Opinião: Os desafios do background check frente à LGPD

A Lei Geral de Proteção de Dados (LGPD), inspirada no Regulamento Geral sobre a Proteção de Dados europeu, traz aos agentes de tratamento inúmeras obrigações com o objetivo de proteger os dados do titular da lei.

Entre essas obrigações, uma delas consiste em prover a segurança da informação compatível e necessária para o atendimento das medidas determinadas no artigo 46, quais sejam, medidas de segurança, técnicas e administrativas que se demonstrem aptas para a proteção de dados em que estejam envolvidos o controlador e ou operador [1]. Nessa mesma linha, o artigo 44 também define como irregular aquele tratamento que, além de não observar a lei, não forneça a segurança que o titular espera [2].

O Regulamento Geral sobre a Proteção de Dados (RGPD), ao tratar dos princípios relativos ao tratamento de dados pessoais, em seu artigo 5º, dispõe que os dados pessoais devem ser tratados com segurança, impondo aos agentes de tratamento a adoção de medidas técnicas e organizativas adequadas para o atingimento dessa finalidade [3]. Deve, ainda, o responsável ser capaz de comprovar o atendimento dessa responsabilidade, cumprindo com denominado princípio da *accontability*, que significa não ser suficiente agir em conformidade com a lei, sendo também necessário fazer a prova desse bem agir.

E, nessa lógica de garantir a proteção dos dados dos titulares, é necessário prevermos o fator humano, o qual representa um dos principais componentes para o sucesso ou fracasso da segurança da informação. Portanto, torna-se imprescindível que as empresas conheçam melhor os seus funcionários, os seus parceiros de negócios, os seus históricos comprovados, de forma que seja viável aferir um certo grau de confiabilidade e integridade no desempenho de suas funções.

Ao agir de forma cautelosa, estaria o agente de tratamento cumprindo com os princípios da Lei Geral de Proteção de Dados, ou seja, os da segurança, da prevenção e da prestação de contas. Ocorre que o *background check*, conhecido como uma forma de recolha de dados em rede aberta, ou seja, aqueles dados tornados públicos pelo próprio titular, nos moldes do artigo 7, IV, da Lei Geral de Proteção de Dados, para fins de investigação e verificação de antecedentes passa a requerer limites sob pena de estarmos infringindo a própria lei [4].

As informações que decorrem desse processo, seja na esfera criminal, na financeira e na profissional, entre outras, são processadas para diferentes finalidades, tais como, processo seletivo para contratação de funcionários de uma organização, avaliação de parceiros comerciais e checagem e validação de documentação para coibir fraudes, entre outras.

E, tanto no cenário internacional como no nacional, após a vigência do Regulamento Geral sobre a Proteção de Dados europeu (GDPR) [5] — e a Lei Geral de Proteção de Dados (LGPD) [6] —, tornou-se imperioso adequar qualquer tratamento de dados para que a referida lei seja observada na íntegra, surgindo nessa esteira alguns desafios na implementação da atividade de *background check*, os quais, de forma meramente ilustrativas, trazemos à tona, sem a pretensão de exaurirmos o panorama que se apresenta no dia a dia das empresas.

Inicialmente, cabe destacar que qualquer tratamento de dados, para que seja considerado lícito, precisa respeitar os princípios elencados no artigo 6º, bem como requer seja a sua finalidade autorizada por alguma das hipóteses do artigo 7º da Lei de Proteção de Dados [7]. Significa dizer então que, inobstante a natureza pública dos dados pessoais, o seu processamento impõe a compatibilização com a lei. Nesse contexto, a limitação para o tratamento de dados públicos é encontrada no próprio texto. O §3º dispõe que tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização [8]. Portanto, no caso concreto, é indispensável a análise desses requisitos.

Olhando para a União Europeia, encontramos algumas orientações no Parecer 2/2017 sobre o processamento de dados no trabalho, adotado pelo Grupo de Trabalho de Proteção de Dados do artigo 29, o qual ressalta os limites na utilização dos dados públicos, estando condicionados para fins de conformidade com a lei à necessidade e ao interesse do empregador no recebimento das informações, bem como à expectativa do titular no tratamento dos seus dados [9].

O princípio da transparência, tão caro às leis protetivas dos dados pessoais, jamais deve ser desprezado, visto que não basta que o tratamento se enquadre em uma das bases legais do artigo 7º ou 11º da LGPD [10]. É imprescindível que o titular tenha conhecimento de que os seus dados serão utilizados e para qual finalidade. Importante destacar que não se confunde o conhecimento com o consentimento, pois este último, em se tratando de dados públicos, restou dispensado por força do artigo 7º, IV.

Ainda convêm lembrar que existem situações que envolvem processamento de dados para investigações corporativas internas e também para o cumprimento de obrigação legal ou regulatória do controlador com o objetivo de investigação de infrações éticas e atos ilegais, representando esse tratamento não somente um interesse legítimo do controlador em detectar e interromper condutas ilegais, como também um dever de *compliance*.

Considerando a notável influência do Regulamento Europeu sobre a Lei Geral de Proteção de Dados, oportuno buscarmos subsídios no Considerando 47 do Regulamento Europeu [11], o qual dispõe expressamente que o processamento de dados pessoais para fins de prevenção e controle da fraude constitui um interesse legítimo do responsável pelo seu tratamento, desde que sejam estes estritamente necessários.

Conclui-se, dessa feita, que as atividades de *background check* e investigações corporativas são perfeitamente lícitas e muitas vezes necessárias por parte dos agentes de tratamento, inclusive para o cumprimento das obrigações impostas pela própria legislação de proteção de dados, na medida em que imputam ao controlador e operador a responsabilidade em prover medidas técnicas e organizacionais para prover a segurança dos dados dos titulares. Isso sem mencionarmos as exigências decorrentes de obrigações legais e regulatórias, a depender do setor que justificam e autorizam o tratamento.

Entretanto, estas atividades demandam especial cuidado na observância dos princípios do artigo 6º, em especial aos princípios da necessidade, da transparência, da prevenção e segurança e da existência de uma finalidade legítima, sob pena de violarem os fundamentos do artigo 2º da Lei de Proteção de Dados, em especial o respeito à privacidade, à dignidade e ao livre desenvolvimento da personalidade [12].

Em sendo a LGPD uma lei contextual [13], cada vez mais evidencia-se a importância de uma análise aprofundada ao caso concreto e do devido balanceamento dos direitos e das obrigações.

Referências bibliográficas

BRASIL. Presidência da República. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 21 set. 2021.

GENERAL DATA PROTECTION REGULATION – GPDR. [Site institucional]. Disponível em: https://gdpr-info.eu/. Acesso em: 21 set. 2021.

[1] BRASIL. Presidência da República. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 21 set. 2021.

[2] *Ibidem.*

[3] GENERAL DATA PROTECTION REGULATION – GPDR. [Site institucional]. Disponível em: https://gdpr-info.eu/. Acesso em: 21 set. 2021.

[4] BRASIL. Presidência da República. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 21 set. 2021.

[5] GENERAL DATA PROTECTION REGULATION – GPDR. [Site institucional]. Disponível em: https://gdpr-info.eu/. Acesso em: 21 set. 2021.

[6] BRASIL, *loc. cit.*

[7] BRASIL, *loc. cit.*

[8] BRASIL. Presidência da República. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 21 set. 2021.

[9] GENERAL DATA PROTECTION REGULATION – GPDR. [Site institucional]. Disponível em: https://gdpr-info.eu/. Acesso em: 21 set. 2021.

[10] BRASIL, *loc. cit.*

[11] GPDR, *loc. cit.*

[12] BRASIL. Presidência da República. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 21 set. 2021.

[13] *Ibidem.*

Date Created
29/09/2021