteligência e as operações de empresas, governos e comunidades em que vivemos. Seu principal produto, o Security Center, é uma plataforma de arquitetura aberta que unifica vigilância por vídeo baseada em IP, controle de acesso, reconhecimento automático de placas de veículos (ALPR), comunicações e análises. Fundada em 1997 e sediada em Montreal, Canadá, a Genetec atende seus clientes por meio de uma extensa rede de parceiros de canal e consultores certificados em mais de 159 países.

Fonte: Ink, em 20.04.2022