

Daniela Cravo: Sobre pedidos abusivos pelo titular dos dados

A Lei Geral de Proteção de Dados Pessoais (LGPD) trouxe um catálogo específico de direitos ao titular dos dados no seu terceiro capítulo. Cabe, todavia, a reflexão quanto ao modo e à forma de exercício desses direitos e seus próprios limites para fins de que não haja um ônus desproporcional e não razoável



A respeito, indaga-se: será que pode haver limitações ao

exercício de certos direitos, para fins de evitar o desenvolvimento da figura do peticionante contumaz em matéria de LGPD? O controlador poderá recusar pedidos que sejam infundados e excessivos?

A resposta é positiva, já que nos próprios termos do artigo 187 do Código Civil também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. Afastando-se do antigo abuso do direito francês, esse artigo, por representar uma ilicitude civil objetiva, dispensando o dano e a culpa, serve muito bem para tutelar questões complexas, como as trazidas pelo exercício dos direitos previstos na LGPD.

A dúvida reside, todavia, no que consiste exceder manifestamente os limites impostos no que toca aos direitos da LGPD. E, para melhor elucidar a questão, parte-se dos precedentes já consolidados em tema de acesso à informação na Administração Pública, que podem servir de analogia aos direitos da LGPD e, em especial, ao direito de acesso [\[1\]](#), pelas suas semelhanças.

No âmbito da Controladoria-Geral da União (CGU), há uma série de precedentes que reconhecem a figura do solicitante frequente e, em certos casos, o abuso do direito de acesso a informações. No Processo nº 08850.000645/2017-08, há o relato de um peticionante que já apresentou, pelo sistema e-SIC, 1.760 pedidos de acesso a informação perante órgãos e entidades do Poder Executivo federal [\[2\]](#).

Segundo o parecer constante no mencionado processo [\[3\]](#), pedidos desproporcionais ou desarrazoados podem vir a configurar abuso do direito. Por pedidos desarrazoados, citam-se os seguintes exemplos: pedidos desrespeitosos (quando redigidos em tons ofensivos, depreciativos ou até mesmo direcionados a servidores identificados), pedidos obsessivos, que buscam prejudicar/sobrecarregar as atividades da instituição, ou pedidos frívolos, cujo único objetivo é expor a entidade ao ridículo.



Já com relação aos pedidos desproporcionais, *"a CGU tem enfatizado bastante o aspecto quantitativo desse instituto, avaliando a relação entre fins e meios para se disponibilizar determinada informação"* [4], havendo proporcionalidade quando harmônico os esforços do Estado para se disponibilizar determinada informação.

Claro que nem todo pedido desarrazoado ou desproporcional é um abuso do direito. Para configuração deste, no nosso entender, é importante que o exercício exceda os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes, de acordo com o artigo 187 do Código Civil.

Alguns casos em que reconhecido o abuso no direito de acesso à informação são os seguintes: cidadão que faz pedidos recorrentes sobre os mesmos fatos; pedido de informações para usos proibidos por lei; uso da via recursal sem impugnação específica da decisão recorrida; elevado número de pedidos desarrazoados; solicitação de informação que o solicitante comprovadamente já possui [5].

Transplantando tal inteligência para os direitos da LGPD, é possível afirmar que pedidos desarrazoados ou desproporcionais pelo titular dos dados, caso estejam em desacordo com o fim econômico ou social, com a boa-fé ou com os bons costumes, podem ser considerados abusivos e, por isso, serem recusados.

A título exemplificativo, citam-se as seguintes hipóteses de condutas que podem ser consideradas abusivas: pedidos extremamente detalhados sobre as operações de tratamento de dados sem que haja finalidade ou utilidade nesse pedido, tendo em vista a possibilidade do controle da legitimidade do tratamento por meio de informações já prestadas, pedidos reiterados de informações já prestadas, pedidos de acesso frequentes, mensais ou semanais, sem o transcurso de um intervalo razoável.

Nem sempre tais pedidos violam a boa-fé objetiva. Poderão, todavia, ser considerados abusivos quando desvirtuado o fim econômico ou social, especialmente quando onerem de uma forma não proporcional o agente de tratamento (como nos pedidos reiterados ou muito detalhados). Da mesma forma, pedidos que contém ofensas, acusações ou xingamentos podem eventualmente ser considerados abusivos por estarem em desacordo com os bons costumes.

Assim, pedidos abusivos, à luz das normas da LGPD e do artigo 187 do Código Civil, são aqueles que estão em desacordo com o fim econômico ou social, com a boa-fé ou com os bons costumes, conforme exemplos trazidos acima. Apesar dessa possibilidade de recusa de atendimento à requisição do titular dos dados quando abusiva, a análise pelo controlador deve ser feita sempre caso a caso, não podendo haver uma política geral de recusas. Ademais, a recusa deve ser sempre motivada e transparente, para que seja possível o controle pelo titular, pela Autoridade Nacional de Proteção de Dados (ANPD) e por outros agentes legitimados.

Desta feita, o controlador deverá, com base no artigo 18, §4º, inciso II, indicar as razões de fato e de direito para recusa da requisição. Tal recusa, todavia, não impede que o titular busque a ANPD, os órgãos de defesa do consumidor ou até mesmo peticione em juízo para fins de impugnar a recusa do controlador quando entender que essa não foi legítima, nos moldes previstos nos artigos 18, §1º e §8º, e 22 da LGPD.



A propósito, a ICO [6] possui orientações sobre pedidos de titulares que sejam manifestamente infundados ou excessivos, aduzindo que a análise pelo controlador deve ser sempre feita caso a caso. Segundo a autoridade, uma solicitação pode ser manifestamente infundada se o indivíduo não tiver uma intenção clara de acessar as informações ou for mal-intencionada, quando a solicitação tem a única finalidade de causar perturbação para a organização, sem nenhum outro propósito real.

Como exemplo de pedidos manifestamente infundados, a ICO [7] cita o seguinte: pedidos que tenham alvo um determinado funcionário por rancor pessoal, solicitações sistemáticas ou frequentes como uma campanha para causar interrupção das atividades, pedido de correção de informações quando não há correções a serem feitas, entre outras. Já os pedidos excessivos para a ICO [8] podem ser vislumbrados quando há uma repetição do conteúdo das solicitações anteriores sem ter decorrido um intervalo razoável de tempo, ou quando um pedido sobrepõe-se a outros pedidos. Cabe a ressalva que o enquadramento de um pedido como infundado ou excessivo sempre dependerá das circunstâncias de cada caso concreto.

Caso judicial interessante sobre essa temática foi o *Lees v Lloyds Bank Plc [2020] EWHC 2249 (Ch)* [9], julgado em julho de 2020. O requerente fez uma reclamação em face de Lloyds Bank Plc alegando que esse não teria dado uma resposta adequada aos seus pedidos de acesso em violação à Lei de Proteção de Dados 2018 e ao Regulamento Geral de Proteção de Dados.

Ao analisar o caso, a corte concluiu que Lloyds tinha respondido adequadamente a todos os pedidos do reclamante à luz dos seguintes motivos [10]: 1) as requisições de acesso aos dados do titular foram numerosas e repetitivas; 2) o objetivo final das requisições de acesso aos dados não versavam sobre o controle dos dados pelo titular, mas, sim, obtenção de documentos para uso em processos contra o banco. Por tal razão, as requisições de acesso aos dados eram abusivas; 3) os dados solicitados não trariam nenhum benefício real para o requerente; entre outros.

Com base nos argumentos expostos acima, a reclamação foi rejeitada. Conforme consignou a corte, a reclamação do titular dos dados era totalmente desprovida de mérito [11].

A respeito de pedidos frequentes que podem inviabilizar as atividades do controlador ou gerar custos muito altos a suas atividades, cita-se a limitação feita na legislação da Califórnia sobre privacidade dos consumidores, *California Consumer Privacy Act* (CCPA), que prevê que a empresa deve fornecer informações pessoais a um consumidor a qualquer momento, mas não será obrigada a fornecer informações pessoais a um consumidor mais de duas vezes em um período de 12 meses [12]. Na Proposta 24, conhecida como *California Privacy Rights Act of 2020* (CPRA), que traz modificações à CCPA, também há a mesma limitação na seção 1798.130, (7), (B), que determina que uma empresa não é obrigada a fornecer as informações exigidas pelas seções 1798.110 e 1798.115 ao mesmo consumidor mais de duas vezes em um período de 12 meses.



Tal limitação temporal do exercício dos direitos pelo titular pode servir de modelo ou inspiração para o Brasil [13]. Considerando a proposta de regulamentação dos direitos dos titulares pela ANPD [14], que consta na Fase 3 da agenda regulatória, e que a LGPD estabeleceu no §5º do artigo 18 que os requerimentos para exercício dos direitos pelo titular serão atendidos nos prazos e nos termos previstos em regulamento, a ANPD poderá, eventualmente, dispor nos instrumentos normativos que pretende elaborar sobre eventuais limites ou restrições temporais.

Por fim, cabe destacar que os direitos dos titulares são uma conquista que consagram uma grande evolução na promoção da autodeterminação informativa. Por isso, qualquer recusa precisa sempre ser muito bem justificada à luz de cada caso concreto, e apenas quando presente algum excesso com base nos limites impostos pela boa-fé, pelo fim econômico ou social ou pelos bons costumes.

[1] O foco no direito de acesso da LGPD justifica-se por ser esse o direito cujo exercício é condição prévia para o exercício dos demais direitos. Perceba-se que para ser factível o pedido de eliminação, retificação, anonimização, entre outros, é quase indispensável receber antes a resposta ao direito de acesso. Em razão disso, é muito provável que o direito de acesso venha a ser o direito mais exercido pelos titulares à luz da LGPD e o que mais seja passível de eventuais abusos no seu exercício.

[2] BRASIL. CGU. Processo n.º 08850.000645/2017-08. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/08850000645201708_CGU.pdf. Acesso em 28 de agosto de 2021.

[3] BRASIL. CGU. Processo n.º 08850.000645/2017-08. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/08850000645201708_CGU.pdf. Acesso em 28 de agosto de 2021.

[4] BRASIL. CGU. Processo n.º 08850.000645/2017-08. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/08850000645201708_CGU.pdf. Acesso em 28 de agosto de 2021.

[5] BRASIL. CGU. Processo n.º 08850.000645/2017-08. Disponível em: http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/08850000645201708_CGU.pdf. Acesso em 28 de agosto de 2021.

[6] ICO. *Manifestly unfounded and excessive requests*. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>. Acesso em 28 de agosto de 2021.



[7] ICO. *Manifestly unfounded and excessive requests*. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>. Acesso em 28 de agosto de 2021.

[8] ICO. *Manifestly unfounded and excessive requests*. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>. Acesso em 28 de agosto de 2021.

[9] HIGH COURT OF JUSTICE BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES PROPERTY TRUSTS AND PROBATE LIST. *Lees v Lloyds Bank Plc* [2020] EWHC 2249 (Ch), 2020.

[10] HIGH COURT OF JUSTICE BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES PROPERTY TRUSTS AND PROBATE LIST. *Lees v Lloyds Bank Plc* [2020] EWHC 2249 (Ch), 2020.

[11] HIGH COURT OF JUSTICE BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES PROPERTY TRUSTS AND PROBATE LIST. *Lees v Lloyds Bank Plc* [2020] EWHC 2249 (Ch), 2020.

[12] Cabe destacar, no entanto, que tal redação será substituída em 1º de janeiro de 2023 pela redação trazida pela Proposta 24 – California Privacy Rights Act of 2020 (CPRA). CALIFORNIA LEGISLATIVE INFORMATION. Disponível em:

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.100. Acesso em 29 de agosto de 2021.

[13] Veja que tal limitação pode ser uma forma de reduzir os custos do *compliance* de certos direitos, como o da portabilidade. Inclusive, poderia ser uma alternativa para evitar uma dispensa geral da portabilidade de dados pessoais para agentes de tratamento de pequeno porte, como constou na proposta normativa da ANPD, em consulta pública recentemente.

[14] ANPD. Portaria n.º 11, de 27 de janeiro de 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Disponível em 30 de agosto de 2021.

Meta Fields