Borges e Schwertner: Cautelas no tratamento de dados

22/03/2022

Em setembro de 2020, entrou em vigor a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados, que trata sobre a proteção de dados pessoais no país. A LGPD vem na esteira de outras legislações ao redor do mundo que tratam sobre dados pessoais, tema em discussão desde a década de 70 que ganhou força com a Diretiva 95/46 e com a GDPR, o regulamento de proteção da dados Europeu promulgado em 2016.

No Brasil, a discussão sobre a proteção de dados tomou força em 2018 com a promulgação da lei. Após duas prorrogações em seu prazo de vigência com as medidas provisórias 869/2018 e 959/2020, finalmente, em 2020, a lei começou a surtir seus efeitos, trazendo evolução no tema sobre proteção de dados, o que culminou na Emenda Constitucional nº 115/2022, elevando o direito à proteção de dados pessoais à categoria de direito fundamental, incluso no artigo 5º, inciso LXXIX da Constituição.

Na legislação, encontramos definições que anteriormente não eram tão conhecidas pelo público, como a definição de titular de dados pessoais, que se resume em toda pessoa física (natural) que possua dados pessoais (artigo 5º,V), o próprio dado pessoal, como toda informação de pessoa natural identificada ou identificável (artigo 5º, I), tratamento de dados pessoais que é toda operação realizada com dados pessoais em meio físico ou digital (artigo 5º, X) e os agentes de tratamento, que são controlador e operador, pessoas físicas ou jurídicas que realizarão o tratamento de dados pessoais.

Todos esses elementos e muitos outros, fazem parte das atividades diárias de operação com dados (tratamento de dados), que por sua vez move a máquina tanto privada quanto estatal ao redor do mundo. Afinal, quase todas as atividades de qualquer setor ou categoria tratam dados pessoais. Uma empresa, ou, até mesmo a Administração Pública, mesmo que não realize uma atividade que atenda diretamente ao público, ao ter em seu quadro funcionários ou servidores, trata dados pessoais.

Além das definições importantes para entender o que são dados pessoais, encontramos na legislação também, regras de boas práticas para tratarmos (operarmos) dados pessoais com autorização e segurança, regras estas que ao serem descumpridas podem ensejar a aplicação das duras sanções do artigo 52 da LGPD.

A partir das regras postas na LGPD, compilamos pequenas, porém relevantes cautelas para serem aplicadas nas rotinas diárias de atividades nas quais ocorram tratamento de dados pessoais, cautelas estas aplicáveis tanto a empresas privadas quanto a entidades públicas.

Tais cuidados não esgotam a complexidade de procedimentos e adequações elencadas na Lei nº 13.709/2018 — LGPD, mas são boas práticas que demonstram a boa-fé dos agentes de tratamento em tratar dados com segurança, de acordo com a Lei e minimizam o risco de uso indevido de dados pessoais em posse da Instituição.

Cautelas essenciais

a) Minimização na coleta de dados pessoais

Um dos princípios da LGPD é o da finalidade, segundo o qual o tratamento de dados pessoais somente deverá ser realizado para finalidades legítimas, específicas, explícitas e informadas ao seu titular, sem possibilidade de tratamento posterior de forma incompatível com as finalidades inicialmente informadas.

De forma coerente com este princípio, em todas as situações em que for necessária a coleta de dados pessoais, deve ser analisada a finalidade desta coleta e coletados apenas os dados necessários para que ela seja atendida.

b) Obtenção de consentimento de titular de dados

Em seu artigo 7º, a LGPD traz as hipóteses em que poderá ser realizado o tratamento de dados pessoais.

A Lei apresenta situações que autorizam o tratamento de dados como a proteção da vida ou da incolumidade física do titular ou de terceiros, a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados e a tutela da saúde.

Com exceção das situações que estão expressamente previstas pelo artigo 7º, a regra é que o tratamento de dados somente poderá ser realizado mediante o consentimento do titular.

O consentimento se refere à uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Caso haja dúvida se a situação que você está resolvendo se enquadra nas hipóteses em que a LGPD dispensa o consentimento do titular de dados pessoais, solicite este consentimento mediante documento escrito, o qual deverá ser devidamente arquivado.

c) Utilização de computadores com *login* e senhas individualizados

O acesso a qualquer terminal ou dispositivo eletrônico por colaboradores/servidores ocorrer mediante *login* e senha individuais, sendo expressamente vedado o compartilhamento do *login* e senha com colegas de trabalho.

d) Restrição de acesso aos departamentos
Com finalidade de evitar vazamentos e uso indevido de dados pessoais, restringir o acesso de pessoas externas ou de outros departamentos da Instituição, nos locais onde são tratados maiores volumes de dados pessoais ou dados pessoais sensíveis, como RH, TI, financeiro, sala de armazenamento de servidores (*hardware*).

e) Utilização preferencial de gavetas e armários com chave
Para a guarda de documentos físicos que contenham dados pessoais, recomenda-se a utilização, preferencial, de gavetas e armários com chave.

f) Descarte seguro de documentos
De acordo com a LGPD, o dever de proteção aos dados pessoais vai até o momento da eliminação destes dados. Desta forma, o descarte de documentos deve ocorrer de forma que, após sua inutilização, não seja possível identificar eventuais dados pessoais constantes destes documentos.

O uso de picotadeiras é recomendado, caso disponível nos departamentos. Porém, não havendo este equipamento, a cautela é realizar o corte manual dos documentos.

g) Uso do celular
Com o objetivo de aprimorar a segurança no uso do aparelho celular, em situações em que seja utilizado para fins corporativos ou funcionais, recomenda-se a utilização de senha individual, reconhecimento facial ou biometria.

h) Uso do Whatsapp ou outros aplicativos de mensagens instantâneas
Com o objetivo da aprimorar a segurança no uso do aplicativo Whatssapp (ou outro aplicativo de mensagens instantâneas) em situações em que seja utilizado para fins corporativos ou funcionais, recomenda-se a ativação de verificação em duas etapas para acesso ao aplicativo.

Ainda, recomenda-se evitar o envio de mensagens contendo dados pessoais, mas caso isso seja essencial para o seu trabalho, recomenda-se a exclusão de mensagens contendo tais dados após concluir a demanda.

i) Cautelas para dados sensíveis
A LGPD protege de forma especial uma categoria de dados pessoais a que denomina sensíveis.

Dados sensíveis são aqueles que se referem à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (artigo 5º, inciso II).

No tratamento destes dados, as cautelas quanto o acesso a terceiros devem ser redobrada, ficando o compartilhamento condicionado ao consentimento expresso formalizado por escrito do titular ou responsável legal e embasado em uma finalidade específica.

j) Salvamento de dados pessoais em computador particular
Com o objetivo de prevenir vazamento de dados bem como outros acessos indevidos a dados de pessoais que os colaboradores/servidores tem acesso em razão do trabalho, recomenda-se

evitar que arquivos com dados pessoais sejam salvos em computadores particulares.

Caso seja estritamente necessário para a execução de suas atividades, manter estes dados no equipamento apenas até o término da execução do trabalho promovendo sua eliminação ao final.

k) Cautelas no compartilhamento de dados pessoais
Ao compartilhar dados pessoais, precisamos tomar algumas cautelas como:

— Compartilhar os dados estritamente necessários para a atividade realizada, como por exemplo, ao enviar e-mail no qual seja necessário mencionar dados pessoais, recomenda-se analisar a necessidade do compartilhamento destes dados com o destinatário da mensagem, evitando o compartilhamento de dados não essenciais.

— Autorização para o compartilhamento: ao compartilhar dados pessoais, analisar se o compartilhamento atende à finalidade informada ao titular no momento da coleta.

Podem ser citadas também algumas medidas para o compartilhamento seguro, tais como:

— Evitar compartilhar dados por telefone ou meios que impeçam o controle e comprometimento da parte que receberá os dados em seguir boas práticas de proteção de dados.

— Sempre que possível, antes de compartilhar dados pessoais, verificar o conhecimento do receptor sobre as boas práticas em proteção de dados pessoais

— Havendo trâmite de dados pessoais por e-mail, recomenda-se a eliminação periódica destas mensagens.

— Também, sempre que possível, formalizar regras de boas práticas em proteção de dados de forma documentada, oficial e por mecanismo que possa comprovar a leitura ou aceite do receptor, antes do compartilhamento.

— Evitar também compartilhar dados pessoais em grupos de aplicativos de mensagens instantâneas onde vários destinatários têm acesso.

— O compartilhamento de dados pessoais através de aplicativos de mensagens instantâneas deve ser evitado, porém quando for muito necessário, além de ativar as medidas de segurança do celular, como biometria e verificação em duas etapas, apagar a mensagem assim que seu uso não for mais necessário, evitando vazamento de dados por invasão no aparelho ou mesmo sua perda.

Segurança cibernética nos dispositivos
Assegurar requisitos mínimos de segurança cibernética em todos os dispositivos eletrônicos da Instituição, ou, dispositivos pessoais de colaboradores/servidores usados em serviço (computadores, *notebooks*, *tablets*, celulares, relógios inteligentes), como antivírus, bloqueio de e-mails spam com links suspeitos (*phishing*), bloqueio de anúncios nos navegadores, *firewall*, configuração VPN para acesso remoto, entre outros.

Além de orientar os usuários a não clicarem em links suspeitos, navegar em sites com violação de segurança etc.

Considerações finais

As cautelas e recomendações aqui apresentadas estão respaldados nos diversos princípios que norteiam a LGPD, como a finalidade, autodeterminação informativa, entre outros, que trazem ao titular o empoderamento como verdadeiro "dono" do seu dado pessoal. Conceito que antes da promulgação da legislação não gerava reflexão ao brasileiro, os dados pessoais de terceiros eram vistos como algo que qualquer um poderia ter em sua posse e utilizar como bem entender.

Hoje, caminhamos para um aculturamento sobre a posição do titular, como o centro de decisão dos limites da utilização do seu dado pessoal, por esse motivo, a lei no seu artigo 7º delimitou as hipóteses legais que um dado pessoal pode ser tratado, hipóteses estas aplicadas na esfera privada e no poder público.

Com tantas mudanças de costumes e paradigmas que a Lei nos traz, sua vigência já há quase dois anos e a movimentação da Autoridade Nacional de Proteção de Dados regulamentando os pontos em branco da norma bem como a forma de aplicação das sanções, os entes da esfera pública e da esfera privada precisam construir com urgência uma cultura de proteção de dados com o fim de evitar as sanções da legislação e demandas judiciais sobre o tema.

A eventual demora na implementação de medidas estruturais mais profundas voltadas à adequação à LGPD pelas entidades não impede que os colaboradores que realizam tratamento de dados pessoais adotem cautelas essenciais, como as aqui abordadas, com vistas a minimizar, desde logo, os riscos de responsabilização de ordem civil e administrativa.

Fonte: https://conjur.jumps.com.br/2022-mar-22/borges-schwertner-cautelas-tratamento-dados/