Mariana Battochio STUART[1]
Victor Augusto Estevam VALENTE[2]
José Eduardo Figueiredo de Andrade MARTINS[3]

Argumenta
Journal Law
n. 37 p. 177-208
mai/ago 2022

A RESPONSABILIDADE PENAL DO ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS

THE CRIMINAL LIABILITY OF THE DATA PROTECTION OFFICER

LA RESPONSABILIDAD CRIMINAL DE LOS ENCARGADOS DE TRATAMIENTO DE DATOS PERSONALES

Como citar este artigo:
STUART, Mariana, VALENTE, Victor, MARTINS, José. A responsabilidade penal do encarregado de proteção de dados pessoais. Argumenta Journal Law, Jacarezinho – PR, Brasil, n. 37, 2022, p. 177-208

Data da submissão:
20/09/2020
Data da aprovação:
25/06/2021

SUMÁRIO:

RESUMO:

Este artigo tem por escopo perquirir sobre a responsabilidade criminal do encarregado de proteção de dados à luz da Lei nº 13.709/18 ("Lei Geral de Proteção de Dados"). Discorre-se sobre as relações obrigacionais entre os agentes de tratamento e o encarregado, figura similar ao *Data Protection Officer* no Regulamento Europeu nº 2016/679, com a finalidade de delinear as funções de cada personagem no trata-

1. Pontifícia Universidade Católica de Campinas - Brasil
2. Pontifícia Universidade Católica de Campinas - Brasil
3. Pontifícia Universidade Católica de Campinas - Brasil

mento de dados. Faz-se a análise dos fundamentos dogmáticos de autoria em estruturas empresariais, cujas bases revelam ter certa aplicabilidade em face dos delitos cometidos no tratamento de dados, máxime na definição da responsabilidade criminal do encarregado.

ABSTRACT:

This article aims to investigate the criminal liability of the data protection officer under Law 13.709/18 ("General Data Protection Law"). It is discussed about the obligatory relations between the agents of treatment and the person in charge, figure similar to the Data Protection Officer in the European Regulation nº 2016/679, with the purpose of outlining the functions of each character in the treatment of data. It is made the analysis of the dogmatic foundations of authorship in business structures, whose bases reveal to have a certain applicability in the face of crimes committed in the processing of data, mainly in the definition of the criminal responsibility of the person in charge.

RESUMEN:

Este artículo tiene como alcance investigar la responsabilidad penal del encargado de protección de datos conforme a la Ley número 13.709/18 (Lei General de Protección de Datos Personales). Se discuten las relaciones obligatorias entre los agentes del tratamiento y el encargado, figura similar a la del Encargado de Protección de Datos en el Reglamento Europeo número 2016/679, con la finalidad de delinear las funciones de cada personaje en el tratamiento de datos. Se analizan los fundamentos dogmáticos de la autoría en estructuras empresariales, cuyas bases muestran una cierta aplicabilidad delante los delitos cometidos en el tratamiento de datos, máxime en la definición de la responsabilidad penal del encargado.

PALAVRAS-CHAVE:

Agentes de Tratamento; Encarregado de Proteção de Dados; Responsabilidade Criminal; Lei Geral de Proteção de Dados Pessoais; Omissão Penalmente Relevante.

KEYWORDS:

Treatment Agents; Data Protection Officer; Criminal Liability; Ge-

neral Law on Protection of Personal Data; Penalty Relevant Omission.

PALABRAS CLAVE:
Agentes de Tratamiento; Encargado de protección de datos; Responsabilidad Pena; Ley General de Protección de Datos Personales; Omisión Penalmente Relevante.

1. INTRODUÇÃO

A privacidade assumiu nova roupagem diante das novas tecnologias da informação, apartando-se da definição clássica do "direito de estar só" ("*the right to be let alone*"), fundada na dicotomia entre público e privado. Com efeito, tornou-se indispensável assegurar ao titular de dados um melhor controle do seu fluxo informacional (autodeterminação informativa), reconhecendo-lhe uma gama de direitos e, ao mesmo tempo, atribuições legais sejam aos agentes de tratamento, seja ao encarregado de dados[1].

A proteção de dados pessoais (liberdade positiva) não é simplesmente evolução da privacidade (liberdade negativa), mas um novo direito da personalidade, é dizer, designa o aspecto personalíssimo de cada indivíduo, insuscetível de propriedade ou de transmissão (BIONI, 2020, p. 90 e 204).

Em nível global, o Regulamento Geral de Proteção de Dados da União Europeia (Regulamento nº 2016/679) é considerado um marco na consolidação da proteção dos dados pessoais, embora tenha confiado aos Estados-membros a definição das sanções jurídicas aos responsáveis pelo tratamento de dados, sobretudo de natureza penal, sempre que as sanções administrativas previstas no Regulamento não forem suficientes ou diante da prática de infrações graves[2].

Sob o ângulo do Direito brasileiro, a Lei nº 13.709/18, intitulada de "Lei Geral de Proteção de Dados", prevê uma miríade de conceitos e institutos, entre os quais os agentes de tratamento (art. 5º, incs. VI, VII e IX) e o encarregado de proteção de dados (art. 5º, inc. VIII)[3]. O novel legislativo também disciplina as responsabilidades civil e administrativa[4] decorrentes do tratamento inadequado de dados pelos agentes de tratamento, em diálogo com os sistemas preceituados no Código Civil, no

Código de Defesa do Consumidor e na Lei nº 12.529/11 (Lei Antitruste).

Nada obstante, certos pontos da aludida legislação ainda geram inquietudes, máxime quanto à falta de previsão expressa sobre a responsabilidade criminal. Vale dizer, a opção legislativa, visando à punição da violação de dados pessoais, se deu pela via do Direito Administrativo Sancionador, "*in pari passu*" com o Direito Civil, em homenagem à intervenção mínima ("*ultima ratio legis*") e à fragmentariedade[5].

Nessa senda, faz-se indispensável a compreensão técnica e acurada acerca das funções e responsabilidades quer dos agentes de tratamento, quer do encarregado no contexto do fluxo informacional, envolvendo desde a coleta e a vigilância até a transparência aos titulares dos dados e à ANPD (Autoridade Nacional de Proteção de Dados).

A partir dessa premissa, urge ponderar até em que medida o encarregado pode ser responsabilizado criminalmente, principalmente tendo em conta as atuais discussões dogmáticas sobre a imputação por crimes omissivos impróprios na estrutura empresarial.

2. DOS AGENTES DE TRATAMENTO DE DADOS

A análise acerca das funções e das pretensas responsabilidades jurídicas do encarregado se condiciona à compreensão, como ponto de partida, sobre as atribuições dos agentes de tratamento, ou seja, o controlador e o operador, que são os verdadeiros responsáveis pela integridade do fluxo informacional e pela concretização dos princípios regentes da proteção de dados pessoais (art. 6º, LGPD)[6].

Essa classificação é necessária para a definição das responsabilidades desses agentes, permitindo que as organizações delimitam, de forma precisa, a função que pretendem desempenhar no tratamento de dados pessoais[7].

Primeiramente, o controlador será o único a determinar como e por qual motivo os dados serão usados pela organização. Esse é a previsão tanto da LGPD[8] como do Regulamento Europeu (Regulamento nº 2016/679), quer dizer, o controlador é pessoa natural ou jurídica, seja de direito público, seja de direito privado, competindo-lhe as decisões atinentes ao tratamento de dados pessoais.

Em regra, o controlador pode processar e tratar dados coletados se utilizando dos seus próprios meios. Em outros casos, tem a opção de con-

tar com serviço externo ou de terceiro (operador) para operar os dados que foram coletados, sendo que, mesmo nessa hipótese, o próprio controlador não se renunciará do controle de dados, seguindo o disposto no artigo 39 da LGPD[9].

Certo é que qualquer pessoa que intervenha em uma das etapas de tratamento será considerada controladora. Ao mesmo tempo em que esse controle de dados implica em certas vantagens econômicas e em melhor conhecimento da atividade empresarial, o controlador assume elevado ônus na esfera civil, eis que lhe compete, em caso de violação de dados pessoais, responder diretamente pelos danos causados ao titular e, paralelamente, em conjunto com outros controladores que participam da mesma relação, nos moldes do art. 42, §1º, inc. II, LGPD (CRUZ *et. al.*, 2020, p. 47).

Também é comum, na prática, a figura dos controladores conjuntos, embora seja inexistente previsão legal sobre tal temário na LGPD. Por exemplo, uma empresa detentora de aplicativo que tem por escopo a intermediação da venda de alimentos, figura como uma primeira controladora ao coletar os dados do consumidor e viabilizar a venda de restaurante responsável pelo fornecimento do alimento, no que o último se torna controlador conjunto de dados[10].

Para que o controlador possa terceirizar o tratamento de dados a um operador, ambos devem preparar uma minuta e assinar um contrato por escrito, garantindo a confidencialidade dos dados, além de definir os objetivos e os métodos de tratamento.

Bem assim, o controlador tem a incumbência de determinar um nível de segurança para a realização do tratamento de dados pelo operador. Exemplificativamente, cabe ao controlador, mediante contrato escrito e devidamente assinado, estatuir se o operador usará ou não um método de criptografia ou qualquer outro seguro para o tratamento de dados, velando pela segurança da informação.

Importante salientar que não é necessário solicitar à ANPD (Autoridade Nacional de Proteção de Dados) permissão para cada caso de terceirização, vez que a ANPD não é um departamento jurídico e, via de consequência, não lhe cabe verificar a conformidade de contratos.

Por outro lado, o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome

do controlador (art. 5º, inc. VII, LGPD). Cabe dizer, tem a atribuição de simplesmente processar e tratar os dados em nome do controlador, sem se envolver em processo decisório sobre o controle ou tratamento (CRUZ *et. al.*, 2020, p. 47).

Isso significa que o operador não poderá alterar a finalidade e os meios pelos quais os dados são usados, sob o risco de responder pelos danos a que der causa por descumprimento de lei ou contrato ou quando não tiver seguido as instruções lícitas do controlador (art. 42, §1º, inc. I, LGPD), cuja hipótese o operador se equipara ao controlador.

Além disso, é possível que um operador seja, ao mesmo tempo, controlador, como no caso de empresa que possui sob seu controle os dados dos seus próprios empregados. Sugere-se, nesse sentido, que o próprio operador, agora na qualidade de controlador, indique um encarregado de proteção de dados pessoais, sobretudo se envolver dados sensíveis e legítimo interesse, para melhor resguardo perante a Autoridade Nacional.

Importante observar que, "*de lege lata*", a LGPD privilegia, em regra, a responsabilidade civil subjetiva, razão pela qual é necessária a demonstração da culpa e do dano, com lastro no artigo 186, c./c. o artigo 927, ambos do Código Civil. Porém, o tratamento de dados pode produzir, por sua natureza e circunstâncias, riscos lhe sejam inerentes, no que será o caso de responsabilidade objetiva pelos danos causados.

O controlador poderá se elidir da responsabilidade civil em caso de comprovação de que o dano decorrera por culpa exclusiva do operador, incidindo na hipótese do artigo 43, inciso III, da LGPD[11].

Mas não é só. Dúvidas exsurgem quanto às funções e à responsabilidade do encarregado no ciclo de tratamento de dados.

Entendemos, nesse quadrante, que o encarregado tem atuação na etapa final de tratamento de dados, cabendo-lhe, unicamente, a avaliação acerca da conformidade dos agentes de tratamento com a LGPD e demais legislações pertinentes. Vale dizer, a função do encarregado se cinge a auxiliar o controlador no monitoramento da conformidade interna, razão pela qual não será ele, em regra, responsável por qualquer ilícito em decorrência de violação de dados pessoais, sendo que eventuais consequências cíveis e administrativas recairão somente às custas dos agentes de tratamento.

Já em outras situações, vislumbramos uma zona nebulosa quanto

à responsabilidade jurídica do encarregado, inclusive na seara criminal. Nada impede, "*de lege ferenda*", que o encarregado também incorra em dolo e, consequentemente, seja responsável pela violação de dados pessoais e os delitos correspondentes, como nos casos de quebra da confidencialidade ou da omissão ou falha de comunicação de não conformidade.

Visando à melhor análise desse temário, faz-se necessário, em um primeiro momento, compreender as funções do encarregado sob o prisma da LGPD e, de forma análoga, do DPO ("*Data Protection Officer"*) no Regulamento Europeu, com o fito de melhor aclarar seus direitos e obrigações no tratamento de dados.

3. *DATA PROTECTION OFFICER* NO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA (REGULAMENTO Nº 2016/679)

O Regulamento Geral europeu (*General Data Protection Regulation* ou RGPD), preceitua critérios objetivos que, uma vez existentes, tornam obrigatória a nomeação do DPO ("*Data Protection Officer*"). Vale dizer, o controlador ou subcontratante terá a obrigatoriedade de nomear o DPO nas seguintes hipóteses: (i) tratamento de dados realizado por autoridade ou organismo público, exceto por tribunais no exercício de sua função jurisdicional; (ii) entidades que controlam regularmente dados pessoais em grande escala; e (iii) entidades que controlam regularmente dados sensíveis em grande escala ou dados pessoais referentes a condenações criminais e infrações penais (MAGALHÃES; PEREIRA, 2018, p. 50).

Nota-se que o RGPD menciona quais são as atividades em que será obrigatória a nomeação do DPO, conquanto os conceitos das atividades sejam vagos (MAGALHÃES; PEREIRA, 2018, p. 51). Caso o controlador ou subcontratante não se insira em qualquer uma dessas hipóteses, ainda assim será possível a nomeação do DPO, mas sem a incidência das mesmas obrigações estatuídas em lei.

Exige-se, outrossim, conhecimento apropriado em proteção de dados pessoais para o cargo de DPO, pressupondo o domínio da legislação e das práticas nacionais e europeia sobre o tema. Pode assumi-lo tanto um colaborador interno como um consultor externo, sendo que a especialização do profissional dependerá da complexidade das operações de tratamento de dados, além do nível de proteção exigido para o tratamento[12].

A rigor, o DPO desempenha função essencial à proteção de dados, incumbindo-lhe garantir o cumprimento do controlador em face de todas as obrigações legais do Regulamento Europeu. Assim, servirá como um eixo entre a organização e a autoridade de controle nacional, além de figurar como mediador junto aos titulares de dados.

O artigo 39º do RGPD prevê, em rol não taxativo, as diversas funções do DPO, com destaque para a sua atuação nas seguintes situações: (i) informar e aconselhar o responsável pelo tratamento ou o subcontratante, assim como os trabalhadores que tratem dos dados, acerca de suas obrigações no contexto da proteção de dados; (ii) controlar a conformidade da organização com o RGPD e com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante referentes à proteção de dados pessoais; (iii) prestar aconselhamento, quando tal lhe for solicitado, sobretudo no que se refere à avaliação de impacto sobre a proteção de dados e o controle de sua realização, nos moldes do artigo 35º do Regulamento; (iv) cooperar com a Autoridade Nacional de controle; e (v) atuar como ponto de contato junto à autoridade de controle sobre questões afetas ao tratamento.

Se não bastasse, o Regulamento Europeu demonstra certa preocupação em garantir a autonomia do DPO em face da governança do controlador. Por exemplo, assegura-se ao DPO, dentro da estrutura organizacional, a liberalidade de se reportar diretamente ao mais elevado nível de responsabilidade pelo tratamento de dados na organização[13].

O DPO também não poderá ser destinatário de instruções que influam no exercício legítimo de suas funções, tampouco poderá ser destituído ou penalizado por conta delas.

Ainda assim, o encarregado pode desempenhar outras funções e atribuições, cabendo ao responsável pelo tratamento ou o subcontratante viabilizá-las sem conflito de interesses (art. 38º, item 6).

Importante registrar que a realização da avaliação de impacto é de responsabilidade do controlador, e não do DPO, a despeito deste prestar assistência ao responsável pelo tratamento para tanto.

Não sem razão, o Grupo de Trabalho do artigo 29 traz recomendações ao responsável pelo tratamento de dados, no sentido de solicitar parecer ao DPO sobre os seguintes pontos: (i) da necessidade de realizar ou não uma avaliação de impacto; (ii) de qual metodologia a ser aplicada

na avaliação de impacto; (iii) de proceder à avaliação de impacto internamente ou, se necessário, contar com terceiro para realizá-la; (iv) de indicar mecanismos para a atenuação de eventuais riscos aos interesses e direitos dos titulares de dados; e (v) de analisar se a avaliação de impacto foi ou não realizada corretamente, assim como se as suas conclusões estão em conformidade com o Regulamento (MAGALHÃES; PEREIRA, 2018, p. 51).

É de incumbência do responsável pelo tratamento notificar a Autoridade de controle competente sobre caso que envolva a violação de dados pessoais. Esse caso deve ser notificado sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da notificação, salvo se a violação dos dados pessoais não for suscetível de resultar em risco para os direitos e liberdades das pessoas singulares. Caso a notificação à autoridade não seja transmitida no prazo de 72 horas, deverá ser acompanhada dos motivos do atraso (art. 33º, item 1).

Da mesma forma, o titular de dados pessoais deve ser comunicado quando a violação implicar um elevado risco aos seus direitos e liberdades fundamentais (art. 34º, item 1).

Infere-se que o DPO assume responsabilidades significativas, em particular a de relatar eventual não conformidade ao nível de gerenciamento mais elevado da organização.

O RGPD não disciplina qualquer responsabilidade jurídica específica ao DPO, sendo que, de acordo com as diretrizes do Grupo de Trabalho do artigo 29, tão somente o controlador e o operador são responsáveis pelo cumprimento da legislação, cabendo-lhes demonstrar a conformidade, independentemente da autonomia assegurada ao DPO.

Porém, isso não significa que o DPO não será responsabilizado juridicamente, inclusive na área criminal, por seu mau desempenho, pela violação do seu dever de cuidado ou pelo descumprimento de suas obrigações contratuais ou das normas estatais, a depender do estabelecido pelas leis internas de cada Estado-membro da União Europeia.

Isto porque o RGPD não disciplina responsabilidades jurídicas em caso de violação de dados pessoais, confiando aos Estados-membros da União Europeia essa faculdade. Diante disso, alguns países, de acordo com as suas conveniências e necessidades, disciplinaram formas próprias de responsabilidade dos controladores e subcontratantes, notadamente de

cariz civil e criminal (v.g., Portugal e Itália).

No caso da Itália, o DPO poderá ser responsabilizado juridicamente não somente por violação de disposições contratuais, como também por violação do seu dever de cuidado ("*diligenza*") ou da obrigação de lealdade ("*obbligo di fedeltà*") em relação ao controlador, como ocorre nos casos de quebra do sigilo ou das obrigações de confidencialidade.

Sob o ângulo do Direito Penal, o controlador é quem será responsabilizado pelos crimes preceituados no Código de Proteção de Dados italiano, tais como os delitos de tratamento ilegal de dados ("*tratamento illecito di dati*"), previsto no artigo 167, ou de não adoção de medidas mínimas se segurança. E, em casos excepcionais, essas disposições penais podem se entender ao DPO, máxime se este agir, diretamente, mediante comunicação e divulgação ilegal de dados pessoais sujeitos a processamento em grande escala (art. 167-bis) ou declarações falsas apresentadas perante a Autoridade Italiana de Proteção de Dados (art. 168)[14].

Em Portugal, a Lei nº 58/2019 prevê crimes específicos no contexto de tratamento e armazenamento de dados pessoais: (i) utilização de dados de forma incompatível com a finalidade da recolha (art. 46º); (ii) acesso indevido (art. 47º); (iii) desvio de dados (art. 48º); (iv) viciação ou destruição de dados (art. 49º); (v) inserção de dados falsos (art. 50º); (vi) violação do dever de sigilo (art. 51º); e (vii) desobediência (art. 53º). Também se reconhece a responsabilidade criminal das pessoas jurídicas pela violação de dados pessoais, exceto em se tratando do Estado, de pessoas jurídicas no exercício de prerrogativas de poder público e de organizações de direito internacional (art. 54º).

Portanto, a maioria dos Estados europeus, cada qual em seus ordenamentos internos e em sincronia com o RGPD, estabeleceu funções e responsabilidades jurídicas claras e precisas aos agentes de tratamento, inclusive de jaez criminal, cujos reflexos podem atingir o DPO em casos excepcionais.

4. ENCARREGADO NA LGPD

A LGPD, em seu artigo 5º, inc. VIII, prevê a definição do encarregado pelo tratamento de dados pessoais, cujo cargo é semelhante ao DPO contemplado no RGPD.

Tanto o "*Data Protection Officer*" no RGPD como o encarregado à

luz da LGPD, possuem pontos em comum: atuam como verdadeiros garantidores da organização no cumprimento das legislações de proteção de dados. Cabe dizer, são responsáveis por auxiliar o controlador no cumprimento das suas obrigações legais de proteção de dados, por meio do aconselhamento, monitoramento, entre outras funções de suma importância.

Nesse viés, o encarregado é 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 (ANPD) (art. 5º, inc. VIII, LGPD).

Discute-se, assim, se somente o controlador ou se o operador também deverá indicar um encarregado de proteção de dados. Conforme já salientado, é possível que um operador de dados seja, ao mesmo tempo, controlador de dados dos seus próprios empregados, tornando necessária a indicação de um encarregado.

O encarregado pode ser pessoa natural ou jurídica, além de comitês ou grupos de trabalho. Também pode ser um empregado da organização ou terceiro prestador de serviços.

O artigo 41 da lei de regência disciplina obrigação genérica de nomeação do encarregado, sob a previsão de que "O controlador deverá indicar encarregado pelo tratamento de dados pessoais" (art. 41, "caput", da LGPD). Em cotejo com o RGPD, a LGPD apresenta redação demasiadamente ampla quanto à nomeação do encarregado, sendo que critérios objetivos deverão ser regulamentados, mediante orientações e resoluções, pela Autoridade Nacional de Proteção de Dados (ANPD), que, inclusive, poderá prever hipóteses de dispensa, seguindo o disposto no artigo 41, §3º, da lei de regência.

De todo caso, a empresa tem a opção de nomear, voluntariamente, o encarregado, mesmo que diante da decisão de que a nomeação deste não é obrigatória. Ainda assim, tudo o que for aplicável ao encarregado obrigatório sê-lo-á também ao encarregado nomeado voluntariamente.

Assinala-se que a decisão da organização de não nomear um encarregado não a desonera de cumprir com as obrigações da LGPD, tampouco retira a sua incumbência de contratar ou alocar profissionais voltados à proteção de dados, tais como seu pessoal e consultores externos. Preza-se, no entanto, que a designação de tais profissionais seja técnica e cautelosa, evitando conflito de interesse (OPICE BLUM; NÓBREGA MALDONA-

DO, 2019, p. 319).

Nessa vereda, o artigo 41, §2º, da LGPD prevê, em rol meramente exemplificativo, as funções do encarregado pelo tratamento de dados pessoais, a saber: (i) interagir com os titulares de dados pessoais, sobretudo com o fornecimento de esclarecimentos, além de adotar as providências necessárias relativas a esses contatos ou às reclamações dos titulares; (ii) interagir com a ANPD (Autoridade Nacional de Proteção de Dados), atuando como ponto de contato para recebimento das comunicações da Autoridade, além de ser responsável pela adoção das providências requeridas; (iii) orientar os colaboradores da entidade da qual é encarregado sobre as práticas relacionadas à proteção de dados pessoais; (iv) executar todas as atribuições determinadas em normas complementares pela ANPD ou outros órgãos; (v) assessorar os responsáveis pelo tratamento de dados pessoais na emissão de relatórios de impacto à proteção de dados pessoais, emitindo opiniões e pareceres que possam embasar tais relatórios; (vi) monitorar a conformidade das atividades de tratamento de dados pessoais de acordo com a regulamentação e as normas vigentes; (vii) cooperar com a ANPD, sempre que demandado; (viii) recomendar a realização de relatórios de impacto à proteção de dados pessoais, ou não, inclusive sobre a metodologia da sua realização; (ix) recomendar as salvaguardas para mitigar quaisquer riscos aos direitos dos titulares de dados pessoais tratados pela empresa, inclusive salvaguardas técnicas e medidas organizacionais; e (x) decidir sobre a adequação dos relatórios de impacto à proteção de dados, e se as suas conclusões estão de acordo com a regulamentação, ou não (OPICE BLUM; NÓBREGA MALDONADO, 2019, p. 319).

O encarregado pela proteção de dados pessoais precisa ser acessível aos titulares de dados. Tanto assim que o artigo 41, §1º, da LGPD estabelece a obrigatoriedade de se divulgar, de forma clara e objetiva, os dados de contato do encarregado.

Entendemos, conforme já assinalado, que o encarregado tem atuação somente na etapa final de tratamento dados, cabendo-lhe a avaliação acerca da conformidade dos agentes de tratamento com a LGPD.

Tendo em vista que a sua atuação principal é a de analisar a conformidade, o encarregado não assume, à primeira vista, qualquer responsabilidade jurídica em decorrência da violação de dados pessoais, sendo que

eventuais consequências cíveis e administrativas recaem sobre o controlador e o operador. Porém, é certo que o encarregado ocupa posição de suma importância na cadeia de tratamento de dados pessoais, constituindo em elo entre o controlador, os titulares dos dados e a ANPD.

Ademais, todo e qualquer incidente de segurança deve ser comunicado, previamente, pelo controlador ao encarregado, com o objetivo de que este proceda à avaliação definitiva de que se houve ou não violação de dados pessoais.

Assim, eventual ação ou omissão do encarregado, quer seja ela dolosa, quer seja culposa, rompe com o ciclo de tratamento de dados, podendo configurar, ainda que indiretamente, violação de dados pessoais a ensejar responsabilidades jurídicas.

Reconhecemos, nesse ponto, que o encarregado é suscetível, em casos específicos e excepcionais, à responsabilidade jurídica por violação de dados pessoais, tanto nas searas civil e administrativa, como na esfera criminal, sobretudo quando ele se omite ou falha no seu dever de agir. Resta esclarecer até que ponto se fundamenta, dogmaticamente, a sua autoria nesse contexto, demonstrando ter certa relação com a participação em omissão penalmente relevante, nos termos do artigo 13, §2º, do CP.

5. DA LOCALIZAÇÃO E DOS REQUISITOS DO ENCARREGADO

Embora não seja expressamente previsto na LGPD, recomenda-se que o encarregado esteja localizado em território brasileiro. Caso não esteja em território nacional, deve ter condições de se comunicar, ainda que minimamente, com os titulares e com a ANPD, além de contar com a disponibilidade de estar no Brasil, quando necessário.

Pontua-se, ademais, que a LGPD tem alcance extraterritorial, por força do princípio da extraterritorialidade. Pode ocorrer de a empresa não estar situada no território brasileiro, mas realizar qualquer operação ou tratamento de dados no Brasil, razão pela qual se sujeitará à LGPD[15].

É evidente, a nosso ver, que o encarregado atua como garantidor do cumprimento da legislação de proteção de dados, tanto no Brasil, como no estrangeiro – embora se reconheça que ele não tem a capacidade de ditar ou estabelecer quais são os propósitos ou meios de proteção de dados pessoais.

Nesse sentido, a designação do encarregado deve se basear nos se-

guintes requisitos: (i) conhecimento das operações realizadas pela empresa controladora ou operadora; (ii) conhecimento da legislação de proteção de dados; (iii) conhecimento acerca das práticas de tratamento de dados pessoais; (iv) capacidade de cumprir com os requisitos da LGPD.

Por esse motivo, seria um contrassenso, a nosso ver, a afirmação de que o encarregado, em hipótese alguma, responderia por qualquer ilícito no contexto de tratamento de dados pessoais.

É salutar que seja assegurado ao encarregado o reporte direto à Diretoria ou à Presidência da empresa, valendo-se de todos os recursos necessários para o exercício de suas funções, de forma autônoma e independente, sob o risco de responsabilidade ao longo da estrutura empresarial.

6. DOS CRIMES OMISSIVOS IMPRÓPRIOS E DO DEVER DE VIGILÂNCIA DO ENCARREGADO EM RELAÇÃO AOS DADOS PESSOAIS

Nos últimos anos, a dogmática penal tem se inclinado ao estudo da responsabilidade criminal na estrutura empresarial, mormente quanto à imputação de crimes omissivos impróprios ao "*compliance officer*".

Vislumbra-se que as bases dogmáticas então edificadas nessa seara, sobretudo no âmbito do Direito Penal Econômico, têm se endereçado a melhor definir a autoria nas organizações empresariais, evitando a "irresponsabilidade organizada" (Schünemann)[16].

Ocorre que a LGPD não prevê qualquer matéria afeta à responsabilidade criminal, tampouco delitos específicos relativos ao tratamento inadequado de dados pessoais, ao contrário do que se verifica em outros países[17].

À primeira vista, os fundamentos dogmáticos de autoria em organizações empresariais revelam ter certa aplicabilidade e grau de incidência nos mais diversos delitos cometidos nesse ambiente, servindo de base para a responsabilidade criminal do encarregado no contexto do tratamento ilegítimo de dados, com supedâneo na omissão penalmente relevante, também chamada de crimes omissivos impróprios, impuros, espúrios, promíscuos ou comissivos por omissão[18].

O artigo 13, §2º, do Código Penal, com a Reforma da Parte Geral de 1984 (Lei nº 7.209), confere contornos precisos aos crimes omissivos

impróprios, evitando o alargamento da punição nesse campo[19]. A propósito das hipóteses legais da omissão penalmente relevante, pontua Juarez Tavares que as relações devem ser interpretadas restritivamente, não só em decorrência do princípio da legalidade, como também da necessidade de limitação do poder estatal, com balaústre na intervenção mínima e na dignidade humana[20].

Exsurgem, assim, duas teorias que se dedicam a fundamentar a omissão penalmente relevante, quais sejam, a causal ou naturalista e a normativa jurídica.

Na primeira, é necessária a comprovação do nexo de causalidade entre a omissão e o resultado, caracterizando a relação de causalidade quando o omitente podia e devia agir para evitar o resultado, porém não o fez, sendo que desta omissão advém o resultado (FRAGOSO, 1961. p. 43 e ss). Na segunda, a omissão é "um nada e, do nada, nada vem" ("*ex nihilo nihil fit*"), não possuindo qualquer relevância penal; contudo, a omissão tornar-se-á penalmente relevante à medida que o agente, por meio de seu comportamento omissivo, causa lesão ou expõe a perigo de lesão certo bem jurídico[21].

Para a teoria normativa jurídica, exige-se, a um círculo de autores que ocupam posição especial de salvaguarda a dado bem jurídico, um dever e poder legal de agir para evitar o resultado. Prevalece que é essa a teoria consagrada no Direito Penal brasileiro, a despeito de controvérsias doutrinárias[22].

Nos crimes omissivos impróprios, o tipo penal descreve uma ação ("facere" ou conduta positiva), mas o agente descumpre um dever jurídico que lhe é imposto (artigo 13, §2º, do Código Penal), a ponto de omitir uma conduta que deveria ser cumprida, acarretando a produção do resultado naturalístico. Nada obsta que esse dever jurídico também advenha de outras leis que geram reflexos na área criminal, tal como se verifica nos deveres específicos do Diretor e dos membros do Conselho de Administração na Lei das Sociedades Anônimas (Lei nº 6.494/76), por exemplo.

Em miúdos, sob a égide do Direito Penal brasileiro, a omissão penalmente relevante é adicionável a todos os tipos comissivos, com supedâneo na teoria normativa ou jurídica, conjugada com a escola finalista, admitindo tanto o dolo como a culpa, sendo que a norma proibitiva se transforma em norma preceptiva (mandamental ou de dever de segundo

grau) dirigida a um círculo de possíveis autores (destinatário próprio ou "*delicta propria*") que têm uma especial relação de proteção a certo bem penalmente tutelado ("dever de agir específico"), advindo, da omissão, um resultado (crime material).

Todo crime omissivo impróprio é um crime próprio, estabelecendo uma qualidade especial do sujeito ativo, representada, a rigor, pela condição de garantidor (tipo normativo de autor), que somente assim será considerado se enquadrar nas hipóteses previstas no §2º.

Impende ressaltar que o §2º do artigo 13 do Código Penal funda-se na teoria formal do dever jurídico, que envolve três requisitos alternativos para a determinação da autoria: "a) tenha por lei a obrigação de cuidado, proteção ou vigilância", denominado dever legal (pleno da lei); "b) de outra forma, assumiu a responsabilidade de impedir o resultado", que compreende a posição de garantidor (plano do contrato), ou seja, quem tem, por lei, obrigação de cuidado ou vigilância; e "c) com seu comportamento anterior, criou o risco da ocorrência do resultado", referente à ingerência de risco (agir prévio).

Em que pensem esses fundamentos clássicos da omissão imprópria, a doutrina contemporânea tem se dedicado à ampliação do seu espectro de incidência, vislumbrando certa margem de extensão dessas bases para a determinação da responsabilidade criminal do encarregado de proteção de dados.

7. TENDÊNCIAS ATUAIS DA OMISSÃO IMPRÓPRIA NAS ESTRUTURAS EMPRESARIAIS

A despeito da previsão do §2º do artigo 13, a tendência hodierna é a de considerar que a posição de garantidor não se funda apenas das hipóteses previstas no aludido dispositivo, mas também em outros ramos jurídicos e sociais ligados ao Direito Penal, v.g., o Direito administrativo, digital, civil, comercial e do trabalho, assim como nos programas de *compliance* e nas regras internas de repartição de atribuições dentro de uma empresa (GRECO; ASSIS, 2014, p. 110).

Corroborando do entendimento de Jesús-María Silva Sánchez, há a propensão de que a responsabilidade em comissão por omissão seja cada vez mais aplicada aos delitos de empresa ou de estruturas organizadas (SILVA SÁNCHEZ, 2011, p. 117-118). No mesmo sentido, afirmam Enri-

que Bacigalupo e Yacobucci que a distribuição de competência no âmbito empresarial deve ser fundada na comissão por omissão (ZAPATER, 1998, p. 93; YACOBUCCI, 2003. p. 241-245).

A depender da espécie societária, a doutrina contemporânea também tem se inclinado a estabelecer um conteúdo material à posição do garantidor, analisando-o na perspectiva de dois grupos, a saber: (i) a especial posição de defesa de certos bens jurídicos; e (ii) a responsabilidade pelas fontes produtoras de perigo.

Para Tavares, a especial posição de defesa de certos bens jurídicos justifica-se por alguém se encontrar incapacitado ou sem condições de proteger seus próprios bens e, por isso, outra pessoa assume o ônus dessa proteção; quer dizer, a primeira pessoa espera e pode confiar que a outra a protegerá. A responsabilidade pelas fontes produtoras de perigo pressupõe, por sua vez, um dever de vigilância sobre objetos ou pessoas subordinados, esperando-se um estado de segurança (TAVARES, 2012. p. 316).

Igual sistemática tem sido aplicada aos crimes econômicos nos últimos anos, máxime no que se refere à responsabilidade por omissão penalmente relevante dos administradores, membros do Conselho de Administração e do "*compliance officer*", como no caso das sociedades anônimas.

Segundo Heloisa Estellita, os diretores devem se nortear pelo binômio liberdade-responsabilidade, ou seja, têm eles a liberdade de gerir pessoas e coisas para o atendimento dos objetivos econômicos da empresa e, concomitantemente, possuem o dever de agir para evitar que decorram danos a terceiros ou à coletividade. Em miúdos, o diretor é garantidor originário de vigilância no âmbito das sociedades anônimas (ESTELLITA, set./dez. 2018. p. 408-409).

Os diretores assumem as seguintes funções de garantia: (i) relação de controle sobre a empresa fundada juridicamente, pois são sujeitos que, por força legal e estatutária, têm a capacidade de atuar em nome da sociedade (anônima) perante terceiros e, acima de tudo, de exercer a gestão para alcance do objeto social - logo, assumem deveres de vigilância para atividades intrinsecamente perigosas no contexto empresarial e, "*interna corporis*", passaram a assumir, devido à importância do cargo que ocupam, uma posição de garantia secundária ou derivada mediante a prática de atos de delegação; e (ii) assunção fática das funções, sob o fundamento de que devem exercer, efetivamente, a administração da empresa no plano

fático, não bastando que sejam formalmente – leia-se, no plano documental - apontados como "sócios" ou "diretores", sob violação da responsabilidade subjetiva (ESTELLITA, set./dez. 2018. p. 410-411).

Assim, a posição de garante da Diretoria (CEO - *Chief Executive Officer*) tem como fundamento legal o artigo 13, §2º, "a", do CP, combinado com o artigo 138, "caput" e §1º (poder de gerir a sociedade anônima), e artigo 143, inc. IV, e 144 (funções a serem exercidas individualmente por cada diretor), da Lei nº 6.404/76 (Lei das Sociedades Anônimas).

O Conselho de Administração, por seu turno, é órgão colegiado que, ao lado da diretoria (sistema dual das sociedades anônimas), exercerá a administração da empresa (art. 138, §2º, da lei de regência). Os membros do Conselho são eleitos e destituídos pela Assembleia-Geral de acionistas; suas atribuições e poderes são previstos no artigo 140 da Lei das S.A.´s, com destaque para as seguintes: (i) fixar a orientação geral dos negócios da companhia; (ii) eleger e destituir diretores e fixar suas atribuições, observando o disposto no estatuto social; (iii) fiscalizar a gestão dos diretores, entre outros (ESTELLITA, set./dez. 2018. p. 416).

Compete ao Conselho exercer tais funções por meio de decisões colegiadas, sendo que tais são materializadas pela conjugação da vontade dos conselheiros (vontade do órgão social) - diferentemente dos diretores, que exercem tomada de decisão individual. Assim, os conselheiros se sujeitam aos mesmos deveres de vigilância dos administradores nas sociedades anônimas (ESTELLITA, set./dez. 2018. p. 414-415).

Observa Estellita que não há hierarquia, ao menos no plano da Lei das S.A.´s, entre a Diretoria e o Conselho de Administração - há uma divisão meramente horizontal, e não vertical -, sendo que o último exerce ou participa, ainda que mediante controle parcial ou atuação limitada, da gestão da companhia, competindo-lhe: (i) supervisionar a gestão da companhia; (ii) aprovar, antecipadamente, certas operações ou negócios a serem desenvolvidos no contexto da atividade empresarial; e (iii) destituir diretores, sobretudo diante da iminência da prática de crimes por parte da direção (ESTELLITA, set./dez. 2018. p. 432-433).

Inclusive, compete ao Conselho organizar a estrutura da Diretoria, determinando suas atribuições, nos termos em que dispuser o estatuto social (art. 142, inc. II, da Lei das S.A.´s). Logo, os membros do Conselho exercem um dever de diligência - decorrente das suas posições de garan-

tidores -, sendo obrigação de cada conselheiro evitar ou impedir qualquer gestão que implique na prática de condutas criminosas. Por exemplo, compete a um conselheiro, vislumbrando a ocorrência da prática de uma infração penal pelo diretor, acionar os demais membros do Conselho para que possam deliberar sobre uma advertência ou destituição do diretor[23].

Já para Rodrigo De Grandis, é indispensável, para a responsabilização criminal, que os Conselheiros, por meio de seus votos, proporcionem risco juridicamente desaprovado ao bem jurídico. Assim, não é cabível a imputação da responsabilidade penal dos Conselheiros que porventura apresentam votos dissidentes (DE GRANDIS, 2014, p. 198).

Complementa Pierpaolo Cruz Bottini que a estrutura empresarial também envolve a responsabilidade pela conduta de terceiros, com destaque para condutas complementares, delegação e transferência. No que se refere à ingerência e às atividades delegadas, os seguintes aspectos devem ser tomados em conta: (i) da delegação do dever de controle, envolvendo a delegação de controle de riscos permitidos e não permitidos, além dos direitos residuais do delegante; (ii) da delegação do dever de salvamento; e (iii) da interrupção de cursos causais salvadores[24].

Nesse sentido, o "*compliance office*" ou superintendência de "compliance" é um departamento autônomo e independente que tem por finalidade fiscalizar a conformidade da organização com as normas internas e externas, norteando-se pela prevenção, detecção e remediação. O "*compliance officer*" deve se valer de mecanismos de controle e de monitoramento dos riscos operacionais, com os seguintes objetivos: (i) mitigar a ocorrência de tais riscos em caráter preventivo ("*ex ante*"); ou (ii) se inviável ou insuficiente a prevenção, buscar, em etapa posterior ("*ex post*"), a imediata amenização dos danos para o restabelecimento regular da atividade empresarial.

Em linhas gerais, compete ao "*compliance officer*": (i) analisar, detidamente, os riscos operacionais; (ii) auxiliar nos controles internos, ou seja, as normas e procedimentos em todas as esferas da organização; (iii) elaborar projetos de melhoria contínua e voltados **à adequação às normas técnicas**; (iv) avaliar e prevenir fraudes; (v) gerenciar e rever as políticas de gestão de pessoas, em conjunto com os responsáveis pelo setor de gestão de capital humano, entre outros.

Sem prejuízo, uma das funções de maior importância do "*complian-*

ce officer" é o de se dedicar à análise e ao acompanhamento de todos os riscos operacionais das corporações, em especial das instituições financeiras, devendo comunicá-los, prontamente, à alta administração, além de atuar na resolução desses riscos[25].

Para Renato de Mello Jorge Silveira e Eduardo Saad-Diniz, o "*criminal compliance*" tem sua responsabilidade fundada na infração de um dever, mediante simples conhecimentos abstratos, elidindo-se da verificação do domínio do fato (SILVEIRA; SAAD-DINIZ, 2013, p. 624).

Em que pesem entendimentos em sentido contrário, prevalece que o "compliance" assume a posição de garante na estrutura empresarial, razão pela qual deve responder, nas situações em que incorre em omissão, como se tivesse agido como partícipe de conduta alheia, desde que comprovado, suficientemente, o seu elemento subjetivo. A mesma sistemática pode ser aplicada aos membros do Conselho de Administração, vez que possuem o dever de supervisão sobre os "*compliance officers*".

A título de exemplo, a omissão dolosa ou culposa do "*compliance officer*" quanto à comunicação de uma informação sobre a ocorrência de algum ilícito, notadamente de uma infração penal, aos instituidores ou à alta administração, o torna responsável criminalmente, em particular se podia e devia ter agido para evitar o resultado.

Esse dever de comunicação se dirige aos órgãos de cúpula empresarial, pois eles têm a incumbência de evitar a ocorrência de uma possível infração penal no quadro societário, além de, eventualmente, comunicar o ilícito às autoridades públicas para as providências necessárias. Quanto aos fatos delituosos já ocorridos, o "compliance" atuará meramente como testemunha (art. 342, CP), não havendo margem para imputar-lhe a omissão penalmente relevante[26].

Nesse contexto, os responsáveis pela organização assumem a posição de garantidores no âmbito empresarial, possuindo o dever de vigilância nos seguintes casos: (i) dever de vigilância dos produtos; e (ii) dever de vigilância em relação a subordinados.

No primeiro, assumem o dever de vigilância dos produtos que a empresa distribui e comercializa no mercado, no lado externo da organização societária (dever de vigilância em relação aos produtos). Neste caso, prevalece o entendimento de que os responsáveis devem impedir danos aos consumidores do produto que distribui e comercializa, mesmo em

havendo dissensões sobre o fundamento e o alcance de tal dever. Logo, a omissão do empresário quanto ao recolhimento do produto, mesmo com a descoberta posterior do perigo que este produz, torna-o responsável pelo delito comissivo por omissão, como nos casos de homicídio ou de lesões corporais do consumidor, por exemplo.

Luís Greco e Augusto Assis citam o seguinte exemplo: o empresário que fabricou ou comercializou determinado produto, desconhecendo inicialmente sua natureza nociva, vem a tomar ciência posteriormente sobre tal condição, mas não recolhe o produto de circulação do mercado, de modo que consumidores vêm a falecer. Neste caso, responderá pelo crime de homicídio doloso por omissão.

Outro exemplo: também pode ocorrer, durante a fase de fabricação ou de distribuição do produto, de a empresa violar alguma norma de cuidado, devendo a própria empresa retirar o produto do mercado, sob pena de configurar fato ilícito prévio (ingerência), em que o empresário será punido culposamente, nos termos do art. 13, § 2º, alínea "c", do Código Penal. Contudo, se o empresário posteriormente toma ciência do perigo do produto e não o retira do mercado, daí responderá a título de dolo[27].

Apontam-se, outrossim, propostas referentes à cegueira deliberada em crimes omissivos impróprios em estruturas empresariais. Para Pardini Gonçalves, se o garante possui indícios da ocorrência da situação de perigo e, em vez de buscar a sua confirmação, decide permanecer em estado de suspeita ou incerteza, caracteriza-se a cegueira deliberada[28].

Independentemente da teoria a ser perfilhada, é certo que as acusações não devem possuir uma visão redutora da realidade dos fatos ao ponto de desconsiderarem a análise do dolo. Quer dizer, é descabida a ampliação demasiada da responsabilidade no âmbito empresarial, sobretudo do elemento volitivo. Repugna-se, portanto, qualquer afronta à responsabilidade subjetiva, com fundamento no princípio constitucional da culpabilidade.

Por estas razões, no intento de reafirmar o conteúdo do dolo eventual e evitar a responsabilidade objetiva, é necessário ter-se em conta a teoria do dolo como compromisso cognitivo, que é consentâneo com os crimes de omissão imprópria cometidos na cúpula de estruturas organizadas. Essa proposta teórica possui três requisitos basilares, a saber: (i) a representação, por parte do sujeito ativo, da existência de perigo relevante,

nos moldes do artigo 13, §2°, do Código Penal; (ii) a estratégia adotada para diminuir a concretização do resultado; e (iii) o grau de vulnerabilidade da vítima, ou seja, sua capacidade de autossalvação[29].

Segundo Eduardo Viana e Adriano Teixeira, o autor do delito deve adotar, diante do perigo de resultados não permitidos, estratégias que diminuam a ocorrência deste, sendo que esta situação seria a única forma de se afastar o dolo, subsistindo, quando muito, a culpa "stricto sensu"[30].

Portanto, eventual responsabilização criminal, a fim de que seja necessária e constitucionalmente legítima, deve consubstanciar-se nas garantias do Direito Penal liberal, realçando a responsabilidade subjetiva.

8. ASPECTOS CRIMINAIS DAS ATIVIDADES DO ENCARREGADO E DA SUA PARTICIPAÇÃO OMISSIVA EM CRIME ATIVO DE OUTREM: DELIMITAÇÕES A PARTIR DA RESPONSABILIDADE SUBJETIVA E DO PRINCÍPIO DA CONFIANÇA

Conforme já salientado, o art. 41, §2º, da LGPD atribui funções específicas ao encarregado, imputando-lhe um vínculo obrigacional de atuação, malgrado o rol seja meramente exemplificativo[31].

Compete ao encarregado aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências (inc. I). Da mesma sorte, tem a incumbência de receber comunicações da Autoridade Nacional e adotar providências (inc. II).

Na estrutura empresarial, também ocupa importância a governança de TI (Tecnologia da Informação), consistente em mecanismo de controle que assegura o alinhamento da área de tecnologia da informação, em especial da segurança da informação, com as boas práticas e os objetivos estratégicos da organização, além de garantir que os recursos sejam aplicados adequadamente, possibilitando a mitigação de riscos. Assim, a governança de TI é de responsabilidade dos executivos e do conselho de diretores, sendo que a liderança de estruturas organizacionais e processos devem assegurar a capacidade do TI de sustentar os objetivos e estratégias da organização[32].

Em meio a essa estrutura, o vazamento ou compartilhamento ilegal de dados pessoais e sensíveis pode possuir as seguintes causas: (i) falhas estruturais na governança de TI (Tecnologia da Informação) e na segurança da informação, principalmente envolvendo a figura do controlador

e com reflexos no encarregado; e (ii) intrusão em aplicações ou sistemas operativos e no *hardware* de servidores, no que os "hackers", fraudadores, o crime organizado e carteis criminosos buscam o controle de dados e das pessoas (GOODMAN, 2015, p. 140).

Na primeira situação, os riscos oriundos de vulnerabilidades internas às organizações devem ser objeto de mitigação pelos agentes de tratamento e por qualquer pessoa que intervenha nas fases de tratamento, além de contar com a prevenção, detecção e remediação do encarregado. No segundo caso, um terceiro, mediante invasão a um equipamento, consegue acesso a dados e arquivos sensíveis, câmeras, senhas, entre outras informações.

Suponhamos que o encarregado deixe de adotar as providências necessárias aos quais está vinculado na LGPD, sendo que podia e devia ter agido para comunicar ao controlador uma suposta não conformidade para que evitasse um vazamento ou compartilhamento ilegal de dados, porém não o faz.

Sustentamos, primeiramente, que há um vínculo do encarregado à legislação, máxime na esfera criminal, assumindo o dever de garante com base no artigo 13, §2º, "a", do CP, c./c. o artigo 41, §2º, da LGPD.

Esse dever e poder de agir é robustecido na expressão "adotar providências", prevista nos incisos I e II do §2º do artigo 41, pressupondo uma conduta passiva no início e ativa "a posteriori". É dizer, o encarregado, por meio de sua omissão penalmente relevante, tinha a responsabilidade legal de impedir a violação de dados pessoais, em particular o vazamento ou compartilhamento ilegal, conquanto, intencionalmente, tenha deixado de agir, infringindo o disposto no artigo 41, §2º, inc. II, da LGPD, c./c. o artigo 13, §2º, inc. II, do CP. Assim, poderá ele responder pelas mais diversas infrações penais, com especial destaque para delitos perpetrados no ambiente digital: (i) invasão de dispositivo informático (art. 154-A, CP, inserido pela Lei nº 12.737/12), eis que, culposa ou dolosamente, deixou de sugerir o aprimoramento na segurança da informação da organização; (ii) difusão de vírus computacional (art. 154-A, §1º, CP) ou extorsão em decorrência de "*ransomware*" (art. 158, CP), haja vista que, mesmo tendo ciência acerca de eventual vulnerabilidade ou incidente de segurança, deixa de tomar as providências necessárias para impedir a conduta delituosa; (iii) furto mediante fraude (art. 155, §4º, inc. II, CP) em função

de "*phishing*" ou "pesca online"; (iv) crime de divulgação de segredo (art. 153, CP), entre outros.

Meramente a título de ilustração, caso envolvendo o "*ransomware*" ocorreu no caso do inquérito civil nº 08190.097749/18-95, cuja situação sugere, nos dias atuais, reflexões sobre possíveis reflexos criminais não só do controlador, como também do encarregado. *In casu*, o Ministério Público do Distrito Federal e dos Territórios, por intermédio da sua Comissão de Proteção de Dados Pessoais, pugnou, em ação civil pública, pela condenação de um banco digital à indenização de danos causados a interesses coletivos, em decorrência de um incidente de segurança, isto é, omissão na segurança da informação em face de extorsão de um suposto "hacker", culminando no vazamento de dados pessoais de clientes e membros da instituição financeira (v.g., funcionários e executivos).

Imaginemos, em situação análoga, que o controlador, uma vez ciente de falha na segurança da informação em sua empresa, não age para evitar as consequências da extorsão na forma de '*ransomware*", ao passo que o encarregado, também possuindo o conhecimento dessa falha, não comunica dolosamente o controlador ou ambos atuam em de forma orquestrada. Assim, haveria a possibilidade de responsabilização do encarregado ao menos por participação omissiva em crime ativo de outrem (omissão penalmente relevante)[33].

Se não bastasse, é possível que o encarregado incorra em omissão, dolosa ou culposa, na comunicação de qualquer espécie de ilícito penal seja à alta cúpula empresarial, seja à Autoridade Nacional de Proteção de Dados. Neste caso, também há certa margem para que seja responsabilizado criminalmente, em especial por participação omissiva em crime ativo de outrem. Vale dizer, o encarregado contribuirá para delito de outro na estrutura empresarial, em razão do descumprimento do seu dever de vigilância e desde que tenha consciência de sua contribuição.

Ademais, o inciso IV do §2º do artigo 41 da LGPD consiste em verdadeira cláusula genérica ou aberta, sendo que o controlador, mediante regramento e políticas internas à organização, tem o condão de estabelecer outras atribuições específicas ao encarregado.

De se ver que, em todos os casos, deve restar suficientemente demonstrado o elemento subjetivo do encarregado, a título de dolo ou culpa, evitando-se a responsabilidade objetiva.

Entendemos, outrossim, que o princípio da confiança serve como mecanismo indispensável para melhor limitar não só o dever de vigilância ou a ingerência de risco, senão também o dolo na estrutura empresarial, a fim de que não seja alargada nem desvirtuada a responsabilidade do encarregado de proteção de dados[34].

O princípio da confiança tem lastro em valores éticos e no bem jurídico da solidariedade, viabilizando os contatos sociais de caráter anônimo e estimulando atividades ou prestações de alto valor que seriam impossíveis de outra maneira, ocupando importância para a delimitação das funções no contexto do "*compliance*" digital.

Destarte, cabe a aplicação dessa princípio nos seguintes casos: (i) divisão horizontal de funções ou de trabalho, em que indivíduos de um mesmo grupo trabalham em um mesmo nível ou nível equivalente (v.g. a relação entre controlador e encarregado, tal como se verifica nas relações entre cirurgião e anestesista ou o piloto de avião e controlador); e (ii) divisão vertical de funções ou de trabalho, na qual sujeitos trabalham em distintos níveis ou em uma relação hierarquizada, em que um recebe instruções de outra pessoa que se encontra em nível superior, v.g. a relação entre o controlador e o operador, assim como ocorre com o chefe diante de seus empregados (FEIJÓO SÁNCHEZ, 2000. p. 243).

Esse princípio tem o condão de conferir um conteúdo mais específico à posição de garantia na empresa, principalmente envolvendo o "*compliance officer*" ou encarregado ("*compliance digital*") (SILVA SÁNCHEZ, 2013. p. 22-27).

CONCLUSÃO

Ao contrário de diversas legislações de proteção de dados (v.g., Portugal, Itália e Colômbia), a Lei nº 13.709/18 (Lei Geral de Proteção de Dados) não disciplina qualquer responsabilidade criminal, restringindo-se às responsabilidades civil e administrativa dos agentes de tratamento, em sincronia com a intervenção mínima ("*ultima ratio legis*") e a fragmentariedade.

Na esfera civil, a LGPD consagra, via de regra, a responsabilidade subjetiva, tornando-se indispensável a demonstração da culpa e do dano, com lastro no artigo 186, c./c. o artigo 927, ambos do Código Civil. Bem assim, o controlador poderá se elidir da responsabilidade civil em caso de

comprovação de que o dano decorreu por culpa exclusiva do operador, enquadrando-se na hipótese do artigo 43, inciso III, da LGPD[35]. Contudo, será o caso de responsabilidade objetiva se o tratamento de dados produzir, por sua natureza e circunstâncias, riscos lhe sejam imanentes.

Entendemos, nessa senda, que a função do encarregado ou DPO ("*Data Protection Officer*") se circunscreve em auxiliar o controlador no monitoramento da conformidade interna, motivo pelo qual ele não será, em regra, responsável por qualquer violação de dados pessoais.

Vislumbramos, no entanto, uma zona cinzenta quanto à responsabilidade jurídica do encarregado, inclusive na seara criminal, pois nada obsta que ele também incorra em dolo e, consequentemente, seja responsável pela violação de dados pessoais na esfera cível e com possíveis reflexos na área criminal, como nos casos de quebra da confidencialidade ou da omissão na comunicação de não conformidade seja junto ao titular de dados e aos agentes de tratamento, seja à Autoridade Nacional de Proteção de Dados.

Nesse prisma, os fundamentos dogmáticos de autoria em organizações empresariais revelam ter certa aplicabilidade e grau de incidência nos mais diversos ilícitos engendrados no ambiente societário, havendo certa margem para a responsabilização criminal do encarregado com base na participação omissiva em crime ativo de outrem.

Constatamos a existência de um vínculo do encarregado à legislação, máxime na órbita criminal, assumindo o dever de garante com base no artigo 13, §2º, "a", do CP, c./c. o artigo 41, §2º, da LGPD, desde que a sua responsabilidade seja consubstanciada no elemento subjetivo e no princípio da confiança, ou seja, sem se esvaecer das garantias liberais.

Em suma, há possibilidades de que o encarregado responda por certas infrações penais, com ênfase aos crimes praticados no ambiente digital, tais como invasão de dispositivo informático (art. 154-A, CP, inserido pela Lei nº 12.737/12), difusão de vírus computacional (art. 154-A, §1º, CP) ou extorsão em decorrência de "*ransomware*" (art. 158, CP), furto mediante fraude na forma de "*phishing*" (art. 155, §4º, inc. II, CP), divulgação de segredo (art. 153, CP), entrou outros.

REFERÊNCIAS

BERGSTEIN, Laís. Internet das Coisas e "Target Advertising": Riscos e Possibilidades do Uso de Dados Pessoais. In: *Direito do Consumidor Contemporâneo*. OLIVEIRA, Júlio Moraes (Org.). Belo Horizonte: D´Plácido, 2019.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 2 ed. Rio de Janeiro: Forense, 2020.

BOTTINI, Pierpaolo Cruz. *Crimes de Omissão Imprópria*. 1 ed. São Paulo: Marcial Pons, 2018.

CRUZ, Andressa; RIBEIRO, Carlos Alberto; TEIXEIRA, João Pedro Ferraz; BAÑOS, José; MIRANDA, Leandro Alvarenga; COTS, Márcio; AZEVEDO, Ricardo; OLIVEIRA, Ricardo. *O Legítimo Interesse e a LGPD*. Ricardo Oliveira; Márcio Cots (Coords.). 1 ed. São Paulo: Thomson Reuters, 2020.

DE GRANDIS, Rodrigo. *A Imputação Nas Organizações Empresariais*. Dissertação de Mestrado. Universidade de São Paulo, 2014.

ESTELLITA, Heloisa. Causalidade na omissão: um panorama dos problemas das omissões paralelas e sucessivas na criminalidade de empresa. In: *Comentários ao Direito Penal Econômico Brasileiro*. Belo Horizonte: D'Plácido, 2017.

ESTELLITA, Heloisa. Responsabilidade Por Omissão dos Membros de Conselhos de Administração. In: *Revista Portuguesa Ciência Criminal*. Ano 28, nº 3, Coimbra: Instituto de Direito Penal Económico e Europeu da Faculdade de Direito da Universidade de Coimbra set./dez. 2018.

ESTELLITA, Heloisa. *Responsabilidade Penal de Dirigentes de Empresas Por Omissão*: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membro da empresa. 1 ed. São Paulo: Marcial Pons, 2017.

FEIJÓO SÁNCHEZ, Bernardo José. El principio de confiança como critério normativo de imputación en el derecho penal: fundamento y consecuencias dogmáticas. *Revista Ibero-Americana de Ciências Penais*, n. 1, v. 1, p. 227-265, 2000.

FRAGOSO, Heleno Cláudio. *Conduta punível*. São Paulo: José Bushatsky,

1961.

GONÇALVES, Lucas Pardini. *Imputação Dolosa do Crime Omissivo Impróprio Ao Empresário Em Cegueira Deliberada*. Dissertação de Mestrado. Universidade Federal de Minas Gerais, 2019.

GOODMAN, Marc. *Future Crimes*: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. Curitiba: HSM, 2015.

GRECO, Luís; ASSIS, Augusto. O que significa a teoria do domínio do fato para a criminalidade de empresa. In: GRECO, Luís; LEITE, Alaor; TEIXEIRA, Adriano; ASSIS, Augusto. *Autoria como domínio do fato*: estudos introdutórios sobre o concurso de pessoas no Direito Penal brasileiro. São Paulo: Marcial Pons, 2014.

ITÁLIA. Código em Matéria de Proteção de Dados Pessoais. Decreto Legislativo de 30 de junho de 2003. *Garante Per La Protezione Dei Dati Personale*. Disponível em: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.8.

ISACA, COBIT 5: *Modelo Corporativo para Governança e Gestão de TI da organização*, 2012.

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. *Regulamento Geral de Proteção de Dados*: Manual Prático. 2 ed. Porto: Vida Económica, 2018.

OPICE BLUM, Renato. NÓBREGA MALDONADO, Viviane. *LGPD – Lei Geral de Proteção de Dados Comentada.* 2ª edição. São Paulo: Revista dos Tribunais, 2019.

PASCHOAL, Janaína Conceição. *Ingerência Indevida*: os crimes comissivos por omissão e o controle pela punição do não fazer. Porto Alegre: Sergio Antonio Fabris, 2011.

REALE JÚNIOR, Miguel. *Teoria do delito*. São Paulo: Revista dos Tribunais, 2000.

RAMIRO, Mônica Arenas. *El derecho fundamental a la protección de datos personales en Europa*. Valencia, Tirant to Blanch, 2006.

SCHÜNEMANN, Bernd. *Delincuencia empresarial*: cuestiones dogmáticas e de política criminal. Buenos Aires: Fábian J. di Plácido, 2004.

SILVA SÁNCHEZ, Jesús-María. *Aproximação ao Direito Penal contemporâneo*. Tradução de Roberto Barbosa Alves. São Paulo: Revista dos Tribunais, 2011.

SILVA SÁNCHEZ, Jesús-María. *Fundamentos del derecho penal de la empresa*. Montevideo-Buenos Aires: B de F, 2013.

SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. Criminal compliance: os limites da cooperação normativa quanto à lavagem de dinheiro. In: *Revista peruana de ciencias penales*. n. 25. Lima: 2013.

SOUSA, Susana Aires de. A responsabilidade criminal do dirigente: algumas considerações acerca da autoria e comparticipação no contexto empresarial. In: ANDRADE, Manuel da Costa;

ANTUNES, Maria João; SOUSA, Susana Aires de (Org.). *Estudos em homenagem ao Prof. Doutor Jorge Dias de Figueiredo Dias*. v. II. Coimbra, 2009.

STEIDEL, Evelin; GUARAGNI, Fábio André. Desvios de Personalidade em Grupos Empresariais e Neutralização Por Compliance: uma tentativa para minimizar o impacto da corrupção no horizonte da criminalidade? In: *Direito Penal Econômico*: Administrativização do Direito Penal, Criminal Compliance e Outros Temas Contemporâneos. Londrina: Thoth, 2017.

TAVARES, Juarez. *Teoria dos crimes omissivos*. São Paulo: Marcial Pons, 2012.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&-from=PT.

VALENTE, Victor Augusto Estevam. Princípio da confiança em Direito Penal. In: *Boletim IBCCRIM*, São Paulo, v. 22, n. 259, p. 10-13, jun.. 2014.

VIANA, Eduardo; TEIXEIRA, Adriano. A imputação dolosa no caso do "racha em Berlim" comentários à decisão do Tribunal de Berlim, de 27 de fevereiro de 2017 - In. *Revista do Ministério Público do Estado de Goiás*, Goiânia, ano XXI, n. 36, p. 77-98, jul./dez. 2018.

VIANA, Eduardo. *Dolo Como Compromisso Cognitivo*. São Paulo: Marcial Pons, 2017.

ZAFFARONI, Eugenio Raúl. PIERANGELLI, José Henrique. *Manual de Direito Penal brasileiro*: parte geral. 8ª ed. São Paulo: Revista dos Tribunais, 2009.

ZAPATER, Enrique Bacigalupo. *Curso de derecho penal económico*. Madrid: Marcial Pons, 1998.

YACOBUCCI, Guillermo Jorge. *Algunas cuestiones sobre la responsabilidad penal al interno de la empresa*. In: Pensamiento penal e criminológico: Revista de derecho penal integrado, v. 4, n 7, p. 201-259, Córdoba, 2003.

'Notas de fim'

1 No Brasil, o artigo 18 da Lei nº 13.709/18, intitulada "Lei Geral de Proteção de Dados" ou de LGPD, prevê uma série de direitos aos titulares de dados.

2 Eis o item 152 na parte das considerações do Regulamento Europeu: "Sempre que o presente regulamento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do presente regulamento, os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deverá ser determinada pelo direito do Estado-Membro." (UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho)

3 Embora a entrada em vigor da LGPD tenha se tornado objeto de controvérsias no início, é certo que a formação de um sistema de proteção de dados pessoais é uma realidade irrefragável no cenário jurídico brasileiro, assim como se apresenta em outras nações.

4 A responsabilidade civil, tanto de jaez individual como supraindividual, é prevista nos artigos 42 "usque" 45, todos da LGPD, enquanto que a responsabilidade administrativa é disciplinada no artigo 52 da lei de regência.

5 Ao contrário de certos países (v.g., Portugal, Colômbia e Argentina), optou o legislador por não tipificar qualquer conduta relacionada ao fluxo inadequado de dados, permanecendo a incidência das disposições do Código Penal e de legislações penais esparsas pertinentes, tais como o CDC, a Lei nº 8.137/90 (Lei dos Crimes Contra a Ordem Tributária e as Relações de Consumo), a Lei nº 7.716/89 (Lei Antidiscriminação), entre outros.

6 Em que pese a importância desses princípios, não cabe, por ora, estudá-los meticulosamente, sob pena de desvirtuamento temático. De todo caso, merecem destaque não só aqueles contemplados no artigo 6º da LGPD, senão também os princípios da subsidiariedade e da proporcionalidade, consagrados no Regulamento Geral Europeu.

7 Doravante, o controlador sempre estará à vista do titular de dados, cuja sistemática impedirá que seus operadores atuem com plena liberalidade quanto ao uso de dados, como comumente acontecia. Por exemplos, era comum que os operadores se apropriassem das bases de dados repassadas pelos seus contratantes (CRUZ et. al., 2020, p. 47).

8 "Art. 5º. VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

9 Ainda assim, o controlador de dados permanecerá no controle, especificando como os dados serão usados e processados por esse serviço externo. Nos termos do artigo 39 da LGPD: "O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.".

10 É o que ocorre na relação entre o "Ifood" e os restaurantes conveniados, sendo que ambos atuam como controladores conjuntos. E, diferentemente do que se verifica no

Regulamento Europeu, a LGPD não prevê a atuação do controlador subsidiário e de subcontratantes de tratamento de dados (suboperadores).

11 Mesmo que o exemplo se refira à exclusão de responsabilidade do controlador, tal afastamento poderá incidir para o operador, visto que o artigo 43 da LGPD faz menção a "agentes de tratamento".

12 Segundo Magalhães e Pereira: "Em termos gerais, o DPO deve ter capacidade para informar, aconselhar e orientar a administração da empresa/instituição, bem como os seus trabalhadores, a respeito das obrigações constantes do RGPD, assim como das outras disposições de proteção de dados em vigor na União Europeia ou noutros Estados-Membros" (MAGALHÃES; PEREIRA, 2018, p. 55).

13 Essa é a previsão do artigo 38º, itens 1, 2, e 3, do Regulamento Europeu.

14 ITÁLIA. Código em Matéria de Proteção de Dados Pessoais.

15 Para mais detalhes: OPICE BLUM; NÓBREGA MALDONADO, 2019, p. 320.

16 Segundo Schünemann, a descentralização das decisões nas empresas pode gerar o risco de converter a organização da responsabilidade em uma irresponsabilidade organizada. Ou seja, ocorreria na empresa um deslocamento da responsabilidade para os setores inferiores de sua estrutura, os quais acabam por executar materialmente a conduta típica (SCHÜNEMANN, 2004, p. 25-26).

17 Além das experiências italianas e portuguesas já mencionadas, também aponta-se a legislação colombiana, em particular a Lei nº 1.273/09, que inseriu o "Título VII Bis" no Código Penal, em sincronia com a Lei 1.581/12, regulamentada pelo Decreto nº 1.377/13, visando à tutela de um novo bem jurídico-penal, qual seja, a proteção da informação e dos dados, que abrange os Capítulos Primeiro ("Dos Atentados Contra Confidencialidade, a Integridade e a Disponibilidade dos Dados e dos Sistemas Informáticos") e Segundo ("Dos Atentados Informáticos e Outras Infrações").

18 A propósito das discussões conceituais e terminológicas, cf. TAVARES, 2012. p. 312; REALE JÚNIOR, 2000. p. 185

19 Nesse sentido: PASCHOAL, 2011, p. 44-45.

20 TAVARES, 2012, p. 317. Noutro viés, Zaffaroni e Pierangeli apontam problemáticas sobre a posição de garante sob o ângulo do princípio da legalidade. Cf. ZAFFARONI; PIERANGELLI, 2009, p. 466-467 e 472-473.

21 A propósito da teoria naturalística, cf. FRAGOSO, 1961. p. 40.

22 Acerca da causalidade na omissão e da falta de apoio naturalístico, cf. ESTELLITA, 2017, p. 257.

23 Em caso análogo ao do crime preceituado no artigo 6º da Lei nº 7.492/1986, cf. ESTELLITA, set./dez. 2018. p. 436.

24 Para mais detalhes: BOTTINI, 2018, p. 272-296. Também se discute sobre as omissões sucessivas e paralelas no âmbito da empresa, sobretudo acerca da responsabilidade criminal do "compliance officer" a partir de estudo de casos e segundo o modelo de Schrott, cf. ESTELLITA, 2017, p. 100-113.

25 A alta administração apresenta formato próprio a depender da estrutura empresarial. No âmbito das sociedades anônimas, compõe-se pelo Diretor Executivo e pelo Conselho de Administração.

26 Na mesma esteira: STEIDEL; GUARAGNI, 2017. p. 66.

27 Além disso, o responsável tem o dever de vigilância em relação a seus subordinados nos quadros da empresa. Nesse sentido, são os entendimentos de Luís Greco e Augusto Assis e Susana Aires de Sousa. (GRECO; ASSIS, 2014, p. 116; SOUSA, 2009, p. 1030-1035).

28 A propósito da imputação por dolo eventual em crime omissivo impróprio pelo garante em cegueira deliberada, discorre Pardini: "O garante já se omitirá, dolosamente, de

impedir o resultado lesivo, caso este se materialize, mesmo na hipótese de decidir nada fazer quanto a essa comunicação recebida, não obtendo, portanto, conhecimento pleno acerca de sua procedência ou não, e permanecendo na mera suspeita, o que já configura, com segurança, dolo eventual" (PARDINI, 2019, p. 84).

29 O grau de vulnerabilidade da vítima significa que esta não teve nenhuma capacidade de apresentar resistência "in concreto".

30 Para mais detalhes: VIANA; TEIXEIRA, jul./dez. 2018, p. 89 e 92-93; VIANA, 2017, p. 354-358.

31 "Art. 41. §2º. As atividades do encarregado consistem em: I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II – receber comunicações da autoridade nacional e adotar providências; III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem adotas em relação à proteção de dados pessoais; e IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.".

32 Para mais detalhes: ISACA, Cobit, 2012.

33 O "ransomware", em linhas gerais, consiste em prática por meio do uso de "malware" que impede o acesso do usuário ao sistema informático, em particular ao banco de dados pessoais em seu computador, mediante a exigência de um valor ou qualquer outra vantagem indevida a título de resgate, a fim de que seja reestabelecido o acesso, sendo punido ora como difusão de vírus computacional (art. 154-A, §1º, CP), ora como extorsão (art. 158, CP).

34 Segundo Valente: "Por esse princípio, todo aquele que se comporta dentro dos limites do cuidado objetivamente exigido ou do risco permitido, pode confiar que os demais coparticipantes da mesma atividade também atuarão cuidadosamente, seguindo as regras de experiência ("id quod plerumque accidit"), de modo que sua aplicação exclui a responsabilidade dos agentes quanto aos fatos que se situam fora do dever concreto que lhes é exigido no momento da ação." (VALENTE, 2014, p. 11).

35 Mesmo que o exemplo se refira à exclusão de responsabilidade do controlador, tal afastamento poderá incidir para o operador, visto que o artigo 43 da LGPD faz menção a "agentes de tratamento".