DOI 10.5433/21788189.2022v26n2p103

DATA MAPPING: ADEQUAÇÃO DE ESCRITÓRIOS DE CONTABILIDADE À LEI GERAL DE PROTEÇÃO DE DADOS

DATA MAPPING: ADEQUACY OF ACCOUNTING OFFICES TO THE GENERAL DATA PROTECTION LAW

Rennan Herbert Mustafá*
Fábio Fernandes Neves Benfatti**

Como citar: MUSTAFÁ, Rennan Herbert; BENFATTI, Fábio Fernandes Neves. Data mapping: adequação de escritórios de contabilidade à lei geral de proteção de dados. **Scientia Iuris**, Londrina, v. 26, n. 2, p. 103-116, jul. 2022. DOI 10.5433/21788189.2022v26n2p103. ISSN: 2178-8189.

*Mestrando em Direito Negocial e Pós-graduado em Direito do Estado com ênfase em Direito Tributário, ambos pela Universidade Estadual de Londrina. Pós-graduado em Contabilidade Fiscal e Tributária pela Faculdade Paranaense. Professor na Faculdade Paranaense. Contador.
E-mail: rennan.h.mustafa@gmail.com

**Doutor em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Graduação em Direito e Mestrado em Direito Negocial, ambos pela Universidade Estadual de Londrina. Pós-Doutorado pela Università degli Studi di Messina, UNIME, Itália.
E-mail: benfatti@prof.faccar.com.br

Resumo: A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) foi elaborada com a finalidade de salvaguardar os dados pessoais de pessoas naturais, estabelecendo normas de conduta que devem ser observadas na realização de atividades empresariais de tratamento de dados. Sabe-se que o tratamento de dados pessoais é inerente ao desenvolvimento da atividade contábil, da abertura de uma empresa ao fechamento da folha de pagamentos. Desse modo, é de suma importância que os escritórios de contabilidade se adaptem às novas políticas de proteção de dados. Diante disso, o presente trabalho objetiva demonstrar de que forma os escritórios de contabilidade podem se adequar à Lei Geral de Proteção de Dados a partir da averiguação do inventário de dados (*data mapping*). Para isso, utilizar-se-á do método dedutivo e de pesquisa bibliográfica. Ao final, conclui-se que para uma efetiva aplicação de políticas de proteção de dados, é imprescindível a realização do *data mapping*.

Palavras-chave: empresas; inventário de dados; Lei n. 13.709/2018.

Abstract: The General Data Protection Law (Law No. 13,709 / 2018) was implemented with the purpose of safeguarding the personal data of natural persons, establishing rules of conduct that must be observed when carrying out business data processing activities. It is known that the processing of personal data is inherent to the development of accounting activity, from opening a company to closing the payroll. As such, it is of paramount importance that accounting firms adapt to new data protection policies. In light of this, the present study aims to demonstrate

how accounting offices can adapt to the General Data Protection Law from the investigation of data inventory (data mapping). For this, the deductive method and bibliographic research will be used. It will be concluded that for the effective application of data protection policies, data mapping is essential.

Key-words: Companies. Data inventory. Law n. 13.709/2018.

INTRODUÇÃO

A promulgação da Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/2018) (BRASIL, 2018a) tem como objetivo a defesa dos direitos fundamentais de liberdade e de privacidade e do livre desenvolvimento da personalidade da pessoa natural em face do tratamento[1] indevido de seus dados pessoais[2] , equacionando os direitos do titular com o desenvolvimento econômico, tecnológico e de inovação, estabelecendo diretrizes a serem observadas pelos agentes econômicos.

Trata-se de um anseio internacional para a criação de políticas específicas sobre a proteção de dados pessoais em decorrência dos efeitos da globalização, em especial, do desenvolvimento do comércio internacional e do avanço tecnológico, que impulsionaram um grande crescimento na coleta e no compartilhamento de dados[3], inclusive internacionalmente.

Na era da informação, o acesso a dados pessoais constitui uma importante fonte de poder político e econômico, possibilitando que os agentes possuam informações sobre os titulares dos dados e direcionem suas ações políticas e comerciais. Ademais, na economia digital, o banco de dados pessoais pode representar um intangível extremamente valioso.

Nesse contexto, com inspiração na legislação europeia de proteção de dados pessoais, *General Data Protection Regulation*, o Brasil promulgou, em 2018, a Lei Geral de Proteção de Dados, prevendo, também, a criação da Autoridade Nacional de Proteção de Dados, visando garantir maior efetividade às novas diretrizes implementadas.

Essas novas políticas impactam na atuação das empresas, inclusive as contábeis, que deverão se adequar às normas de conduta impostas pela Lei n. 13.709/2018, sob penas administrativas que variam de uma simples advertência a multas que podem chegar ao montante de R$ 50.000.000,00 (cinquenta milhões de reais).

Apesar de o artigo 65 da Lei Geral de Proteção de Dados (BRASIL, 2018a) prever, quanto aos artigos que dispõem sobre a Autoridade Nacional de Proteção de Dados (ANPD), como marco temporal para início de vigência o dia 28 de dezembro de 2018, estabelecendo a data de agosto de 2020 para os demais, esclarece-se que esse cenário foi alterado em 29 de abril de 2020, em razão da Medida Provisória n. 959/2020, que estabeleceu, em seu artigo 4º, a ampliação da *vacatio legis* da Lei para a data de 03 de maio de 2021[4].

1 "Tratamento: 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" (BRASIL, 2018a).

2 "Para fins desta Lei, considera-se: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II – pessoal sensível: dado pessoal sobre 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, dados genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018a).

3 De acordo com estudos realizados pela BSA em 2015, naquele ano, cerca de 2,5 quintilhões de bytes de dados eram criados por dia (BSA THE SOFTWARE ALLIANCE, 2015). Além disso, releva-se que para os líderes empresariais globais, os dados constituem recurso fundamental para o negócio, resultando em ganhos de eficiência por meio da tecnologia da informação que podem agregar aproximadamente US$ 15 trilhões ao PIB global até 2030.

4 Segundo Alex Mecabô (2020), "a medida, em verdade, já era objeto de discussão em outras inúmeras propostas legislativas semelhantes, datadas de antes mesmo da eclosão da pandemia do novo coronavírus".

No entanto, embora tenha ocorrido a prorrogação da data de início da vigência da Lei n. 13.709/2018, há uma estimativa de prazo de quatro a quatorze meses para adequação completa da empresa aos dispositivos das normas de proteção de dados[5] . Por essa razão, mostra-se necessário que as empresas busquem se adequar com a maior antecedência possível.

Assim, diante da importância e da contemporaneidade do tema, visando a disseminação do assunto no meio contábil, o presente trabalho tem por objetivo demonstrar de que forma os escritórios de contabilidade podem se adequar à Lei Geral de Proteção de Dados a partir da averiguação do inventário de dados (*data mapping*).

Para isso, utilizar-se-á do método dedutivo e de pesquisa bibliográfica, com enfoque na intepretação da Lei n. 13.709/2018 em consonância com o desenvolvimento das atividades contábeis.

Importa esclarecer que apesar de o presente trabalho focar sua análise na implementação da Lei Geral de Proteção de Dados Pessoais em Escritório de Contabilidade, tal estudo se aplica a todos os ramos empresariais que realizam tratamento de dados pessoais e que, dessa forma, estão sujeitos à adequação de privacidade. Delimitou-se, no entanto, a demonstrar de forma prática de que maneira se sucede a averiguação do *data mapping* no cotidiano empresarial. Ressalta-se, ainda, que se deve atentar às peculiaridades de cada setor e empresa.

1 DATA MAPPING: ADEQUAÇÃO DE ESCRITÓRIOS DE CONTABILIDADE À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

De maneira objetiva, pode-se descrever o *data mapping* como sendo um inventário dos dados tratados por uma empresa em determinado momento. Portanto, assim como os demonstrativos contábeis, o *data mapping* representa uma posição estática, que permite compreender de que modo ocorre o "ciclo de vida dos dados"[6] operacionalizados pela empresa.

A apuração do mapeamento de dados possibilita a verificação de vários fatores, dentre eles, a constatação dos tipos de dados que estão sendo coletados, por quanto tempo esses dados ficam disponíveis, os fluxos de dados[7] e o momento que efetivamente são descartados.

Trata-se de uma etapa preliminar no planejamento para a instauração de um sistema adequado de tratamento de dados pessoais com base nas novas diretrizes impostas pela Lei Geral

5 Variar-se-á de acordo com os seguintes critérios: "o nível de maturidade da empresa no assunto; as regras e procedimento já existentes; a quantidade de áreas e projetos que tratam dados pessoais; o nível de sensibilidade dos referidos dados objeto do tratamento; o orçamento previsto para a adequação" (COELHO, [201-?], p. 19).

6 Os dados são considerados como potenciais objetos de informação. Nessa perspectiva, sob a ótica da ciência da informação, Ricardo Cesar Gonçalves Sant'ana (2016, p. 119) identifica as fases (momentos em que distintas necessidades e competências são necessárias) envolvidas no acesso e no uso dos dados - sendo: coleta; armazenamento; recuperação e descarte - identificando os fatores e as características que propiciam a ampliação do equilíbrio entre os agentes envolvidos no processo e a máxima otimização do uso dos dados.

7 "Caminho" percorrido pelos dados pelos setores da empresa.

de Proteção de Dados, possibilitando uma visão geral e detalhada de todo o fluxo de dados dentre da organização.

A implementação desse sistema depende da compreensão das peculiaridades de cada organização, pois o tratamento adequado de dados pessoais relaciona-se com variáveis que devem ser observadas em cada caso, como é, por exemplo, a classificação de determinado dado pessoal. Dependendo da empresa, o dado é considerado como útil no desenvolvimento de sua atividade econômica, sendo, portanto, permitido, por lei, seu tratamento, desde que com consentimento do titular. Por sua vez, para outros ramos empresariais, o mesmo dado pessoal pode ser classificado como sem função para o desenvolvimento das atividades da empresa, sendo vedado o seu tratamento.

Do mesmo modo, da coleta até o descarte, os dados percorrem um "caminho" dentro da organização, no qual vários colaboradores possuem acesso. Logo, deve-se conhecer esses fluxos e identificar todos que tenham alcance a essas informações.

Nessa toada, é importante ressaltar que o mapeamento de dados deve ser feito de forma desmembrada por sistemas ou por setores da empresa, pois o mesmo dado pode ter finalidades diferentes dependendo do departamento que realizará o tratamento. Mister destacar, ainda, que a metodologia aplicada na elaboração do *data mapping* deve levar em consideração as especificidades da empresa analisada.

As empresas contábeis se destacam pelo fato de trabalharem com uma grande variedade, quantitativa e qualitativa, de dados pessoais em decorrência de suas atividades. É comum que o departamento pessoal dos escritórios de contabilidade receba dados pessoais de trabalhadores das empresas clientes, como documentos pessoais, carteira de trabalho, dentre outros.

Do mesmo modo, o departamento jurídico faz o tratamento de dados pessoais ao coletar documentos pessoais de sócios e administradores para a confecção dos contratos sociais. Os departamentos fiscais e contábeis realizam tratamento de dados pessoais ao trabalharem com notas fiscais ao consumidor, entre outros dados que podem ser necessários para o desenvolvimento das atividades contábeis.

Nesse cenário, faz-se necessário que os escritórios de contabilidade se adequem às diretrizes da Lei Geral de Proteção de Dados (BRASIL, 2018a). Esses cuidados transpassam os interesses da empresa contábil, sendo, também, de responsabilidade das empresas clientes que fiscalizem a aplicação e observação da proteção de dados, em razão de que é de sua responsabilidade fiscalizar as empresas parceiras no desenvolvimento de suas atividades e no cumprimento das obrigações legais.

Com base nessas ressalvas, é possível classificar o ciclo de vida dos dados em quatro fases: a) fase do planejamento; b) fase da coleta; c) fase da organização, e d) fase da utilização e divulgação[8] . Ao implementar as diretrizes da Lei Geral de Proteção de Dados (BRASIL, 2018a), tem-se perspectivas diferentes para cada fase.

8 Gervânia Alves (c2022) apresenta uma discriminação pormenorizada do ciclo de dados, classificando-os em: coleta; processamento; análise; compartilhamento; armazenamento; reutilização; e eliminação.

Na fase do planejamento, a empresa contábil deve realizar a coleta do consentimento[9] do titular dos dados (BRASIL, 2018a), informando-lhe sobre a finalidade[10] e o objetivo dessa coleta. O consentimento do titular só é dispensado nas hipóteses discriminadas nos incisos de II a X do artigo 7º da Lei Geral de Proteção de Dados (BRASIL, 2018a), destacando-se, quanto à atividade contábil, o inciso II, que se refere ao "cumprimento de obrigação legal ou regulatória pelo controlador[11] "; o inciso V, que prevê a dispensabilidade do consentimento quando o tratamento for "necessário para a execução do contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados", bem como o inciso IX, que torna o consentimento dispensável "quando necessário para atender aos interesses legítimos do controlador ou de terceiro".

Na prestação de serviços contábeis, o tratamento de dados pode ocorrer em diversos setores[12] e com distintas finalidades[13]. Em regra, grande parte das atividades contábeis estão voltadas ao cumprimento de obrigações impostas por lei, como no caso do tratamento de dados para o preenchimento da declaração do eSocial, assim como para execução de contrato firmado com o titular do dado, por exemplo, na abertura de uma empresa em que o escritório contábil solicita os dados dos sócios. Porém, deve-se prestar atenção aos casos em que a coleta de dados não se enquadra nas hipóteses de dispensa, sendo imprescindível a coleta do consentimento do titular.

Na segunda fase ocorre a coleta dos dados, em que a empresa deve manter-se transparente[14] quanto aos dados que estão sendo coletados, de modo a viabilizar que o titular tenha acesso a essas informações, além de manter a qualidade dos dados (BRASIL, 2018a), preservando-os íntegros, atualizados e protegidos de acordo com a necessidade para o cumprimento da finalidade do seu tratamento.

Nesse momento, por meio da constatação dos dados coletados, é fundamental que a empresa realize a classificação dos dados quanto à sua finalidade, detectando os dados que possuem pouca ou nenhuma relevância para a empresa e, por conseguinte, que devem ser descartados, daqueles que possuem relevância e devem ser tratados.

Na fase da organização, a empresa contábil deve implementar ferramentas hábeis para gerir esses dados de forma segura[15]

9 "O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (BRASIL, 2018a).

10 "O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei" (BRASIL, 2018a).

11 "Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018a).
"Pessoa natural ou jurídica de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018a).

12 Departamento contábil, financeiro, fiscal, pessoal, jurídico, dentre outros.

13 Como exemplo, podemos citar os dados pessoais do sócio administrador. Para o departamento jurídico, eles terão a finalidade de preencher cadastros de abertura de empresa, enquanto que para o departamento pessoal, os dados têm como finalidade o lançamento do pró-labore, por sua vez, para o departamento fiscal, os mesmos dados, em tese, não terão finalidade.

14 "Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" (BRASIL, 2018a).

15 "Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não

e que garantam os direitos do titular. É necessário observar que a Lei Geral de Proteção de Dados visa regulamentar o tratamento de dados por quaisquer meios, seja físico ou eletrônico.

Assim, é impreterível que se tenha também um planejamento quanto à proteção dos dados físicos que estejam em posse do escritório, como arquivos, documentos e registros, estabelecendo meios que inviabilizem que pessoa não autorizada tenha acesso a essas informações.

A última fase é composta pela utilização e divulgação dos dados, devendo ser observados todos os requisitos anteriores, de prevenção, de transparência, de segurança e de prestação de contas aos titulares dos dados. Após o tratamento, os dados serão eliminados, conservados ou compartilhados (BRASIL, 2018a).

Uma prática muito comum nos escritórios de contabilidade é o armazenamento de dados já tratados, por meio de arquivos digitais e físicos, pelo período decadencial ou prescricional estabelecido por lei, a depender do tipo de dado. Ocorre que a Lei n. 13.709/2018 dispõe que os dados já tratados devem ser eliminados, autorizada sua conservação apenas nas hipóteses discriminadas nos incisos de I a III do artigo 16, dentre elas, para o cumprimento de obrigação legal ou regulatória do controlador e para uso exclusivo do controlador, vedado o acesso por terceiros, e desde que anonimizados[16].

Conforme disposição do item 29 das Normas Brasileiras de Contabilidade NBC T XX – Escrituração contábil, "O contabilista deve comunicar formalmente ao empresário ou à sociedade empresária sobre a necessidade de armazenar em meio eletrônico ou magnético (...) os documentos, os livros e as demonstrações referidas nesta Norma [...]" (NORMAS..., [20--?], p. 04).

Dessa maneira, compreende-se que, após a realização do tratamento dos dados, esses documentos devem ser encaminhados ao empresário ou à sociedade empresária que forneceu os dados, ou diretamente a seus titulares, como por exemplo, a entrega da Carteira de Trabalho e Previdência Social (CTPS) ao seu titular.

Caso o escritório seja o responsável pelo armazenamento das informações, deve-se colher o consentimento dos titulares, assim como observar o prazo máximo estabelecido por lei para cada documento e implementar sistemas de proteção que assegurem a inviolabilidade desses dados.

Nesse entendimento, a Egrégia Segunda Turma Cível do Tribunal de Justiça do Distrito Federal, em APL n. 12686620048070006 DF 0001268-66.2004.807.0006, considerou que "A guarda dos documentos fiscais da empresa, principalmente talões de notas fiscais de saída, é de responsabilidade do empresário, não podendo seu extravio ser imputado à empresa de contabilidade" (BRASIL, 2009).

De igual modo a Egrégia Quinta Câmara Cível do Tribunal de Justiça do Rio Grande de Sul, em Apelação Cível n. 70076115732, decidiu que "os livros contábeis devem ser resguardados e ficar sempre sob a posse da sociedade mercantil" (BRASIL, 2018b).

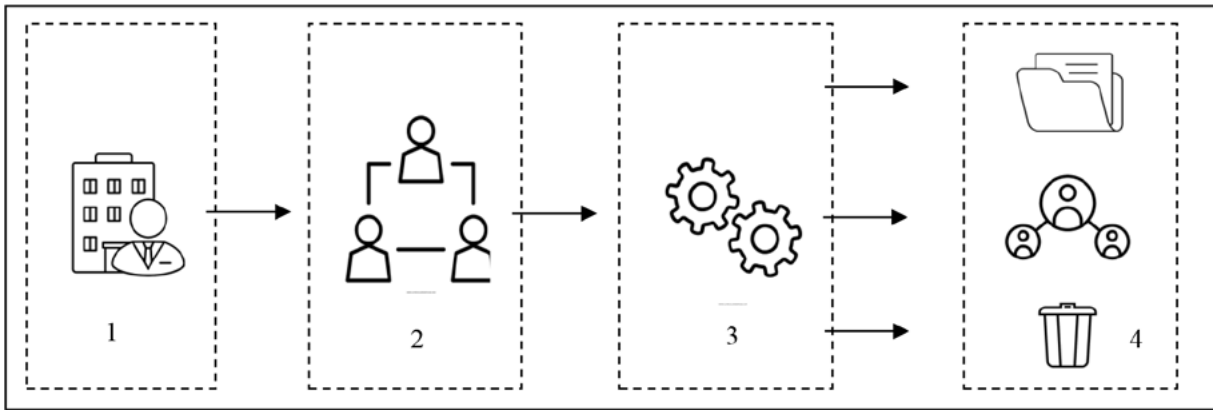
Compreendendo essas fases do ciclo de vida dos dados, **é possível** montar o seguinte

autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (BRASIL, 2018a).

16 "Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (BRASIL, 2018).

organograma de mapeamento de dados:

Figura 1 – *Data Mapping* empresa contábil



Fonte: Elaborado pelos autores.

À vista desse organograma, de forma sucinta, observa-se que o fluxo de dados em um escritório de contabilidade percorre o seguinte caminho: 1) coleta dos dados; 2) encaminhamento dos dados para os respectivos departamentos (fiscal, financeiro, contábil, pessoal, jurídico); 3) tratamento dos dados, e 4) arquivamento, compartilhamento ou descarte desses dados.

Como visto, diante da complexidade de dados a serem analisados, para a melhor elaboração do *data mapping* é importante que esse processo seja realizado por todos os setores da empresa, com auxílio técnico e jurídico para que seja possível constatar eventuais vulnerabilidades no processo (BRANDÃO, c2021).

Assim, de forma prática, quanto às empresas contábeis, os principais itens a serem observados na apuração do mapeamento de dados, são: a) os tipos de dados coletados: cadastrais, pessoais, sensíveis, trabalhistas, fiscais, etc.; b) volume e frequência dos dados: diária, semanal, mensal, etc.; c) etapas do fluxo de dados: coleta, armazenagem, distribuição nos departamentos, processamento, transferências, descarte, etc.; d) tecnologias utilizadas no tratamento: sistemas, bancos de dados, armazenamento em nuvem, etc.; e) locais onde os dados são coletados, armazenados, tratados ou processados: internamente ou externamente; f) origem dos dados e canais de captura: aplicativos, online, estabelecimentos físicos, empresas terceirizadas, etc.; g) campanhas de marketing: eventuais dados pessoais tratados com a finalidade de campanha de marketing; h) compartilhamento de dados com parceiros: profissional terceirizado, empresa de sistemas, órgãos do governo, etc.; i) compartilhamento com empresas coligadas do grupo econômico; j) localidades do tratamento: local onde a empresa exerce atividade; k) transferência internacional de dados; l) base legal: indicar a fundamentação legal com base na Lei Geral de Proteção de Dados referente ao fluxo descrito; m) política de privacidade; n) dados de crianças e de adolescentes: observar o disposto no artigo 14 da Lei n. 13.709/2018; o) política de retenção e extinção de dados; p) segurança da informação: identificação dos principais controles de segurança da informação direcionados a proteção de dados, e q) direito dos titulares: averiguação se o fluxo

de dados permite que o titular do dado pessoal exerça seus direitos (BRANDÃO, c2021).

Ressalta-se novamente que não se trata de uma abordagem exaustiva, cabe a cada empresa verificar a sua realidade. No entanto, esses são os principais itens passíveis de serem destacados em relação às empresas contábeis.

Além disso, o mapeamento de dados resultará em um documento estático, enquanto o fluxo de dados é constante. Por essa razão, deve-se certificar que o *data mapping* demonstre a realidade do tratamento de dados na empresa.

Desse modo, é possível estabelecer um plano de adequação de desenvolvimento das atividades operacionais da empresa com as diretrizes da Lei Geral de Proteção de Dados. Dessarte, o mapeamento de dados servirá de subsídio para as próximas etapas de implementação das políticas de segurança (CRUZ, 2019).

A partir disso, a empresa contábil poderá definir as "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (BRASIL, 2018a).

Para a concretização dessas medidas, é essencial que exista a cooperação de todos os agentes colaboradores da empresa, assim como de fornecedores e de clientes. Trata-se de um sistema que deve funcionar em harmonia, em que cada componente é fundamental na concretização das políticas de segurança.

Dessa forma, visando efetivar suas políticas de segurança, a empresa contábil poderá, conforme dispõe o artigo 50 da Lei n. 13.709/2018:

> [...] formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018a).

Esse sistema composto por processos, condutas e políticas gerencia a atuação da empresa de acordo com os interesses dos seus sócios. Para mais, "as práticas da governança corporativa não devem buscar o lucro a qualquer custo, mas sim satisfazer todas as partes interessadas no negócio" (SBCOACHING, 2018, p. 1).

Outro ponto relevante a ser observado pelas empresas contábeis, diz respeito a implementação da metodologia do *Privacy by Design* definida nos artigos 46, § 2º e 47 da Lei n. 13.709/2018 (BRASIL, 2018a), que estabelecem que as medidas de proteção de dados deverão ser verificadas em todas as fases de desenvolvimento do serviço, da concepção até mesmo após o término da execuç**ão,** incluindo o conceito de proteção e de privacidade dos dados entre seus valores e determinando-os como norteadores de suas condutas (O QUE..., 2019).

Por essa metodologia, tem-se que a aplicação de medidas de proteção de dados em todos

os processos de desenvolvimento de produtos e serviços otimiza os custos operacionais e é mais eficiente em comparação com a implementação em sistemas já existentes (GONZÁLEZ, 2019).

Na prática contábil, a implementação da metodologia do *Privacy by Design* deve ocorrer sob o prisma dos princípios da prevenção, da privacidade como configuração padrão, da segurança de ponta a ponta, da visibilidade e da transparência e do respeito pela privacidade do titular (GONZÁLEZ, 2019).

A responsabilidade do escritório de contabilidade começa com a coleta dos dados, que por vezes ocorre no local da empresa tomadora do serviço. A partir desse momento, já devem ser observados os procedimentos de segurança, desde medidas simples quanto ao modo de transporte desses documentos, a sistemas complexos de transferência de dados online.

Posteriormente, em regra, tem-se a fase de classificação desses dados e da distribuição aos departamentos competentes. Nesse aspecto, alguns cuidados são fundamentais, como o controle de quem recebe esses dados e para quem estão sendo transferidos, o modo que eles são armazenados e o controle desses fluxos.

Subsequentemente, na fase do tratamento dos dados, é de suma importância que o escritório de contabilidade se certifique que os meios utilizados estejam em conformidade com a Lei Geral de Proteção de Dados.

Atualmente, a maior parte dos serviços contábeis está direcionada a processamentos realizados de forma online ou por meio de sistemas. Preenchimento de obrigações como o Sistema Público de Escrituração Digital (SPED), a Declaração de Débitos e Créditos Tributários Federais (DCTF) e o eSocial representam considerável fração das atividades desenvolvidas, bem como a escrituração e o processamento de dados por meio de programas contábeis.

Em razão disso, é fundamental que as máquinas utilizadas nesse processo possuam sistemas de proteção contra invasões de hackers, vírus e contra acesso de pessoas não autorizadas. Além disso, os programas contábeis contratados também devem estar alinhados às diretrizes da Lei n. 13.709/2018 (BRASIL, 2018a).

Após o tratamento dos dados, a empresa contábil deve se certificar de destiná-los de forma correta. Tratam-se das hipóteses previstas no artigo 16 da Lei Geral de Proteção de Dados, sendo a eliminação, conservação ou compartilhamento.

Por fim, destacam-se as figuras do controlador, do operador e do encarregado que são estabelecidos pela Lei, pois o tipo de responsabilidade é diferenciada para cada um. Ao controlador compete as decisões referentes ao tratamento de dados pessoais, podendo ser representado por pessoa natural ou jurídica, de direito público ou privado (BRASIL, 2018a).

Por sua vez, o operador é aquela pessoa natural ou jurídica, de direito público ou privado, que realizará o tratamento de dados pessoais em nome do controlador (BRASIL, 2018a).

Já o encarregado, é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados." (BRASIL, 2018a).

As funções do controlador e do operador estão dispostas dos artigos 37 a 40 da Lei n.

13.709/2018 (BRASIL, 2018a), enquanto que os deveres do encarregado estão discriminados no artigo 41 da referida Lei.

A Lei atribui ao controlador ou ao operador o dever de reparar os danos causados em razão do exercício da atividade de tratamento de dados pessoais, (BRASIL, 2018a) o operador responder solidariamente pelos danos causados em função do descumprimento das obrigações impostas por lei ou quando descumprir as instruções lícitas do controlador, equiparando-se, nesse caso, ao controlador (BRASIL, 2018a).

No que diz respeito ao controlador que estiver diretamente envolvido no tratamento que resultou em danos, responderá solidariamente, salvo nos casos de exclusão dispostos no artigo 43 (BRASIL, 2018a).

De forma precisa e clara, no entendimento de Gisele Kauer, controlador é que "manda", o operador **é** quem cumpre as ordens e os dispositivos legais, e o encarregado é aquele que atua como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (KAUER, [201-?]).

Questiona-se se haveria a possibilidade de a mesma pessoa figurar como controlador e operador simultaneamente. Ainda não h**á** muita discussão sobre esse tema, contudo, usando como base a interpretação do ICO.UK **(***The Intergovernmental Oceanographic Commission of UNESCO*), não seria apropriado que a mesma pessoa fosse um controlador e um operador ao mesmo tempo, para um mesmo conjunto de dados e para o mesmo tratamento (COMO..., [20--?]).

> Apesar de não haver muito material sobre o tema na LGPD, ser um controlador e operador simultaneamente poderia dificultar seriamente a identificação de quem é o responsável por determinar como o dado é processado e o tipo de processamento necessário, bem como criar dificuldades na hora de definir as funções e responsabilidade administrativas de cada parte (COMO..., [20--?]).

Dessa forma, diante de tal questionamento, recomenda-se que as empresas haja com prudência, atribuindo à agentes diferentes as funções de controlador e de operador.

CONCLUSÃO

Constatou-se que a promulgação da Lei Geral de Proteção de Dados Pessoais atende a um anseio da comunidade global pela implementação efetiva de uma proteção da privacidade dos indivíduos frente ao exponencial aumento de tratamento de dados realizados nos últimos anos, muito em razão do desenvolvimento da globalização econômica e das novas técnicas de administração, as quais se utilizam de dados pessoais para aumentar o ganho de eficiência dos agentes econômicos privados, tornando, assim, os bancos de dados como um dos ativos mais valiosos do mercado contemporâneo.

Evidentemente não se pretende proibir que as empresas tratem dados pessoais para o desenvolvimento de suas atividades econômicas. Busca-se, essencialmente, regularizar tais atos,

equacionando o princípio do livre desenvolvimento e privacidade dos titulares dos dados com os princípios da livre iniciativa e do desenvolvimento econômico das empresas.

Verificou-se que a implementação das diretrizes da Lei Geral de Dados Pessoais exige uma série e mudanças no cotidiano dos agentes econômicos. Para isso, primeiramente é necessário fazer um estudo de todas as atividades da empresa que necessitam se adequar, nessa premissa, o instrumento do *data mapping* surge com enorme importância para compreender de que forma o tratamento de dados se desenvolve dentro da empresa.

Diante do exposto, conclui-se para uma efetiva adequação dos escritórios de contabilidade à Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018a) é fundamental que se realize, de forma preliminar, o mapeamento dos dados (*data mapping*), para que se tenha maior compreensão do fluxo de dados, bem como dos dados que estão sendo colhidos, as finalidades de tratamento desses dados por cada departamento e o modo que eles são descartados, armazenados ou compartilhados, a fim de viabilizar a implementação de sistemas de proteção, de modo a se adequar à nova legislação.

Essas mesmas premissas se aplicam a todos os demais ramos, desde que observados as peculiaridades de cada empresa. O *data mapping*, portanto, demonstrou-se instrumento essencial para a compreensão do tratamento de dados pessoais dentro da própria organização e para a adequada implementação das diretrizes da Lei Geral de Proteção de Dados Pessoais.

REFERÊNCIAS

ALVES, Gervânia. **Ciclo de vida dos dados e LGPD**. São José dos Pinhais: XPositum Consultoria Empresarial, c2022. Disponível em: https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd. Acesso em: 29 jun. 2022.

BRANDÃO, Graziela. **O que é o mapeamento de dados**. São Paulo: BL Consultoria Digital, c2021. Disponível em: https://blconsultoriadigital.com.br/mapeamento-de-dados/. Acesso em: 29 jun. 2022.

BRASIL. Ministério da Ciência, Tecnologia, Inovação e Comunicações. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, n. 157, p. 59, 15 ago. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#:~:text=LEI%20N%C2%BA%2013.709%2C%20DE%2014%20DE%20AGOSTO%20DE%202018&text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20de,(Marco%20Civil%20da%20Internet). Acesso em: 29 jun. 2022.

BRASIL. Tribunal de Justiça do Distrito Federal (2. Turma Cível). Apelação Cível 0001268-66.2004.807.0006 DF 0001268-66.2004.807.0006. Dano material e moral. Multa por irregularidade contábil. Prova pericial conclusiva. Fato gerador diverso das atribuições afetas à empresa de contabilidade. Sonegação fiscal [...]. Relator: J. J. Costa Carvalho, 15 de abril de 2009. **DJ-e**: jurisprudência do Tibunal de Justiça do Distrito Federal e Territórios TJ-DF, Sobradinho, p. 145, 2009. Disponível em: https://tj-df.jusbrasil.com.br/jurisprudencia/5867450/apelacao-ci-vel-apl-12686620048070006-df-0001268-6620048070006?ref=serp. Acesso em: 29 jun. 2022.

BRASIL. Tribunal de Justiça do Rio Grande do Sul (5. Câmara Cível). Apelação Cível 70076115732. Dissolução e liquidação de sociedade. Prestação de contas. Cearceamente de defesa. Configurado. Apresentação dos livros contábeis. Responsabilidade da parte autora. Documentos sob a guarda da postulante. Cerceamento de defesa reconhecido [...]. Relator: Jorge Luiz Lopes do Canto, 28 de março de 2018b. **Diário da Justiça**: Tribunal de Justiça do Rio Grande do Sul, 2018x. Disponível em: https://tj-rs.jusbrasil.com.br/jurisprudencia/562345814/apelacao-civel-ac-70076115732-rs?ref=serp. Acesso em: 29 jun. 2022.

BSA THE SOFTWARE ALLIANCE. **Estudo da BSA ilustra o impacto mundial da revolução de dados**. Washington: BSA the Software Alliance, 2015. Disponível em: https://www.bsa.org/pt/noticias-e-eventos/comunicados-de-imprensa/estudo-da-bsa-ilustra-o-impacto-mundial-da-revolucao-de-dados. Acesso em: 29 jun. 2022.

COELHO, Luciano Villela (coord.). **LGPD lei geral de proteção de dados**. São Paulo: FIESP, [201-?]. Disponível em: https://www.fiesp.com.br/arquivo-download/?id=252615. Acesso em: 29 jun. 2022.

COMO saber se minha empresa é um operador ou controlador perante a LGPD?. Rio de Janeiro: Macher Tecnologia, [20--?]. Disponível em: https://www.machertecnologia.com.br/operador-ou-controlador-lgpd/. Acesso em: 29 jun. 2022.

CRUZ, Leandro Saad. **Mapeamento de dados para LGPD**. [*S. l.*]: Medium, 2019. Disponível em: https://medium.com/@leandrosaad/mapeamento-de-dados-para-lgpd-c36413d54b73. Acesso em: 29 jun. 2022.

GONZÁLEZ. Mariana. **Veja como implementar o Privacy by Design nos seus processos de tecnologia**. [*S. l.*]: IDBLOG, 2019. Disponível em: https://blog.idwall.co/privacy-by-design-implementar-processos-tecnologia/. Acesso em: 29 jun. 2022.

KAUER, Gisele. **Controlador, operador e encarregado**: quem é quem na LGPD. Perdizes: Infra News Telecom, [201-?]. Disponível em: https://infranewstelecom.com.br/controlador-operador-encarregado-quem-e-quem-na-lgpd/. Acesso em: 29 jun. 2022.

MECABÔ, Alex. **Postergação da vigência da LGPD**: um remédio necessário?. São Paulo: Consultor Jurídico, 2020. Disponível em: https://www.conjur.com.br/2020-mai-01/direito-civil-atual-postergacao-vigencia-lei-geral-protecao-dados-remedio-necessario. Acesso em: 29 jun. 2022.

NORMAS Brasileiras de contabilidade NBC T XX: escrituração contábil. [*S. l.: s. n.*], [20--?]. Disponível em: https://cfc.org.br/wp-content/uploads/2016/02/NBCT_2.pdf. Acesso em: 29 jun. 2022.

O QUE significa “Privacy by design” e qual a relação com a LGPD. Tubarão: OSTEC Segurança Digital de Resultados, 2019. Disponível em: https://ostec.blog/geral/privacy-by-design/. Acesso em: 29 jun. 2022.

SANT'ANA, Ricardo César Gonçalves. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. *Informação & Informação*, Londrina, v. 21, n. 2, p.116-142, 2016. Disponível em: https://www.uel.br/revistas/uel/index.php/informacao/article/view/27940/20124. Acesso em: 29 jun. 2022.

SBCOACHING. **Governança corporativa**: o que é, importância e benefícios. São Paulo: SBCOACHING, 2018. Disponível em: https://www.sbcoaching.com.br/blog/governanca-corporativa /. Acesso em: 1 jul. 2020.

Como citar: MUSTAFÁ, Rennan Herbert; BENFATTI, Fábio Fernandes Neves. Data mapping: adequação de escritórios de contabilidade à lei geral de proteção de dados. **Scientia Iuris**, Londrina, v. 26, n. 2, p. 103-116, jul. 2022. DOI 10.5433/21788189.2022v26n2p103. ISSN: 2178-8189.

Recebido em 13/06/2021
Aprovado em 27/04/2022