TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO
Av. Rangel Pestana, 315 – Centro - CEP 01017-906 - São Paulo/SP-PABX: 3292-3336
Coordenadoria de Comunicação Social (CCS) – Jornalista responsável: Laércio Bispo MTB 33.444

ARTIGO
21/10/2021

Recomendações de medidas técnicas e administrativas de segurança da informação para municípios de pequeno porte na jornada de adequação à LGPD

**** Fabio Correa Xavier***
Diretor do Departamento de Tecnologia da Informação (DTI) do Tribunal de Contas do Estado de São Paulo (TCESP)

A Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – se aplica tanto ao setor privado, quanto ao setor público. A Administração Pública vem há muito tempo coletando dados pessoais de maneira indiscriminada e sem se preocupar com princípios elencados no art. 6º na LGPD – especialmente finalidade, adequação, necessidade ou mesmo segurança –, e nem com o caput do art. 23, que define que o tratamento de dados pessoais pelas pessoas jurídicas de direito público "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". Via de regra, optava-se por maximizar a coleta de dados, mesmo sem ter a certeza em relação à sua necessidade para atender sua finalidade pública, para executar suas competências e atribuições legais, como previsto no caput do art. 23 da LGPD.

Contudo, com a LGPD, é fundamental que o setor público esteja em conformidade com a novel legislação, sem prejuízo à consecução de suas atividades finalísticas. E essa adequação vale para toda e qualquer entidade pública, inclusive para os municípios de pequeno porte, que possuem, invariavelmente, dificuldades com disponibilidade de recursos – orçamentários, de infraestrutura e pessoal –, o que torna a jornada de adequação mais hercúlea.

Reforçando seu papel orientativo, especificado na competência atribuída pelo art. 55-J, XVIII, da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) lançou no último dia 4 de outubro o seu segundo guia orientativo, intitulado 'Segurança da Informação para Agentes de Tratamento de Pequeno Porte', e um *checklist* – disponíveis no *site* da ANPD – para facilitar a visualização das sugestões que serão adotadas. Trata-se de um documento que sugere padrões técnicos mínimos de segurança que as micro e pequenas empresas, além de *startups*, podem utilizar para proteger os dados pessoais sob sua guarda. Não obstante, o guia informa que "[a]s medidas sugeridas devem ser entendidas como boas práticas e **devem ser complementadas** com outras que possam ser identificadas como necessárias para promover a segurança no fluxo informacional da organização". Além disso, a ANPD afirma que o documento não tem efeito normativo vinculante e trata-se apenas de um guia de boas práticas, que poderá ser atualizado e aperfeiçoado sempre que necessário.

Embora não seja direcionado ao setor público, entendo que tais orientações possam ser seguidas pelos municípios, especialmente os de pequeno porte, como forma de se construir um ambiente institucional mais seguro e, consequentemente, materializar os princípios da boa-fé, segurança e prevenção, constantes no art. 6º da LGPD.

O guia é dividido em Medidas Administrativas, Medidas Técnicas e recomendações para dispositivos móveis e serviços na nuvem.

As medidas administrativas são aquelas que tratam de política e procedimentos relacionados à segurança da informação. As medidas citadas no guia são:

(i) Política de Segurança da Informação: mesmo que seja simplificada, perfaz um conjunto de diretrizes e regras para viabilizar o planejamento, a implementação e o controle de ações de segurança da informação dentro da instituição;

(ii) Conscientização e Treinamento: uma vez que as pessoas muitas vezes são negligenciadas, mas são parte vital para o sucesso de qualquer ação em relação à segurança da informação e proteção de dados;

(iii) Gerenciamento de contratos: com a inclusão de termos de confidencialidade para funcionários e em contratos com fornecedores e clientes nos quais deve haver a inclusão de cláusulas que determinem as responsabilidades e funções em relação à LGPD.

Adicionalmente, diferentemente dos agentes de tratamento de pequeno porte, os municípios de pequeno porte **devem indicar um encarregado pelo tratamento de dados pessoais**, como definido no art. 23, inciso III, da LGPD. O encarregado é o responsável pelas comunicações entre o controlador, o titular de dados e a ANPD, sendo um canal interativo entre esses atores. Além disso, o encarregado é o indivíduo responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD. O ideal é que o indicado tenha conhecimento multidisciplinar – legislação, privacidade e proteção de dados, tecnologia da informação, segurança da informação, metodologias de análise de risco e governança, administração e atendimento às demandas internas e externas. Além disso, ele deve ter autonomia, independência e recursos – financeiros, estrutura e pessoal – para exercer suas atribuições. Deve-se, também, evitar possíveis conflitos de interesse e acúmulo de funções dentro da instituição. Ademais, conforme §1º do artigo 41 da LGPD, a identidade e as informações de contato do encarregado devem ser publicadas no sítio eletrônico do controlador, para que ele possa ser facilmente encontrado, tanto pela ANPD, quanto pelos titulares dos dados e demais interessados, atendendo ao princípio da transparência. Isso é importante, pois os "direitos dos titulares (art. 18) são, em regra, exercidos em face do controlador, a quem compete, entre outras providências, fornecer informações relativas ao tratamento, assegurar a correção e a eliminação de dados pessoais, receber requerimento de oposição a tratamento".

As **medidas técnicas** seriam aquelas mais relacionadas às tecnologias e controles que podem ser implementados em relação à segurança da informação.

O guia cita as seguintes medidas técnicas:

(i) **controle de acesso**, baseado na necessidade de acesso aos dados pessoais, implementando política de senhas complexas e desabilitando senhas padrões de fabricantes. Também recomenda que não se faça o compartilhamento de senhas entre funcionários e que se adote o princípio do menor privilégio, ou seja,

atribuir o nível de acesso necessário para a realização das atividades de cada funcionário. Por fim, recomenda a utilização de autenticação com múltiplos fatores, ou seja, usar, além da senha, biometria ou *tokens* para o processo de autenticação e autorização para acesso a sistemas;

(ii) **segurança dos dados pessoais armazenados**, com ressalva para a observação ao princípio da necessidade (art. 6º, III), com a minimização da coleta dos dados, atentando-se para a configuração segura das estações de trabalho e não utilização de dispositivos de armazenamento externo, como HD ou *pendrives*. Essa medida também se relaciona com as cópias de segurança (*backup*) e uso de criptografia nos dados armazenados;

(iii) **segurança das comunicações**, com a utilização de protocolos de comunicação seguros – como TLS/HTTPS – e aplicativos com criptografia fim a fim, inclusive com o uso de e-mails criptografados, se forem utilizados para envio de dados pessoais. Há, ainda, a necessidade de se utilizar tecnologias de proteção de tráfego, como sistema de *firewall*, antivírus, *antispyware* e *AntiSpam*. Por fim, remover qualquer dado pessoal que esteja em redes públicas, como o *site* da empresa, caso não exista a necessidade de tal publicidade;

(iv) **manutenção de programa de gerenciamento de vulnerabilidades**, para monitorar e aplicar correções de sistemas e aplicativos lançadas pelos servidores. É importante manter os sistemas atualizados, para se minimizar o risco de ser vítima de um ataque que explore vulnerabilidades conhecidas. Além disso, deve-se também manter antivírus e *antimalwares* sempre atualizados e com varreduras periódicas em todos os dispositivos da empresa.

Para dispositivos móveis, como *notebooks*, *tablets* e *smartphones*, o guia sugere que estejam sujeitos aos mesmos procedimentos de controle de acesso implantados para os demais equipamentos da empresa, incluindo autenticação com múltiplos fatores. O documento recomenda, ainda, que a empresa separe os dispositivos móveis de uso privado daqueles de uso institucional. Ou seja, a recomendação é que não se utilize dispositivos móveis particulares para fins institucionais, uma vez que estão mais sujeitos a vulnerabilidades, trazendo mais risco para o agente de tratamento. Uma última orientação neste quesito é a implementação de funcionalidade que permita apagar todos os dados no dispositivo, de forma remota, para ser usada em caso de perda ou roubo do equipamento.

Quanto a serviços na nuvem, é importante ter um contrato de acordo de nível de serviço (*Service Level Agreement;* SLA) adequado, que contemple a segurança dos dados armazenados e uso de autenticação com múltiplos fatores, para acesso aos serviços e dados pessoais que estão na nuvem.

Segurança da informação é uma área bastante dinâmica, muito embora as recomendações feitas no guia possam servir como um caminho inicial para os municípios de pequeno porte. Contudo, há outras práticas e recomendações que podem (e devem) ser buscadas, para que se tenha um ecossistema de privacidade e proteção de dados cada vez mais efetivo. A título exemplificativo, há boas práticas já consolidadas no mercado, como as normas da família 27.000 da ABNT/ISO/IEC. Recomendo, também, a observância em relação às principais violações que ensejaram a aplicação de multas pelas autoridades de proteção de dados da Europa, como já abordei em um artigo no *MIT Technology Review*, 'Quais são os padrões técnicos mínimos

exigidos pela LGPD?'. Embora o Poder Público não esteja sujeito às sanções pecuniárias, as principais falhas encontradas na Europa são um ótimo referencial para minimizar a probabilidade de ocorrência de incidentes de segurança, especialmente envolvendo dados pessoais.

É fundamental que todos busquem um comportamento digital cada vez mais seguro, de forma que os direitos dos titulares de dados pessoais sejam sempre respeitados.