A LGPD e o tratamento de dados dos assistidos pela Defensoria

A pandemia ocasionada pelo surto do Covid-19 forçou os atores do sistema de justiça a reinventarem suas formas de atuação, implantando medidas de teletrabalho e atendimento remoto ao público que necessita da prestação jurisdicional. Na Defensoria Pública o rumo também não foi diferente e a suspensão do atendimento presencial deu espaço a uma eficiente organização de atendimento por meios eletrônicos, com criação de canais de facilitação do contato dos assistidos com os Defensores Públicos.

Essa reorganização urgente da forma de atuação da Defensoria Pública obrigou o administrador da instituição a antecipar uma série de medidas de informatização do atendimento, através da utilização de sistemas informáticos e de tratamento de dados que vinham sendo paulatinamente projetados para maior eficiência dos serviços prestados.

Na realidade institucional não raros são os órgãos de atuação que já se utilizavam de programas e aplicativos privados para controle e gestão de dados, contatos com assistidos, elaboração de petições e outras funcionalidades comuns à área jurídica.

O ponto que se traz a debate nesse breve estudo diz respeito à utilização de programas e aplicativos privados de gestão de dados pelos órgãos e instituições públicas e, neste caso, as Defensorias Públicas, considerando que grande parte dos desenvolvedores de tais programas estão situados no exterior e lá mantêm a infraestrutura. Na mesma linha, a concentração de dados pessoais no âmbito da Defensoria Pública é expressiva e a utilização desses dados para finalidades diversas da assistência jurídica também merece algum tipo de controle e regulamentação.

A Lei n. 13.709/2018, espelhada no modelo europeu de proteção de dados (Regulamento Geral de Proteção de Dados) ainda não entrou completamente em vigor, sendo certo que a maior parte de suas disposições terá vigência a partir de agosto de 2020, inobstante haver projetos de lei propondo a extensão desse prazo para o ano 2021.

O novo diploma procura regular o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Na realidade do mundo atual, o controle de dados é de extrema importância por uma série de razões. As relações jurídicas hoje são permeadas pela troca de dados e na prática já se percebe essa busca de dados em situações básicas (cadastros em sítios eletrônicos, compras em estabelecimentos, fornecimento de descontos mediante realização de cadastros etc.).

As instituições públicas estão alcançadas pelo espectro da lei, na forma do art. 3º da Lei n. 13.709/2018, desde que a coleta (inciso III) e a operação (inciso I) de tratamento de dados seja realizada em território nacional, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, e que esse tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços no território nacional (inciso II).

Isso implica dizer que os dados coletados pela Defensoria Pública estão abrangidos pelo diploma legal visto que: 1 – são colhidos e operados no Brasil; 2 – destinam-se à prestação do serviço de assistência jurídica no território; 3 – o titular dos dados se encontra no território nacional por ocasião da coleta (art. 3º, §1º).

Nesta mesma direção, o art. 7º da Lei n. 13.709/2018 autoriza o tratamento de dados para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Pecou o legislador nesse ponto por não mencionar a utilização de outros métodos adequados de solução de controvérsias, que exijam o adequado tratamento de dados.

Não se pode olvidar que na atividade institucional da Defensoria Pública é comum o emprego da mediação e da conciliação, como forma de solução extrajudicial dos litígios, o que implica também a coleta de dados das partes ainda que não haja um processo judicial.

O conteúdo dos dados coletados também merece detida reflexão. O art. 5º da Lei n. 13.709/2018 traz uma série de definições para o seu conteúdo. Interessam-nos, desta forma, os conceitos de dado pessoal, dado pessoal sensível, banco de dados, titular, controlador, operador e tratamento.

Os dados pessoais correspondem a toda informação relacionada à pessoa natural identificada ou identificável e se tornará sensível quando disser respeito à origem racial ou étnica, convicção religiosa, opinião política, 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.

Os dados qualificativos dos assistidos e outros dados que sejam relevantes para a prestação da assistência jurídica e para a tutela de direitos acaba se inserindo no contexto dos dados pessoais.

Quando colhidos os dados e tratados eles devem ser armazenados em bancos de dados, um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico, nos termos da lei.

É importante compreender também que apesar de o dado ser tratado por uma instituição ou organismo estatal isto não desnatura a sua titularidade que será sempre da pessoa natural a quem eles se referem e que são objeto de tratamento.

Assim, quando um assistido fornecer seus dados à Defensoria Pública para tratamento, ele próprio continuará sendo o titular das informações pessoais. A Defensoria Pública exercerá, por meio de seus órgãos e na forma que estabelecer em regulamento, as funções de controladora (tomada das decisões referentes ao tratamento de dados pessoais) e operadora (realização do tratamento de dados pessoais).

Internamente a Defensoria Pública deverá regulamentar quais órgãos serão responsáveis pela função controladora (criação ou indicação de um órgão especifico para essa função) e pela função operadora (órgãos da ponta encarregados pela recepção dos dados e outros órgãos que façam a gestão para as finalidades institucionais).

A atividade de tratamento propriamente devida deve ser encarada como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Sempre que coletar dados pessoais, a instituição deverá buscar o consentimento do titular, de forma livre, informada e inequívoca, a respeito da concordância do tratamento de seus dados para finalidade determinada.

A criação de um termo de consentimento a ser assinado em conjunto com a declaração de hipossuficiência, onde será colhida a concordância do assistido com o fornecimento de seus dados e a finalidade para qual os dados serão utilizados.

Por fim, até pela natureza da atividade de assistência jurídica, é possível que a Defensoria Pública exerça o uso compartilhado de dados, através da comunicação, difusão, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais com órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Considerando que a lei permite o compartilhamento e a transferência de dados, também é importante, até pela ótica do princípio da Unidade da Defensoria Pública, que todas as instituições adotem padrões de tratamento de dados, de modo a facilitar as operações de transferência.

É muito comum que a Defensoria Pública de um Estado atue em favor de parte que resida em outra unidade federativa ou que haja declínio de atribuição, exigindo-se que as instituições sejam capazes de migrar seus dados entre si para a manutenção do serviço de assistência jurídica.

O Colégio Nacional dos Defensores Públicos Gerais – CONDEGE possui um termo de cooperação assinado por grande parte das Defensorias Públicas que regula a protocolização de petições de outros Estados. Ainda que funcione com diversas falhas e mereça uma profunda reorganização, o sistema de peticionamento integrado implantado pelo CONDEGE também é uma forma de compartilhamento de dados. É por essa razão que o CONDEGE deve ser o órgão que proponha a padronização do controle de dados no âmbito da Defensoria Pública.

O art. 6º da Lei n. 13.709/2018 estabelece a necessidade de ser observar a boa-fé e alguns princípios enumerados em seus incisos. Quando tratar dos dados pessoais, a Defensoria Pública deve realizar essa atividade com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Os dados, conforme a necessidade, devem ser tratados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

A Defensoria Pública deve ser transparente na coleta dos dados, evitando práticas como *phishing* (busca de informações pessoais de forma fraudulenta), indicando quais são os seus meios oficiais para coleta de dados dos assistidos. Na realidade atual é muito comum a utilização de e-mails e mensagens telefônicas solicitando o fornecimento de dados, muitas vezes sob a aparência de bancos e instituições públicas.

Sempre será facultando ao titular, o livre acesso aos dados, mediante consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

O ponto mais importante corresponde a segurança. Torna-se necessário que a Defensoria Pública se utilize de todas as medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, inclusive de forma preventiva.

O tratamento de dados no âmbito da Defensoria Pública não pode ocasionar nenhum tipo de discriminação ou abuso em razão das informações colhidas.

Por fim, a Lei n. 13.709/2018 estabelece como princípios a responsabilização e a prestação de contas, sendo responsabilidade do controlador demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Diante das premissas aqui traçadas, as Defensorias Públicas precisam adequar a sua forma de prestar atendimentos iniciais, organizar os seus sistemas de registro e armazenamento de dados e editar normativas internas para regular o acesso e uso dados no exercício da atividade fim e da atividade meio.

Com a nova forma de atendimento, o assistido deve consentir com o tratamento de seus dados pessoais, inclusive os sensíveis, cabendo à instituição adverti-lo de como aqueles dados serão utilizados e com quais finalidades.

Temos visto que os sistemas de dados de algumas Defensorias Públicas mapeiam a predominância de perfis de atendimento (quantitativo de pessoas atendidas de acordo com idade, gênero, estado civil e outras informações) como forma de reorganizar suas estruturas de atendimento. Estas atividades devem ser comunicadas ao titular dos dados por ocasião do termo de consentimento.

Além disso, as instituições devem implantar sistemas próprios de processamento de bancos de dados, evitando a utilização de programas abertos que estejam situados em outros países, considerando a obrigação prevista em lei para tratamento de dados em território nacional. Assim, a utilização de plataformas como Google, Evernote etc. podem não se adequar aos comandos da lei nesse ponto e acarretar a responsabilidade da Defensoria Pública caso haja uso indevido.

Um outro aspecto importante, talvez o mais crítico no âmbito da Defensoria Pública, diz respeito ao controle de acesso e utilização de dados. A mão de obra da Defensoria Pública não se resume apenas aos seus membros, também contando com servidores do quadro de apoio, estagiários, residentes e colaboradores voluntários.

É obrigação da instituição garantir a segurança no acesso aos dados, de modo a evitar que haja captação indevida, utilização diversa da finalidade prevista pelos operadores da instituição. Há que se tratar uma normativa clara e um controle de acesso dos dados pelos operadores da instituição, de modo que se possa identificar quem faz o uso indevido, de modo a aplicar o sancionamento correspondente.

Muitas outras adaptações se tornam também necessárias para regular internamente o tema, sendo certo que a vigência da lei já se aproxima.

Date Created
31/03/2020