



## Matheus Rodrigues: Primeiras impressões sobre o uso da LGPD

Recentemente sancionada, a Lei Geral de Proteção de Dados (LGPD ou Lei nº 13.709/2018) já é utilizada como fundamento em algumas petições. Entre essas, consta a Ação Civil Pública nº 0730600-90/2020-8-07-0001, ajuizada pelo Ministério Público do Distrito Federal e Territórios (MPDFT), na qual se manifesta o *Parquet*.



Em resumo, na ACP, o MPDFT soube da comercialização de

dados pessoais em determinado website. Entre os dados disponíveis, segmentados por ramo de atuação profissional, estavam nome, contato para SMS, endereços eletrônico e postal, bairro, cidade, Estado e CEP. Ressalte-se, ademais, que os dados abrangiam indivíduos residentes em diversos Estados da federação. Pelo exposto, e com base, entre outros, no artigo 42, *caput*, e §3º, LGPD, o MPDFT requereu antecipação dos efeitos da tutela para determinar à demandada que se abstinhasse de vender dados pessoais tratados de forma irregular.

O juízo, porém, extinguiu a ação, sem exame do mérito, por indeferimento da inicial. Alegou ausência de interesse processual, manifesto na falta de utilidade e necessidade do processo. Isso porque o website encontrava-se indisponível, o que, para o magistrado, poderia indicar um processo de adequação à Lei nº 13.709/2018. Em manifestação, o MPDFT alegou que o site ainda encontrava-se em funcionamento no dia da prolação da sentença e que a base de dados continuava intacta e disponível.

Em outro caso, foi noticiado, em Pernambuco, o ajuizamento de uma ação, também fundamentada na LGPD, na qual um usuário do sistema de transporte público, diante da necessidade de cadastramento biométrico facial para recarga do bilhete eletrônico, indagou acerca da Política de Privacidade e Proteção de Dados Pessoais da transportadora.

Diante da negativa em apresentar esse documento, o usuário não consentiu com a coleta da biometria, o que impediu o uso do sistema de transporte público. Assim, o demandante ajuizou ação requerendo antecipação dos efeitos da tutela para determinar a atualização do cadastro sem o uso de biometria.



De início, veja-se que a indisponibilidade do site não indica o início de um projeto de conformidade, o qual, utilizando-se parâmetros otimistas, tem duração média de três meses [1]. Provas mais robustas de um projeto de adequação seriam uma comunicação da diretoria da empresa informando o início de um projeto de *compliance* à LGPD; a apresentação de uma política de segurança da informação, as diretrizes para um mapeamento de dados (*data mapping*, em inglês); ou a formação de um comitê interno de *compliance*. Veja-se, ademais, que a todos esses dados deve-se impor segredo de Justiça, porquanto podem trazer informações essenciais ao funcionamento da própria empresa.

Por outro lado, veja-se estar presente o risco de novas violações à privacidade dos cidadãos cujos dados ainda estão à venda no website. Isso porque a comercialização de dados pessoais é o negócio da demandada e ela encontra-se na posse do principal insumo de sua operação, qual seja, as bases de dados. A transformação dos dados em ativo na atual economia da informação, por sua vez, encontra respaldo em Bioni (2018, p. 38 e seguintes [2]), no qual é descrito o uso dos dados dos cidadãos para direcionar, por exemplo, campanhas de marketing, além da transformação do consumidor em produto.

Face ao perigo de novas violações a um direito protegido não apenas na Lei nº 13.709/2018, mas também no artigo 5º, X, da Constituição Federal de 1988 [3], qual seja, a inviolabilidade da intimidade e da vida privada, caberia uma tutela inibitória para fazer cessar as atividades comerciais da ré nesse setor.

Por outra, veja-se que também foi violado o princípio da autodeterminação informativa, previsto no artigo 2º, II, LGPD (BRASIL, 2018 [4]). Esse princípio, por sua vez, foi definido pelo Tribunal Constitucional Federal alemão como a autoridade dada ao indivíduo de decidir sobre a divulgação e o uso de seus dados pessoais, não devendo haver qualquer atividade de processamento sem seu consentimento (ALEMANHA, 1983 [5]). Logo, se há uma operação com dados pessoais (no caso, a venda deles), o titular do dado tem direito a decidir acerca do destino de suas informações e a eventual cessação dessa operação.

Ademais, ao fixar a autodeterminação informativa como fundamento da proteção de dados pessoais, o Estado brasileiro reiterou a posição contida no artigo 1º, *caput*, LGPD, de privilegiar a tutela dos direitos do cidadão. Com essa escolha política, conforme Danilo Doneda [6], o consentimento passou a ser o meio pelo qual a autodeterminação informativa é exercida e, por conseguinte, a autonomia do indivíduo é manifesta. Logo, sem o consentimento do indivíduo para qualquer operação com seus dados, a operação em si mostra-se ilegal.

Em relação à ação ajuizada em Recife, veja-se que a biometria é considerada dado pessoal sensível, segundo o artigo 5º, II, da LGPD. Outrossim, dados sensíveis podem, conforme o artigo 11, II, "b", Lei nº 13.709/2018, ser tratados, sem consentimento do titular, para execução, pela Administração, de políticas públicas.

Contudo, veja-se que, mesmo sem o consentimento do titular, o Estado e, no caso, as concessionárias de serviços públicos devem estar em conformidade com a LGPD. Isso porque o artigo 6º, IV e VI, da Lei nº 13.709/2018 estabelece que qualquer atividade de tratamento de dados deve se pautar no livre acesso e na transparência, que efetivam, entre outros, o direito ao conhecimento da forma e duração do tratamento de dados.



No caso recifense, a empresa de transporte público não soube informar a forma de tratamento de dados pessoais e as medidas de segurança adotadas para proteger os dados obtidos. Nesse contexto, descumpriu os princípios da transparência e livre acesso acima referenciados e, com isso, sua operação de tratamento tornou-se ilegal.

Observe-se, por fim, que não se defende a impossibilidade de tratar dados pessoais sensíveis, mas que essa operação ocorra com demonstração do fluxo dos dados dentro da empresa (*data flow diagram*, em inglês), verificável pelos órgãos públicos de controle, além de fundamentação legal em alguma alínea do artigo 11, II, LGPD. Uma delas poderia ser a própria alínea "b", que admite o tratamento compartilhado em caso de execução de políticas públicas previstas em lei. No caso, como o transporte público é um direito social, nos termos do artigo 6º, *caput*, da Constituição Federal de 1988, compete ao poder público prevenir tentativas de fraude no uso dos instrumentos de acesso aos meios de transporte público.

Outro embasamento legal, mais atinente à concessionária, seria o artigo 11, II, "d", LGPD, qual seja, exercício regular de direitos, inclusive em contrato. No caso, ao ganhar a concessão, a empresa compromete-se a zelar pela segurança na prestação do serviço (artigo 6º, § 1º, Lei 8.987/95 [7]). A prevenção de fraudes no uso do passe eletrônico, por sua vez, enquadra-se no dever de zelar pela segurança, o que justifica a incidência da alínea "d" da Lei nº 13.709/2018.

Veja-se, entretanto, que a segurança, por ser um direito do cidadão, deve ser demonstrada, razão pela qual não pode a empresa prescindir da elaboração de uma política de segurança da informação, da comunicação da forma de coleta dos dados, quais informações são obtidas dos usuários do serviço, entre outros.

Ao final, observa-se ainda ser necessário aumentar o grau de conscientização do Judiciário acerca da aplicação da LGPD para que se evite extinguir processos sem exame do mérito e, assim, não formar jurisprudência acerca da aplicação da Lei nº 13.709/2018. Por outro lado, observa-se que as empresas necessitam iniciar projetos de conformidade, sob pena de serem cada vez mais demandadas na Justiça e, inclusive, perderem contratos com o poder público.

[1] Calculadora disponível em: <<https://advisera.com/eugdpracademy/eu-gdpr-compliance-duration-calculator/>>. Parâmetros: um a 20 funcionários; a empresa não processa dados sensíveis; atua principalmente como controladora; não utiliza ferramentas de *profiling* ou decisões automatizadas; utiliza operadores terceirizados (por exemplo, *call-center*); aplica normativas de segurança de dados (cite-se, a ISO 27001); terá um consultor com conhecimento em proteção de dados para todo o projeto; tem apoio da direção da empresa; e dispõe de um funcionário com experiência em gerenciamento de projetos para auxiliar o projeto de conformidade.

[2] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.



[3] BRASIL. Constituição da República Federativa do Brasil de 1988, de 5 de outubro de 1988. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm)>. Acesso em: 22 set. 2020.

[4] Lei 13.709, de 14 de agosto de 2018. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)>. Acesso em: 22 set. 2020.

[5] ALEMANHA. Bundesverfassungsgericht (Erste Senat). Julgamento conjunto nº 65 das Reclamações Constitucionais nº 209/83, 269/83, 362/83, 420/83, 440/83, 484/83. Data de julgamento: 15 dez. 1983. Disponível em: <[https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215\\_1bvr0209](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr0209)>. Acesso em: 22 set. 2020.

[6] DONEDA, Danilo César Maganhoto. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters, 2020. Livro eletrônico (sem páginas).

[7] BRASIL. Lei nº 8.987, 13 de fevereiro de 1995. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/L8987compilada.htm](http://www.planalto.gov.br/ccivil_03/leis/L8987compilada.htm)>. Acesso em: 22 set. 2020.

**Date Created**

27/09/2020