DOI: 10.33242/rbdc.2024.01.002

ASPECTOS LEGAIS DA INVESTIGAÇÃO INTERNA POR ANÁLISE DE DADOS NOS PROGRAMAS DE *COMPLIANCE*

LEGAL ASPECTS OF INTERNAL INVESTIGATION BY DATA ANALYSIS IN COMPLIANCE PROGRAMS

Vitor Gabriel de Moura Gonçalves

Mestre em Direito de Empresa e Atividades Econômicas pela Universidade do Estado do Rio de Janeiro (UERJ). Orcid: https://orcid.org/0000-0001-5864-0500
E-mail: vitorgabriel.m@gmail.com

Leonardo da Silva Sant'Anna

Mestre em Direito pela Universidade Gama Filho. Doutor em Saúde Pública pela Escola Nacional de Saúde Pública Sérgio Arouca da Fundação Oswaldo Cruz. Professor do Programa de Pós-Graduação em Direito e da Graduação da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ). Professor Adjunto no Departamento de Direito Comercial e do Trabalho. Orcid: https://orcid.org/0000-0002-5192-2844
E-mail: lsantanna44@gmail.com

Resumo: O artigo trata dos aspectos legais envolvidos na investigação interna por análise de dados nos programas de *compliance*. Procura-se demonstrar que as práticas de governança corporativa não são um fim em si mesmas, precisando também respeitar os direitos da personalidade dos investigados a partir de uma maior participação e transparência no procedimento. Para tanto, são analisados práticas e fundamentos da investigação privada, bem como os aspectos legais na coleta e tratamento de dados pessoais públicos e privados. O método utilizado foi o dedutivo, e a pesquisa bibliográfica se apoia na doutrina civil, empresarial e sobre direito e tecnologia.

Palavras-chave: Lei anticorrupção. Programas de *compliance*. Investigação interna. Privacidade. Proteção de dados.

Abstract: This article discusses the legal aspects within internal investigation by data analysis in compliance programs. The purpose is to demonstrate that corporate governance practices are not an end in themselves, also needing to respect the personality rights of those investigated thru greater participation and transparency in the procedure. For that, practices and fundamentals of private investigation are analyzed, as well as legal aspects in the collection and treatment of public and private personal data. Deductive method was adopted and bibliographic research also leaned in the study of civil law, business law and law and technology doctrines.

Keywords: Anti-corruption law. Compliance programs. Internal investigation. Privacy. Data protection.

Introdução

A adoção de programas de integridade por parte de sociedades empresárias, mais do que uma simples faculdade, tornou-se uma necessidade. A formação de contratos em âmbito nacional e internacional coloca em evidência o nível de reputação e confiança das partes, de modo que a inexistência de qualquer código de ética ou atividade interna de auditoria podem ser vistas com maus olhos por grande parte dos investidores.

O risco sempre foi e sempre será algo inerente ao próprio exercício da atividade empresarial, mas isso não impossibilita sua mitigação na prática. Atualmente, com a vigência da Lei Anticorrupção (Lei nº 12.846), é demonstrado que a responsabilidade civil por atos de corrupção não alcança apenas aqueles que atuaram de forma comissiva, mas também aqueles que se beneficiaram dos atos sem deles ter participado, tenham ou não ciência da sua existência. Fechar os olhos para o risco é estar aberto para futuras responsabilizações indesejadas.

Assim, ganha espaço o investimento em novas técnicas de implementação de programas de integridade, como a investigação interna. Contudo, não há que se pensar na figura de um detetive sorrateiro, com seu sobretudo preto, chapéu e óculos escuros, à espreita de seus investigados. Ao contrário, na era da computação, a relevância dos documentos físicos foi mitigada pela ampla acessibilidade de dados pessoais e dinamicidade de análise via algoritmos e inteligência artificial.

A investigação interna transforma-se numa operação de coleta e análise de informações, acompanhando as pegadas digitais *on-line* e *off-line* dos indivíduos investigados. Com isso, é possível compreender comportamentos para se fazer projeções futuras e analisar potenciais riscos à atividade empresarial. Trata-se de um exercício de criação de perfis individualizados por meio de dados, que direcionará decisões sobre investimentos e desinvestimentos, contratações e demissões, conclusão e rescisão de contratos.

Entretanto, seria possível afirmar que tais informações amplamente disponíveis podem ser de uso ilimitado e irrestrito? Ou que a coleta e tratamento de dados no âmbito corporativo independe de consentimento diante do interesse legítimo do empresário? É preciso compreender a extensão do direito à privacidade e seus desdobramentos na proteção de dados, sob o pretexto de frear eventuais abusos e atos ilícitos na prática investigativa. Nenhum direito deve ser considerado como absoluto, mas é preciso encontrar o limite razoável entre a finalidade dos programas de integridade e o tratamento indiscriminado de dados pessoais.

Para se chegar a uma conclusão sobre os aspectos jurídicos da investigação interna sobre dados pessoais, faz-se mister que antes se desenvolva uma noção prévia sobre os próprios dados e seu procedimento de coleta, armazenamento,

análise e utilização. Não é factível observar o dado pessoal de forma individualizada, ao contrário, verifica-se um uso massificado em grandes aglomerados conhecidos por *big data*, os quais são compilados e interpretados por algoritmos complexos, a fim de agregar valor e natureza informativa aos dados na investigação interna.

1 Compreendendo o *big data* e os algoritmos

É passado o tempo em que o papel era o limite da incorporação de informações. A era da computação trouxe consigo a febre dos dados, de modo que milhares de informações podem ser coletadas e interpretadas em uma mesma máquina, de forma simples e rápida, superando as limitações materiais e humanas até então vigentes.

Nesse sentido, o *Dicionário de Cambridge* traz a seguinte definição para dado: "informação, especialmente fatos ou números, coletada para ser examinada, considerada e utilizada para ajudar tomadas de decisão, ou informação em forma eletrônica que pode ser armazenada e utilizada por um computador" (tradução nossa).[1] Desse verbete, percebe-se que o conceito de dado não é estático, mas passível de divisão em etapas. Trata-se de figura não autossuficiente, que não se satisfaz em sua mera existência, mas depende das fases de coleta, armazenamento, análise e utilização; sempre possui um objetivo final, qual seja, servir como ferramenta para tomada de decisões racionais.

Daí advém a figura do *big data* ou "grandes dados", vez que a utilidade dos dados não reside neles próprios, mas em seu conjunto. Quanto maior e mais variada for a fonte de dados, melhor será sua análise, bem como seu proveito. Nesse sentido, confira-se trecho de estudo desenvolvido pela *Federal Trade Commission* (FTC):

> The term "big data" refers to a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions.[2]

[1] "Information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer" (DATA. *In*: CAMBRIDGE Dictionary. 21 jul. 2020. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/data. Acesso em: 21 jul. 2020).

[2] Tradução livre: "O termo *big data* refere-se a uma confluência de fatores, incluindo a coleta quase onipresente de dados de consumidores através de uma variedade de fontes, o custo do armazenamento de dados, e a poderosa capacidade de analisar dados para estabelecer conexões, bem como fazer inferências e previsões" (FEDERAL TRADE COMISSION. *Big data*: a tool for inclusion or exclusion? 2016. p. 1. Disponível em: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. Acesso em: 21 jul. 2020).

As principais características do *big data* são conhecidas por meio dos seus "Vs", ou seja, uma série de palavras que começam com a letra "v" e sintetizam sua essência. Como exemplos, citam-se: valor, volume, visualização, volatilidade, variedade, vulnerabilidade, validade, veracidade, velocidade e variabilidade,[3] entre outros. Desses, sobressaem-se os mais relevantes, inicialmente identificados por Doug Laney:[4] (i) volume; (ii) variedade e (iii) velocidade.

O primeiro, volume. A quantidade de dados passíveis (e necessárias) de coleta cresce em número exponencial, de modo que as companhias cada vez mais precisam de suas bases de dados sempre atualizadas, bem como avançam na qualidade de seus algoritmos para sua identificação e análise.[5] [6]

O segundo, velocidade. Assim como os dados são produzidos e coletados em ritmo surpreendente, também se tornam obsoletos em curto período de tempo, a depender de sua natureza – trata-se do denominado paradigma dos dados.[7] [8] Por exemplo, dados sobre o fluxo do trânsito em determinada avenida precisam estar constantemente atualizados, de tal forma que dados coletados há um dia, uma hora ou até um minuto podem se mostrar obsoletos e inúteis a determinado fim.

O terceiro, variedade. Os dados podem ser colhidos de forma individual, mas seu completo aproveitamento somente se dará quando analisados de forma global, comparando e conjugando informações de diversas espécies em prol de uma finalidade comum.[9] Isso significa dizer que, reunindo diferentes dados referentes a um mesmo indivíduo, é possível compreender melhor suas personalidade e anseios.

Como se observa, o *big data* seria um fenômeno referente à grande disponibilidade e uso de dados com o objetivo de fazer previsões, conexões e inferências. Para tanto, sua completa utilização depende de três etapas prévias: a) coleta; b) armazenamento; c) análise por algoritmos e *softwares*.[10] Esse procedimento é conhecido como cadeia de valor (*value chain*) e seu estudo é sobremaneira relevante

[3] FIRICAN, George. The 10 Vs of Big Data. *Transforming Data With Intelligence (TDWI)*, 8 fev. 2017. Disponível em: https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx. Acesso em: 21 jul. 2020.

[4] LANEY, Doug. 3D data management: controlling data volume, velocity, and variety. *Application Delivery Strategies*, Stanford, n. 949, p. 1-4, fev. 2001.

[5] LANEY, Doug. 3D data management: controlling data volume, velocity, and variety. *Application Delivery Strategies*, Stanford, n. 949, p. 1-4, fev. 2001. p. 1.

[6] BOURREAU, Marc; DE STREEL, Alexandre; GRAEF, Inge. Big data and competition policy: market power, personalized pricing and advertising. *Centre on Regulation in Europe*, 2017. p. 33.

[7] LANEY, Doug. 3D data management: controlling data volume, velocity, and variety. *Application Delivery Strategies*, Stanford, n. 949, p. 1-4, fev. 2001. p. 2.

[8] BOUTIN, Xavier; CLEMENS, Georg. Defining 'big data' in antitrust. *Competition Policy International (CPI): Antitrust Chronicle*, v. 1, n. 2, mar. 2017. p. 4. Disponível em: https://ssrn.com/abstract=2938397. Acesso em: 21 jul. 2020.

[9] LANEY, Doug. 3D data management: controlling data volume, velocity, and variety. *Application Delivery Strategies*, Stanford, n. 949, p. 1-4, fev. 2001. p. 2.

[10] BOURREAU, Marc; DE STREEL, Alexandre; GRAEF, Inge. Big data and competition policy: market power, personalized pricing and advertising. *Centre on Regulation in Europe*, 2017. p. 11-14.

para a compreensão do *big data*, uma vez que terminará por agregar utilidade aos dados outrora analisados individualmente.

Quanto à origem e coleta de dados, pode-se mencionar aqueles de natureza estritamente pessoal, tais quais: nome, idade, gênero, origem, endereço residencial, geolocalização, comentários em redes sociais e *sites*, buscas em *sites* de pesquisa, valor e objeto de compras *on-line*, informações financeiras, informações sobre saúde, conta bancária, entre outros.[11] Sob uma perspectiva institucional, a coleta de dados pode alcançar o desempenho e rendimento dos empregados e administradores, seus círculos de relacionamentos e histórico de funções, além de dados sobre concorrentes e potenciais parceiros ou novas contratações.

Uma vez coletados os dados, estes serão devidamente armazenados em centros com supercomputadores, com o respectivo suporte de rede para lidar com seu maior ou menor volume e variedade. Todos os dados coletados e armazenados não gozam de valor significativo se não forem devidamente decodificados, organizados, decifrados. Para tanto, utilizam-se complexos programas e fórmulas matemáticas na forma de algoritmos para transformar os dados em informações úteis e com valor.

Um algoritmo pode ser simplesmente compreendido como uma sequência de instruções determinando o que algo (como um *software*) ou alguém deve ou não fazer.[12] Os próprios seres humanos agem conforme lógicas de algoritmo, ou seja, seguem passos para atingir determinado objetivo: como fazer uma receita, como escovar os dentes, como chegar a um endereço ou como elaborar um texto.[13] De toda forma, na lógica de algoritmos aplicados a computadores, tem-se um procedimento computacional bem definido e voltado a agregar valor a determinadas informações.[14]

Por exemplo, o buscador do Google opera por meio de um algoritmo, em que o usuário introduz determinados dados de entrada (*inputs*) para alcançar determinados resultados úteis de pesquisa (*outputs*). Nessa situação é possível identificar três grandes momentos: (i) entrada de dados; (ii) processamento pelo algoritmo; (iii) saída de novos dados ou dados estruturados como resultado.

O algoritmo, por si só, é um mero código lógico e matemático que depende da alimentação de dados e de um sistema para funcionar.[15] Tarleton Gillespie explica

[11] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers*, n. 220, abr. 2017. p. 8.

[12] DOMINGOS, Pedro. *The master algorithm*: how the quest for the ultimate learning machine will remake our world. Nova Iorque: Basic Books, 2015. p. 3.

[13] CORMEN, Thomas. *Algorithms unlocked.* Cambridge: The MIT Press, 2013. p. 16.

[14] CORMEN, Thomas *et al*. *Introduction to algorithms*. 3. ed. Cambridge: The MIT Press, 2009.

[15] SANDVIG, Christian *et al*. Auditing algorithms: research methods for detecting discrimination on internet platforms. *The 64th Annual Meeting of the International Communication Association*, Seattle, 2014, p. 10.

que os algoritmos e os dados são duas metades de uma mesma ontologia, ou seja, máquinas inertes e sem sentido algum, até que sejam pareados com bases de dados para seu correto e esperado funcionamento.[16]

Muito longe de um simples processamento, os algoritmos exercem uma atividade matemática complexa para atingir resultados. Nesse sentido, Rob Kitchin aponta que, por meio de uma perspectiva computacional, os algoritmos seriam a soma dos fatores "lógica" e "controle":[17] (i) lógica, por formular soluções específicas para problemas abstratos (o que fazer); e (ii) controle, com a estratégia para processar resultados dentro de diferentes cenários (como fazer). Os algoritmos vêm sendo amplamente utilizados desde tarefas mais simples, como a organização de dados por categorias predeterminadas, até tarefas mais complexas, como a previsão de riscos em investimentos com terceiros.

Essa maior complexidade no uso de algoritmos passa pelos conceitos de *machine learning* e *deep learning*. No primeiro, a máquina aprende com a base de dados fornecida e identifica uma gama de resultados lógicos e possíveis.[18] No segundo, a máquina também aprende com a base de dados e, mais do que isso, aprende com os próprios resultados para continuar seu processamento de forma automatizada.[19] No *deep learning*, a máquina segue a lógica de que ser compreendido por humanos não é mais um de seus objetivos – organizando-se de forma complexa, tal qual as redes neurais de um cérebro –, mas o que importa é a produção constante e efetiva de *outputs*.[20]

Independentemente da complexidade envolvida nos algoritmos, todos eles possuem o objetivo comum de alcançar um resultado por meio de diferentes situações apresentadas. Direta ou indiretamente, o algoritmo é utilizado como uma forma de exercício de poder, disciplinando cenários, escolhendo o que for mais "importante", classificando e influenciando decisões.[21]

---

16 GILLESPIE, Tarleton. The Relevance of algorithms. *In*: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten. *Media technologies*: essays on communication, materiality, and society. Cambridge: The MIT Press, 2014. p. 169.

17 KITCHIN, Rob. Thinking critically about and researching algorithms. *Information, Communication & Society*, v. 20, n. 1, 2017. p. 16.

18 MOSAVI, Amir; VARGAS, Rocio; RUIZ, Ramon. Deep learning: a review. *In*: SHAKHOVSKA, Natalya (Coord.). *Advances in intelligent systems and computing*. Nova Iorque: Springer, 2017. p. 4.

19 MOSAVI, Amir; VARGAS, Rocio; RUIZ, Ramon. Deep learning: a review. *In*: SHAKHOVSKA, Natalya (Coord.). *Advances in intelligent systems and computing*. Nova Iorque: Springer, 2017. p. 5.

20 BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. *Big Data & Society*, Londres, v. 3, n. 1, 2016. p. 11.

21 BAROCAS, Solon; HOOD, Sophie; ZIEWITZ, Malte. Governing algorithms: a provocation piece. *New York University: Governing Algorithms Conference*, mar. 2013. p. 3.

2 Controle interno e avaliação de riscos

Um relevante movimento internacional direcionado ao combate à corrupção tem sido observado nos últimos anos, tanto em âmbito nacional quanto internacional. Como exemplo, cita-se a lei anticorrupção americana (*Foreign Corrupt Practices Act* – FCPA), a lei anticorrupção inglesa (*UK Bribery Act*), a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, da Organização para a Cooperação e Desenvolvimento Econômico – OCDE (promulgada pelo Decreto nº 3.678/2000), a Convenção Interamericana contra a Corrupção (promulgada pelo Decreto nº 4.410/2002) e a Convenção das Nações Unidas contra a Corrupção (promulgada pelo Decreto nº 5.687/2006).

Criam-se incentivos para que a Administração Pública e a iniciativa privada adotem práticas éticas de governança corporativa por meio do cumprimento de programas de *compliance* nos termos de normas internas e externas anticorrupção. Segundo Richard Steimberg, a partir de uma perspectiva corporativa, enquanto a governança serve para alocar o poder entre administradores, empregados e acionistas, o *compliance* refere-se à adesão às leis e aos códigos de conduta e integridade internos.[22]

Governança e *compliance* são duas faces de uma mesma moeda que devem ser gradadas conforme maior ou menor presença de riscos de fraudes na respectiva atividade. Trata-se de uma importante ferramenta para a prevenção e investigação de ilícitos na estrutura de pessoas jurídicas públicas e privadas que necessariamente terão impacto na cominação de sua responsabilidade civil, penal ou administrativa por eventual ato fraudulento praticado por terceiro contratante ou seu subordinado.

Por isso, a fim de alcançar sucesso na estrutura de governança corporativa, é necessário que o alto escalão dessas organizações adote e mostre compromisso com as práticas éticas e de integridade desejadas para incentivar todos os demais *stakeholders* (prática conhecida como *tone at the top*),[23] além de serem elaborados códigos de conduta claros e minuciosos e oferecidos canais de denúncia que garantam sigilo aos denunciantes e compromisso com a investigação dos fatos anunciados.[24]

[22] STEINBERG, Richard. *Governance, risk management and compliance*. New Jersey: Wiley, 2011. p. 2.

[23] Segundo Richard Steinberg, a expressão *tone at the top* traduz-se no impulsionamento e incorporação de valores éticos e de integridade pela companhia a partir de ações práticas de diretores, administradores e conselheiros. A fim de se consolidar uma cultura de governo da sociedade, faz-se necessário que os superiores hierárquicos deem o exemplo de como se comportar conforme as leis e regulamentos vigentes (STEINBERG, Richard. *Governance, risk management and compliance*. New Jersey: Wiley, 2011. p. 55-56).

[24] STEINBERG, Richard. *Governance, risk management and compliance*. New Jersey: Wiley, 2011. p. 157.

A legislação nacional tem colaborado com o movimento anticorrupção a partir do incentivo à criação de códigos de *compliance* e a adoção de práticas de governança corporativa. Como exemplo, a Lei Anticorrupção (Lei nº 12.846/2013) estabelece um regime amplíssimo de responsabilidade por atos ilícitos praticados contra a Administração Pública. Seu art. 2º consagra a responsabilidade da espécie objetiva, em que a existência de culpa ou dolo no caso concreto é dispensada, atingindo quaisquer atos lesivos praticados no interesse ou benefício da sociedade empresária. Nesse sentido, o art. 7º, VIII estabelece que a existência e funcionamento de programas de integridade, auditoria interna, canais de denúncia e códigos de ética e conduta serão considerados como circunstância atenuante na dosimetria da sanção a ser aplicada à pessoa jurídica.

O Decreto nº 8.420/2015, que regulamenta a Lei Anticorrupção, reitera o caráter minorante da existência de programas efetivos de *compliance* nos arts. 5º, §4º e 18, V, além de estabelecer sua adoção e aplicação ou aperfeiçoamento como condição à celebração de acordo de leniência no art. 37, IV. Ademais, seus arts. 41 e 42 definem o conceito de programa de integridade e, entre outros, estabelecem os seguintes requisitos como essenciais: aplicação a todos os empregados, administradores e terceiros contratantes, análise de riscos e procedimentos independentes de controle interno para prevenção de fraudes e ilícitos, canais de denúncia de irregularidade com proteção aos denunciantes de boa-fé.

Além disso, o Estatuto Jurídico das Empresas Estatais (Lei nº 13.303/2016) determina em seu art. 9º que todas as empresas públicas e sociedades de economia mista da União, estados, municípios e Distrito Federal deverão adotar programas de integridade com código de conduta, auditoria e controle internos, gestão de riscos e canais de denúncia. Por outro lado, o art. 10, III, da Lei de Prevenção à Lavagem de Dinheiro (Lei nº 9.613/98) impõe que as pessoas jurídicas que exerçam atividade financeira e outras elencadas no rol do art. 9º adotem programas de integridade para prevenir a prática de ilícitos e prestar informações às autoridades financeiras.

Já em âmbito administrativo, a Comissão de Valores Mobiliários (CVM), na Instrução nº 480/2009, exige das companhias abertas a existência e efetividade de programas de *compliance* como condição à emissão de valores mobiliários, enquanto o Banco Central do Brasil (Bacen) faz a mesma exigência em relação às instituições financeiras na Resolução nº 4.595/2017. Cumpre ressaltar que o Conselho Administrativo de Defesa Econômica (Cade) dispõe em suas "Orientações sobre estruturação e benefícios da adoção de programas de *compliance* concorrencial" que a existência e funcionamento de programa de *compliance* pode impactar a dosimetria das sanções administrativas de sua competência.[25]

[25] CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. *Guia Programas de Compliance*: Orientações sobre estruturação e benefícios da adoção de programas de compliance concorrencial. Jan. 2016. p. 39-43.

No âmbito das relações administrativas, a Lei nº 7.753/2017, do Município do Rio de Janeiro, e a Lei Distrital nº 6.308/2019 estabelecem a obrigatoriedade de as sociedades empresárias possuírem programa de integridade quando celebrarem contrato, consórcio, convênio, concessão ou parceria público-privada com a Administração Pública, desde que a operação supere determinado valor global. No mesmo sentido caminha o Projeto da Nova Lei de Licitações e Contratos (Projeto de Lei do Senado nº 1.292/95), que tanto impõe a adoção de programas de integridade aos empresários nos contratos de grande valor quanto prevê sua adoção e desenvolvimento como critério de desempate na escolha da melhor proposta.

Do exposto, observa-se um constante movimento do legislador e da Administração Pública no sentido de substituir a faculdade pela obrigatoriedade da existência e funcionamento efetivo de programas de integridade. Caso determinada sociedade empresária decida por não elaborar ou não efetivar seu código de conduta, terá como consequência a restrição de sua entrada em determinados mercados, além de agravar consideravelmente os riscos na exploração da atividade econômica e o *quantum* de eventual responsabilidade civil, penal ou administrativa por ato ilícito.

Muito mais do que uma faculdade, a governança corporativa e o programa de *compliance* podem ser considerados como consequências da aplicação prática do princípio da função social da empresa e do conceito de empresário previsto no art. 966 do Código Civil (CC). A organização dos bens de produção para exercício de atividade econômica não se limita a satisfazer apenas o interesse do empresário, como também de toda a coletividade com a geração de empregos, pagamento de tributos e desenvolvimento econômico e social.[26] Admitir isso permite concluir que a prevenção de fraudes e outros ilícitos é fundamental ao exercício sustentável da empresa enquanto comum aos interesses empresarial e coletivo.

Logo, surge a necessidade de os empresários investirem em procedimentos internos de integridade, com o fim de identificar e prevenir atividades potencialmente suspeitas dentro de sua própria estrutura empresarial, ao mesmo tempo em que se difunde um ideal de comportamento ético aos acionistas ou sócios e *stakeholders* e fornece meios seguros de comunicação de ilícitos. Conviver com altos riscos significa se sujeitar a eles, vez que a responsabilidade civil do empresário independe de atuação ativa, bastando que terceiro lhe proporcione benefícios ou atue em seu interesse. Assim, para melhor compreender o desenvolvimento de um controle interno efetivo, é necessário identificar e avaliar os riscos envolvidos na empresa.

Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf. Acesso em: 2 jul. 2020.

[26] COMPARATO, Fábio Konder. Função social da propriedade dos bens de produção. *Revista de Direito Mercantil, Industrial, Econômico e Financeiro*, São Paulo, v. 130, n. 63, p. 78, 1986.

2.1 Avaliação de riscos

A avaliação de riscos (*risk assessment*) vem sendo considerada como aspecto central dos programas de integridade, tamanha sua relevância prática nas esferas legal, financeira, de negócios e de reputação.[27] Entretanto, como observa David Hilson, os riscos não devem ser considerados como algo ruim, mas como uma relação entre perigos e oportunidades.[28] Toda atividade possui riscos próprios e inerentes, cabendo ao empresário identificar aqueles que são lícitos e vantajosos.

Conhecer melhor seus acionistas ou sócios e *stakeholders*, desde funcionários até terceiros contratantes, permite identificar as áreas de maior e menor risco no exercício da atividade, a probabilidade da concretização desses riscos e seus impactos, ou como evitar possíveis danos futuros. Nesse sentido, David Hilson identifica quatro etapas dentro do procedimento de avaliação de riscos: (i) planejamento, (ii) identificação, (iii) análise, (iv) resultados.[29] Em um primeiro momento, deve-se compreender os objetivos do projeto, estabelecendo a metodologia a ser utilizada. Em seguida, a identificação dos riscos se daria por meio de *brainstorming* e *workshops*, com foco tanto nos aspectos positivos quanto negativos.

Encontrados os riscos, deve ser feita uma análise qualitativa para averiguar sua probabilidade e seus efeitos práticos, bem como uma análise quantitativa com a aferição dos valores relativos à sua duração e custos para superação. Por fim, encontra-se uma resposta sobre como monitorar, priorizar e/ou superar os riscos de forma efetiva e sustentável, ora aceitando, reduzindo ou compartilhando sua existência.[30]

Referidas etapas, não à toa, enquadram-se perfeitamente na cadeia de valor do *big data*, com a ressalva de que o *brainstorming* de ideias seja substituído por algoritmos e dados. Logo, determinada sociedade empresária poderia coletar informações relevantes sobre seu funcionamento, investimentos, funcionários, administradores, terceiros contratantes, entre outros. Em seguida, todas as informações seriam analisadas e organizadas por um algoritmo, de acordo com regras e metodologias prefixadas. Por fim, os dados seriam utilizados para detectar riscos a

[27] COMPLIANCE risk assessments: the third ingredient in a world-class ethics and compliance program. *Deloitte*, 2015. p. 4. Disponível em: https://www2.deloitte.com/us/en/pages/risk/articles/compliance-risk-assessments-the-third-ingredient-in-a-world-class-ethics-and-compliance-program.html. Acesso em: 21 jul. 2020.

[28] HILLSON, David. Extending the risk process to manage opportunities. *International Journal of Project Management*, v. 20, n. 3, 2002. p. 236.

[29] HILLSON, David. Extending the risk process to manage opportunities. *International Journal of Project Management*, v. 20, n. 3, 2002. p. 236-239.

[30] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMISSION. *Risk assessment in practice*. 2012. p. 2. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf. Acesso em: 21 jul. 2020.

que a sociedade está submetida, seus potenciais prejuízos, soluções, entre outros fins estabelecidos.[31]

Em vez de o programa de *compliance* ser guiado por ideias e normas gerais, o processamento de dados faz com que seus objetivos sejam passíveis de maior individualização e aplicação prática para cada companhia em específico. Assim, seria possível identificar com maior grau de certeza os principais riscos (*red flags*) com as respectivas intervenções cabíveis.

Como exemplo de informações relevantes a serem coletadas e analisadas, mencionam-se: como são realizados os pagamentos, descontos em produtos, reembolsos, países visitados pelo cliente, administrador ou empregado, relação despesa-receita, relações com pessoas politicamente expostas, relações de contratantes com a Administração Pública, *e-mail* e telefone corporativos, comportamento em redes sociais, entre outros.

A análise de dados dá vida aos códigos de ética e conduta, moldando-os conforme a situação concreta de cada sociedade empresária. Trata-se de uma verdadeira dinamicidade no procedimento, sempre acompanhando a efetividade do programa, seu cumprimento pelos *stakeholders* e eventuais atualizações. Com isso, permite-se buscar um constante *feedback* sobre a identificação de riscos – quais riscos? Quem os fomenta? Como? Onde? Por quê? –, auxiliando e aperfeiçoando as atividades de auditoria interna e externa.[32]

2.2 Controle por investigação interna

Por dia, 2,5 quintilhões de *bytes* de dados são criados na internet, e esse número não para de crescer, vez que 90% dos dados disponíveis na rede foram criados apenas nos dois últimos anos.[33] Essa é a principal razão do sucesso de investigações envolvendo dados pessoais públicos e privados, na medida em que

[31] A análise de dados como motor de programas de integridade foi considerada como uma ferramenta recomendada pelo Departamento de Justiça dos Estados Unidos: "Control Testing – Has the company reviewed and audited its compliance program in the area relating to the misconduct, including testing of relevant controls, collection and analysis of compliance data, and interviews of employees and third-parties? How are the results reported and action items tracked? What control testing has the company generally undertaken?" (UNITED STATES DEPARTMENT OF JUSTICE. *Evaluation of Corporate Compliance Programs*. 2020. Disponível em: https://www.justice.gov/criminal-fraud/page/file/937501/download. Acesso em: 21 jul. 2020).

[32] OLSEN, Bill; REYNOLDS, Dan; KOLTSOV, Alex. Using data analytics to meet the government's anti-corruption compliance expectations. *The FCPA Report*, v. 5, n. 9, 2016. p. 1.

[33] MARR, Bernard. How much data do we create every day? The Mind-blowing stats everyone should read. *Forbes*, Jersey City, maio 2018. Disponível em: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#5487a9660ba9. Acesso em: 21 jul. 2020.

tamanha quantidade de informações amplamente acessível pode ser usada para mitigar e controlar riscos nas atividades econômicas. Mas quem seriam, de fato, os competentes para realizar tal investigação?

Tim Prenzler nomeia tais agentes como investigadores privados (operadores), os quais, no interesse do contratado (controlador), prestam serviços com fins naturalmente comerciais (análise de riscos), domésticos (dentro de relações familiares), legais (análise de processos judiciais) ou antifraude (como nas companhias de seguro em relação às declarações do segurado).[34] Com isso, presta-se a investigação interna a compreender o funcionamento interno da companhia e sua relação com terceiros a partir de todos os agentes envolvidos na atividade econômica (empregados, administradores, acionistas e terceiros contratantes) com o fim de prevenir ou identificar comportamentos ilícitos.

A noção de controle interno por investigação nas sociedades empresárias assemelha-se significativamente ao conceito de detetive particular, trazido pelo art. 2º, *caput* e §2º da Lei do Detetive Particular – LDP (Lei nº 13.432/2017):

> Art. 2º Para os fins desta Lei, considera-se detetive particular o profissional que, habitualmente, por conta própria ou na forma de sociedade civil ou empresarial, planeje e execute coleta de dados e informações de natureza não criminal, com conhecimento técnico e utilizando recursos e meios tecnológicos permitidos, visando ao esclarecimento de assuntos de interesse privado do contratante.
>
> §1º Consideram-se sinônimas, para efeito desta Lei, as expressões "detetive particular", "detetive profissional" e outras que tenham ou venham a ter o mesmo objeto.

Apesar de o termo "detetive" ser estranho ao contexto de controle interno corporativo, o §1º é claro ao afirmar que qualquer outra expressão sinônima (como investigador privado e operador de dados) pode chamar a aplicação da legislação, desde que sua atividade coincida com aquela referida no *caput* do art. 2º. Em suma, são três os requisitos legais para a classificação de um detetive particular: (i) atividade profissional, habitual e técnica; (ii) coleta de dados e informações de natureza não criminal via meios tecnológicos permitidos; (iii) objetivo de esclarecer assuntos de interesse privado.

A sociedade empresária controladora tanto pode contratar pessoa jurídica ou física especializada para ser responsável pela coleta, organização e tratamento

[34] PRENZLER, Tim. Private investigators. *In*: GILL, Martin (Coord.). *The handbook of security*. Nova Iorque: Palgrave Macmillan, 2006. p. 423.

dos dados disponíveis, quanto pode realizar todas essas etapas por meio de órgãos internos independentes. Seja qual for a opção escolhida pelo empresário, é preciso que o programa de integridade harmonize a finalidade da investigação interna com as competências de seus respectivos órgãos societários.

Quando a investigação atingir diretores, é preciso que seu procedimento e relatório circunstanciado final sejam acessíveis ao conselho de administração, sem oposição e independentemente de justificativa, a fim de consolidar sua competência fiscalizatória (art. 142, III da Lei nº 6.404/76).[35] Por outro lado, sendo o caso de investigação de administradores, o mesmo direito deve ser dado ao conselho fiscal ou a qualquer um de seus membros individualmente, de modo a possibilitar a fiscalização da legalidade e legitimidade de seus atos e eventual denúncia por irregularidade (art. 163, I e IV da Lei nº 6.404/76 e art. 1.069, I e IV do CC).[36]

Em relação à atuação do detetive particular, este terá atribuição para: coletar, armazenar, organizar, tratar e utilizar os dados para compreender as relações internas e externas da sociedade empresária. Todas as atividades envolvidas na cadeia de valor dos dados precisam se desenvolver por meios lícitos, sem a prática de qualquer violação à privacidade de outrem e sujeitas à fiscalização do contratante. Além disso, a norma afasta a possibilidade de a investigação ter fins criminais, vez que se imiscuiria em atividade de atribuição da polícia judiciária.

Aqui se faz necessária uma observação. Dentro do sistema de programas de integridade, a investigação interna terá como fim lógico a apuração de eventuais riscos e atos ilícitos praticados por acionistas ou sócios e *stakeholders*, principalmente os atos de corrupção. Entretanto, o fato de a sociedade empresária realizar atividades preventivas e investigativas sobre eventuais crimes não é suficiente para proibir, por si só, a atividade investigativa com fulcro no mencionado art. 2º.

Primeiramente, porque se trata de uma atividade puramente interna, a fim de avaliar riscos financeiros, contratuais, de reputação e de pessoal. Impedir uma investigação sobre corrupção seria o mesmo que transformar a atividade empresarial em uma caixa preta, vedando-se ao empresário o conhecimento sobre seu funcionamento interno e externo.

E, também, porque a Lei Anticorrupção incentiva, em seu art. 7º, VIII, a implementação de auditorias, programas de integridade, criação de códigos de ética e de conduta, e canais internos de denúncias. Como consequência, tais informações colhidas poderiam ser úteis quando da realização de eventual acordo

[35] CARVALHOSA, Modesto. *Comentários à Lei de Sociedades Anônimas*. 5. ed. São Paulo: Saraiva, 2011. v. 3. p. 191.

[36] Nesse sentido, confira-se: (i) EIZIRIK, Nelson. *A Lei das S/A comentada*. São Paulo: Quartier Latin, 2011. v. 2. p. 444 e (ii) LAMY FILHO, Alfredo; PEDREIRA, José Luiz Bulhões (Coord.). *Direito das companhias*. Rio de Janeiro: Forense, 2009. v. 1. p. 1352.

de leniência, a fim de colaborar com investigações administrativas. Quaisquer informações coletadas e analisadas que possam indicar a prática de crime ou contravenção penal devem ser imediatamente comunicadas às autoridades competentes, vez que ultrapassam os interesses da investigação interna.

A Lei nº 13.432/2017 também estabelece em seu art. 6º que o investigador privado deverá agir com "técnica, legalidade, honestidade, discrição, zelo e apreço pela verdade". Também é colocada como seu dever a atuação cautelosa em relação ao contexto e ao viés das informações coletadas, visto que tal vício poderá se refletir diretamente no relatório circunstanciado a ser entregue ao final das investigações. Disso advém a importância de a sociedade empresária investir em auditorias internas ou contratar serviços externos de alta qualidade, vez que a coleta indiscriminada e desatenta de dados pode gerar resultados discriminatórios ou injustos no caso concreto.

Cumpre ressaltar que o vício pode nascer não apenas dos dados, como também do próprio planejamento da investigação. Petter Gottschalk aponta que o contratante pode solicitar a investigação com intenções ocultas, guiando o procedimento a fim de atingir um objetivo predeterminado.[37] Assim, o viés seria anterior à própria coleta de dados, visto que o meio da investigação foi construído para se atingir determinado fim. Aqui, faz-se necessário um papel ativo do próprio investigador, já que a LDP veda em seu art. 10, I a aceitação de serviços que constituam caráter discriminatório.

Por outro lado, o referido autor também observa que o relatório circunstanciado final da investigação traz consigo uma intrínseca ausência de contraditório.[38] De fato, em se tratando de investigações sigilosas, não há como impor um contraditório prévio, sob risco de fazer com que determinadas provas desapareçam ou sejam modificadas antes de o estudo começar. Entretanto, é necessário compreender que qualquer decisão tomada com base no relatório circunstanciado deve ter seus fundamentos anunciados aos investigados, independentemente de justificativa.

O processo de controle interno pode ser consideravelmente facilitado se os programas de *compliance* tiverem regulamentação específica sobre a investigação interna. Dessa forma, busca-se uma harmonização entre os interesses corporativos e a proteção de dados dos investigados, a fim de permitir que estes compreendam as finalidades das investigações corporativas, bem como tenham ciência sobre seus direitos legais e institucionais na coleta e tratamento de dados.

[37] GOTTSCHALK, Petter. Private police legitimacy: the case of internal investigations by fraud examiners. *Policing: An International Journal of Police Strategies & Management*, v. 40, n. 3, p. 6-11, 2017.

[38] GOTTSCHALK, Petter. Private police legitimacy: the case of internal investigations by fraud examiners. *Policing: An International Journal of Police Strategies & Management*, v. 40, n. 3, p. 6-11, 2017. p. 8.

3 Investigação interna e o direito à proteção de dados pessoais

A investigação interna por coleta de dados não pode ser considerada como um fim em si mesmo, de modo que deverá levar em consideração os direitos da personalidade de seus titulares. Mesmo quando coletados, armazenados, tratados e utilizados por controladores e operadores, os dados continuam pertencendo aos seus titulares originais e não comportam transferência de propriedade pela simples autorização presumida ou expressa de seu acesso por terceiros.

No ordenamento jurídico brasileiro existe farta legislação sobre o tema da proteção de dados pessoais, para além da Lei do Detetive Particular já comentada. Como exemplo, citam-se: Decreto nº 10.046/2019 sobre governança no compartilhamento de dados no âmbito da Administração Pública Federal, Decreto nº 9.854/2019 que institui o Plano Nacional de Internet das Coisas, Decreto nº 9.319/2018 que institui o Sistema Nacional para a Transformação Digital, Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), Marco Civil da Internet – MCI (Lei nº 12.965/2014) regulamentado pelo Decreto nº 8.771/2016, Lei de Delitos Informáticos (Lei nº 12.737/2012), Lei do Cadastro Positivo – LCP (Lei nº 12.414/2011) regulamentada pelo Decreto nº 9.936/2019, Lei de Acesso à Informação – LAI (Lei nº 12.527/2011), Código Civil (Lei nº 10.406/2002), Lei do *Habeas Data* (Lei nº 9.507/97), Lei de Telecomunicações (Lei nº 9.472/97) e Código de Defesa do Consumidor – CDC (Lei nº 8.078/90).

Toda a referida legislação, somada a outras com menores menções à proteção de dados, compõe o que aqui passa a se chamar de microssistema de tutela de dados. Enquanto a LGPD apresenta-se como norma geral sobre a proteção de dados, todas as outras leis do microssistema serviriam ora para regular aspectos específicos, ora para complementar normas gerais e diretrizes outras omissas na LGPD, mas aplicáveis a todas as situações sobre tutela de dados, sejam eles pessoais ou estritamente públicos.

É oportuno perceber que o desenvolvimento legislativo desse microssistema proporcionou um importante giro no fundamento da proteção de dados. Em um primeiro momento, prevalecia uma perspectiva estritamente patrimonialista com o CDC, a LCP e a Lei de Telecomunicações, nas quais o sujeito era visto como simples consumidor e a proteção de seus dados servia ao equilíbrio contratual e à privacidade como direito de não ser incomodado. Com a vigência do MCI e da LGPD, os dados pessoais são inseridos nas relações existenciais como aspectos do desenvolvimento da personalidade da pessoa humana, permitindo-se ampliar o significado de privacidade ao controle e construção das próprias informações.

O reconhecimento da existência de um microssistema de tutela de dados permite melhorar a instrumentalização sobre uma temática comum a todos os

diplomas legislativos, de modo que se potencialize a efetividade de suas normas e reste maximizada a proteção de direitos e garantias fundamentais, o que não poderia ser alcançado com uma simples interpretação autônoma da legislação. A tutela de dados precisa avançar e se expandir pelas áreas do direito, deslocando-se o Código Civil do centro de gravidade do direito privado em proveito de uma constelação de fontes normativas com novos parâmetros interpretativos.[39]

No que se refere especificamente à LGPD, cumpre destacar que não existe qualquer impedimento legal para sua aplicação às investigações privadas, apesar de posições em sentido contrário.[40] O art. 4º, III, "d" da LGPD determina sua não aplicação ao tratamento de dados pessoais realizado exclusivamente para atividades de investigação e repressão de infrações penais, enquanto o §2º do mesmo artigo permite que esse tratamento seja realizado por pessoa de direito privado, desde que sob tutela de pessoa jurídica de direito público. Todavia, não se trata de hipóteses legais direcionadas à iniciativa privada, mas à Administração Pública.

Em primeiro lugar, é necessário perceber que todas as hipóteses do referido inc. III versam sobre atividades típicas de Estado, quais sejam, segurança pública, defesa nacional, segurança do Estado e atuação contra infrações penais.[41] É necessário aplicar uma interpretação sistemática e lógica de acordo com a disposição das alíneas para se compreender a norma em questão. Além disso, o art. 2º da LDP é objetivo ao afastar a investigação de natureza criminal da atividade do investigador privado, pois trata-se de atribuição essencial e exclusiva de Estado exercida pela polícia judiciária nos termos do art. 144, §§1º e 4º da Constituição Federal de 1988 (CF/88) e do art. 2º da Lei nº 12.830/2013.

Em segundo lugar, consequentemente, não haveria que se falar de autorização prévia ou tutela concomitante de autoridade pública na realização de controle interno por investigação. O art. 4º, §2º se refere a hipóteses em que a Administração

[39] TEPEDINO, Gustavo. O Código Civil, os chamados microssistemas e a Constituição: premissas para uma reforma legislativa. *In*: GUSTAVO, Tepedino (Coord.). *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar, 2000. p. 5-6.

[40] Sustentando a aplicação do art. 4º, III, "d" e §2º, confira-se: (i) GONZALES, Nariman Ferdinan. *Compliance*: investigações internas e seus limites à luz da privacidade e da proteção de dados. Tese de conclusão de curso (Bacharel em Direito) – Faculdade de Direito da Universidade Presbiteriana Mackenzie, São Paulo, 2018. p. 48 e (ii) PAGOTTO, Leopoldo; OLIVEIRA, Naiara. Proteger dados ou combater a corrupção? *Valor Econômico*, 10 set. 2018. Disponível em: https://www.valor.globo.com/noticia/2018/09/10/proteger-dados-ou-combater-a-corrupcao.ghtml. Acesso em: 2 jul. 2020.

[41] O Considerando nº 19 do Regulamento-Geral sobre Proteção de Dados da União Europeia (Regulamento 2016/679) também prevê sua não aplicação às hipóteses de segurança pública: "A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos".

Pública contrata particulares para operar o tratamento de seus dados, ou seja, relações em que há contrato administrativo celebrado com particular e que em nada guardam relação com investigações internas feitas pela iniciativa privada.[42]

Admitir interpretação contrária, no sentido de que seria sempre necessária a tutela administrativa nas investigações privadas, causaria afronta direta ao princípio constitucional da livre iniciativa. Além disso, tratar-se-ia de interpretação contra os princípios da intervenção subsidiária e excepcional do Estado sobre o exercício de atividades econômicas e contra a inovação e adoção de novas tecnologias nos termos, respectivamente, dos arts. 2º, III e 4º, IV da Lei de Liberdade Econômica (Lei nº 13.874/2019), normas gerais de direito econômico que requerem interpretação em favor da liberdade econômica e dos investimentos na forma do art. 1º, §§2º e 4º.

Uma vez identificada a existência e a relevância de um microssistema de tutela de dados, bem como afirmada a aplicação da LGPD às investigações privadas, é preciso compreender os limites a que as atividades de controle interno estão sujeitas quando do acesso a dados pessoais, sejam eles públicos, sejam privados, a fim de se maximizar a prevenção de ilícitos sem contrariar quaisquer direitos da personalidade e fundamentais dos envolvidos.

3.1 Proteção e governança de dados pessoais

Como observa Stefano Rodotà, o conceito de privacidade não mais se submete à acepção negativa e estática do direito de ser deixado sozinho, sendo preciso compreendê-la a partir de uma perspectiva positiva e dinâmica como autodeterminação informativa, ou seja, como o direito de controlar suas próprias informações e definir a formação de sua própria esfera particular.[43] Trata-se de uma releitura do giro estritamente patrimonial da proteção de dados destinada a consumidores em relações contratuais, avançando-se a um giro existencial inserido no desenvolvimento da personalidade da pessoa humana.

Cumpre observar que a tutela de dados pessoais está diretamente relacionada à proteção das pessoas naturais como aspecto integrante de direito da personalidade, aplicando-se de forma mitigada e casuística às pessoas jurídicas. Nesse

[42] Nesse sentido, confira-se: MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 86.

[43] RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 15.

sentido, urge a observação do art. 52 do CC, o qual estabelece uma eficácia restrita dos direitos da personalidade às pessoas jurídicas, vez que se constituem de interesses notavelmente patrimoniais e nem sempre compatíveis com a tutela da personalidade. Além disso, a LGPD dispõe apenas sobre o tratamento de dados de pessoas naturais, consoante literalidade do art. 1º.[44]

Isso não quer dizer que toda e qualquer pessoa jurídica está despida de proteção sobre seus dados institucionais. Disposições sobre a proteção de informações sigilosas da companhia, como o art. 155, §1º da Lei nº 6.404/76,[45] são plenamente aplicáveis quando relacionadas à proteção de dados. Ocorre que o objetivo da proteção de dados pessoais dá um passo além, protegendo não apenas a reputação e o segredo, mas a própria personalidade do indivíduo em todos seus atributos.

Além disso, a proteção de dados pessoais está direcionada aos acionistas ou sócios e aos *stakeholders* enquanto pessoas físicas, como funcionários, administradores, diretores e outras pessoas naturais que tenham relação com a empresa. Nesse sentido, faz-se necessário atentar que, ainda que os diretores tenham seus dados colhidos e analisados como presentantes da pessoa jurídica, com ela não devem ser confundidos. O simples fato de atuar em nome de outrem não faz com que o indivíduo seja privado de seus direitos da personalidade.

Nesse sentido, o art. 50 da LGPD sugere que os agentes de tratamento adotem regras de boas práticas por meio de programa de *compliance* de dados, a fim de trazer maior segurança, transparência e qualidade ao tratamento de dados em relação aos seus titulares. Partindo do pressuposto de que os dados pessoais coletados pertencem às pessoas naturais, e não à sociedade empresária, é necessário que seu tratamento esteja fundado em diretivas internas claras e objetivas, de modo a fortalecer sua proteção e a confiança dos titulares no procedimento.

Assim, a lógica da governança em privacidade precisa ser integrada ao corpo da governança corporativa para que os programas de *compliance* alcancem uma maior efetividade, principalmente nos casos de controle interno por investigação. A todo momento são produzidos dados por acionistas, administradores, empregados, contratantes, que serão armazenados e examinados pelo empresário, a fim

[44] Art. 1º da Lei nº 13.809/2018: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

[45] Art. 155, §1º da Lei nº 6.404/76: "Cumpre, ademais, ao administrador de companhia aberta, guardar sigilo sobre qualquer informação que ainda não tenha sido divulgada para conhecimento do mercado, obtida em razão do cargo e capaz de influir de modo ponderável na cotação de valores mobiliários, sendo-lhe vedado valer-se da informação para obter, para si ou para outrem, vantagem mediante compra ou venda de valores mobiliários".

de monitorar e avaliar os riscos existentes em sua atividade; trata-se de uma consequência do exercício da empresa.

Por isso, o *compliance* de dados deve ser compreendido como mais uma ferramenta de governo da sociedade, apta a conduzir a correta aplicação e efetividade das normas protetivas de dados pessoais por parte dos agentes de tratamento, ao mesmo tempo em que mitiga as chances de danos e consequente responsabilização civil por violação aos direitos dos titulares dos dados.[46] Cumpre ressaltar que os arts. 42, §1º e 43 da LGPD preveem a responsabilidade objetiva do operador de dados, podendo responder solidariamente com o controlador que estiver diretamente envolvido no tratamento.

Dessa forma, tal qual uma atuação ética e íntegra do empresário exige a prática de controles internos, auditorias e fornecimento de canais de denúncia, a governança em privacidade estende esses direitos aos dados pessoais de seus titulares, permitindo que estes não apenas compreendam as etapas de coleta e tratamento daqueles, mas também que possam fiscalizar eventuais excessos e desvios de finalidade nas operações, ou até exigir a eliminação e correção de seus dados.

Os princípios e direitos de proteção de dados são amplamente reconhecidos em todos os diplomas legais pertencentes ao microssistema de tutela de dados, fazendo-se mister seu desenvolvimento nos códigos de conduta e programas de *compliance*. Entre essas garantias, é possível mencionar as seguintes: (i) finalidade e necessidade; (ii) transparência e segurança; (iii) qualidade e acesso do titular; (iv) atuação responsável dos agentes de tratamento.

Em primeiro lugar, os princípios da finalidade e necessidade figuram como balizadores da razoabilidade na atividade dos agentes de tratamento.[47] Enquanto a finalidade determina que o tratamento seja realizado apenas para propósitos legítimos, específicos e previamente informados ao titular, a necessidade restringe a quantidade de dados utilizados ao mínimo adequado aos objetivos do tratamento.[48] Dessa forma, uma investigação interna não poderia alcançar dados relativos

[46] FRAZÃO, Ana; OLIVA, Milena Donato; ABÍLIO, Vivianne da Silveira. Compliance de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 372.

[47] Os princípios da finalidade e necessidade encontram previsão no art. 6º, I e III da LGPD, art. 5º, V e VII da LCP e arts. 7º, VII e 16, II do MCI.

[48] É preciso que o processo de coleta e tratamento de dados seja compreensível tanto aos agentes de tratamento quanto aos titulares dos dados, eliminando ou mitigando quaisquer complexidades existentes. Do contrário, Liana Colonna identifica uma potencial incompatibilidade entre os princípios da finalidade e necessidade com exploração dos dados, de modo que os operadores coletem numerosos blocos indiscriminados de dados e sequer saibam identificar onde começa e termina o procedimento sob o argumento de que quanto mais dados, melhor (COLONNA, Liana. Data mining and its paradoxical relationship to the purpose limitation principle. *In*: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul. *Reloading data protection*. Nova Iorque: Springer, 2014. p. 312).

ao tipo sanguíneo ou a condições de saúde de um funcionário, pois ultrapassaria sua finalidade e necessidade com análise de informações desnecessárias ao fim de prevenção de ilícitos corporativos.

Em seguida, os princípios da transparência e segurança buscam resguardar a legitimidade da cadeia de valor do *big data*, desde sua coleta até seu uso.[49] A transparência materializa-se no dever que os operadores e controladores possuem de dar o máximo de informação aos titulares sobre os parâmetros e objetivos do tratamento a que estarão sujeitos seus dados pessoais. Por outro lado, a segurança requer a adoção de medidas técnicas aptas a resguardar a higidez dos dados coletados e armazenados, a fim de resguardar a intimidade e privacidade de seus titulares ao evitar vazamentos ou invasões por terceiros maliciosos.

Por sua vez, a qualidade e acesso do titular garantem a veracidade e exatidão dos dados coletados.[50] A qualidade exige que os dados coletados sejam claros, relevantes, atualizados e exatos para se atingir uma melhor utilidade em seu tratamento, enquanto o direito de acesso garante ao titular que ateste a finalidade e necessidade do tratamento, independentemente de apresentação de justificativa, podendo requerer a correção de informações equivocadas ou incompletas, bem como a eliminação de todos ou alguns dados.

A partir de uma interpretação conforme o microssistema de tutela de dados, é válido ressaltar a aplicação do art. 6º, §1º da LCP à hipótese, o qual determina ser vedada a criação de políticas ou operações que impeçam, limitem ou dificultem o acesso dos dados por seus titulares. De fato, quando do estabelecimento de programa de *compliance* é preciso que o empresário garanta o máximo de transparência e acessibilidade aos titulares dos dados, a fim de atribuir maior legitimidade e legalidade à atividade exercida sem a existência de atos aptos a configurar abuso do direito.

A situação mostra-se ainda mais delicada quando a atividade está inserida em grupo empresarial de fato ou de direito. É preciso que seja informado ao titular quais são as pessoas jurídicas legitimadas a colher, armazenar, tratar e usar seus dados pessoais quando da colheita de seu consentimento. Como a proteção de dados está fundamentada em relações jurídicas existenciais, não é possível admitir uma suposta autorização implícita em prol de todo o grupo empresarial, uma vez que a limitação dos direitos da personalidade não comporta interpretação extensiva.[51]

[49] Os princípios da transparência e segurança encontram previsão no art. 6º, VI e VII, art. 5º, IV da LCP e art. 7º, VII e do MCI.

[50] O princípio da qualidade e o direito ao acesso dos dados pelo titular estão previstos no art. 6º, V e art. 18 da LGPD, art. 5º, II, III e VI da LCP, art. 7º, VII do MCI e art. 43, *caput* e §§1º e 3º do CDC.

[51] MURAD, Raul; REQUENA, Rodrigo. Fluxo de informação no âmbito dos grupos societários e proteção dos dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 360.

Por fim, a atuação responsável dos agentes de tratamento encontra fundamento direto no art. 6º da LDP, o qual enuncia que o tratamento de dados deve ser feito de forma técnica e fundada na legalidade, honestidade, discrição, zelo e apreço à verdade. A prestação de serviços do investigador deve observar os princípios da transparência e segurança e deverá necessariamente ser registrada por escrito em relatório circunstanciado na forma dos arts. 7º e 9º da LDP.

Além disso, como os dados tratados integram o leque de direitos da personalidade de terceiros, os investigadores deverão restituir toda a base de dados fornecida quando do fim do tratamento, conforme arts. 11, VI da LDP e 16 da LGPD. Consequentemente, é vedado que todas essas informações acessadas e analisadas pelo investigador sejam divulgadas sem autorização ou que sejam utilizadas em ação contra o controlador contratante, salvo se constituir elemento de defesa na forma do art. 10, III e V da LDP.

Para além de todos os princípios e direitos mencionados, é necessário também conhecer a natureza dos dados envolvidos no tratamento, se privados ou públicos e, inclusive, se trazem informações de caráter sensível. O maior ou menor grau de acessibilidade dos dados colocará em questão a necessidade ou não de o controlador de dados receber autorização específica para coleta e tratamento, elemento suficiente para eivar todo o procedimento de ilegalidade.

3.2 O uso de dados públicos

A análise de dados voltada para o bom funcionamento dos programas de integridade depende da qualidade e quantidade das informações coletadas. Os dados são o combustível para os algoritmos e os *softwares* de processamento, de modo que quanto mais questionável for a procedência ou quanto menor for o número de insumos, pior será o resultado obtido. Não se quer com isso afirmar que a qualidade e quantidade são parâmetros isolados, mas sim mútuos. Uma grande base de dados pode conter informações enviesadas e incorretas, o que será imediatamente reproduzido nos resultados obtidos pelo algoritmo.[52]

Por outro lado, informações completas e (supostamente) neutras não terão grande valia se presentes em uma pequena base de dados, de modo a limitar o funcionamento e o alcance do algoritmo. Dessa forma, uma informação mal interpretada pode gerar graves consequências, desde a demissão injusta de um funcionário até a quebra de um contrato com determinado fornecedor, ambos por supostos "riscos"

[52] O art. 20 da LGPD identifica o direito à revisão de decisões tomadas unicamente com base em tratamento automatizado, como o procedimento realizado por inteligência artificial via algoritmos.

identificados pelo *software*. Assim, uma simples informação incorreta pode trazer impactos diretos na responsabilidade civil por eventuais danos (morais ou patrimoniais) causados ao titular dos dados.

A atividade de coleta, processamento, análise e disseminação de informações advindas de fontes abertas e legais é chamada de *Open Source Intelligence* (OSINT).[53] Com a possibilidade de ampliar as fontes de pesquisa sem deixar maiores vestígios, seu uso tem origem nas investigações criminais praticadas pelo serviço secreto americano desde 1941.[54] Exemplos comuns de OSINT são pesquisas no Google, documentos públicos, canais de notícias, sítios eletrônicos e *blogs*, redes sociais, mapas, aplicativos, processos judiciais, entre outros.

Trata-se de uma forma muito mais barata e fácil de adquirir informações, vez que tudo está amplamente disponível na internet para qualquer usuário.[55] Afasta-se desse conceito qualquer meio de investigação invasivo (*hacker*), que faça uso de ferramentas para invadir sítios eletrônicos a fim de conseguir acesso a informações privadas e sigilosas.

Dentro do universo da OSINT, também se encontra a *Social Media Intelligence* (SOCMINT), a qual visa à investigação de redes sociais abertas, como Facebook, Google+, Twitter, Instagram, YouTube, entre outros.[56] Em um momento em que cada vez mais pessoas decidem expor seus atos e opiniões na internet, as redes sociais são uma fonte farta e acessível – quando assim a política de privacidade permitir seu compartilhamento com terceiros.

Tanto a OSINT quanto a SOCMINT podem ser classificadas como formas de investigação de dados públicos com diferentes graus de acesso. Enquanto a OSINT tem direcionamento mais amplo para encontrar quaisquer informações que digam respeito a determinada pessoa, tenham sido disponibilizadas por ela ou não, a SOCMINT devassa redes sociais para encontrar dados tornados públicos pela livre vontade do investigado.

A temática dos dados públicos encontra previsão no art. 7º, §§2º e 3º da LGPD, os quais propõem a seguinte divisão: dados manifestamente públicos e dados de acesso público, mas não delimita seus respectivos conceitos. Segundo Bruno Ricardo Bioni, a diferença entre ambos residiria no fato de os primeiros serem disponibilizados por iniciativa do próprio titular, como um perfil aberto em rede

[53] SCHAURER, Florian; STÖRGER, Jan. The Evolution of Open Source Intelligence (OSINT). *Journal of U.S. Intelligence Studies*, v. 19, n. 3, p. 53-56, 2015.

[54] WILLIAMS, Heather; BLUM, Ilana. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. Santa Monica: RAND Corporation, 2018.

[55] EIJKMAN, Quirine; WEGGEMANS, Daan. Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? *Security and Human Rights*, v. 23, n. 4, p. 285-296, 2013.

[56] SCOTT, Jeramie. Social media and government surveillance: the case for better privacy protections for our newest public space. *Journal of Business & Technology Law*, v. 12, n. 2, 2017. p. 153.

social, enquanto os segundos são divulgados por iniciativa de terceiros, como dados constantes na base de dados do Poder Judiciário.[57] Em suma, trata-se de classificação que se adequa aos objetivos da OSINT (dados de acesso público) e da SOCMINT (dados manifestamente públicos).

Dentro dessa dicotomia, o art. 7º, §3º da LGPD faz referência apenas aos dados manifestamente públicos como hipótese de dispensa de autorização do titular para tratamento, mas tal dispositivo deve ser interpretado como se fizesse referência aos dados públicos em sentido lato. Isso, porque o legislador não delimitou diferença entre referidas espécies de dados públicos, e condicionar a autorização ou não à origem da disponibilização da informação pode trazer dúvidas desnecessárias ao caso concreto. Impor ao investigador que colha autorizações de cada dado público tratado implica altos custos à atividade, bem como traz riscos consideráveis ao sigilo de um procedimento preventivo.

Além disso, o fato de os dados terem acesso público não significa que podem ser utilizados ao bel-prazer dos agentes de tratamento, pois, afinal, ainda constituem parte integrante do direito da personalidade de seus titulares. Nesse sentido, o mencionado art. 7º, §3º determina que o tratamento desses dados deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização por terceiros ou pelo próprio titular. É necessário compreender o contexto em que a informação foi tornada publicamente acessível, de modo que a evitar uma investigação baseada em dados excessivos e que escapam da finalidade das práticas de governança.

Por exemplo, ainda que o Poder Judiciário divulgue em sua base de dados informações sobre ações de direito de família (*v.g.*, alimentos, guarda, investigação de paternidade, divórcio), disso não decorre que serão úteis à investigação e precisarão necessariamente ser incorporados ao tratamento. Não é razoável que uma investigação interna corporativa trabalhe com dados relativos à intimidade familiar do investigado, alcançando informações como tipo sanguíneo e outras informações de saúde, dado genético, relação (extra) conjugal, convicção religiosa ou sexualidade – dados tipicamente classificados como sensíveis pelo art. 5º, II da LGPD.

Entretanto, disso não decorre que as investigações internas estão proibidas de colher e tratar dados pessoais sensíveis, mas tão somente que esses dados precisarão estar adequados às finalidades e necessidades do procedimento. Por exemplo, dados referentes à convicção religiosa, opinião política ou filiação a determinada entidade podem levar o investigador a identificar relações entre agentes (*v.g.*, ato fraudulento entre membros ligados a partido político) ou os motivos determinantes do ato ilícito.

[57] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 379.

Não é possível trabalhar com uma negativa cabal ao tratamento de dados pessoais sensíveis e públicos no controle interno, sob risco de se retirar peças fundamentais de qualquer investigação a ser realizada. Deve-se realizar um juízo de necessidade e adequação em relação aos dados disponíveis, ponderando se o contexto de sua disponibilidade traz alguma utilidade aos fins do tratamento. Afinal, os dados pessoais públicos não podem ser considerados como propriedade abandonada disponível a todos que o encontrarem, presumindo-se que seu titular concedeu autorização para uso amplo e irrestrito por qualquer pessoa.[58]

Nesse sentido, o art. 7º, §§4º e 6º da LGPD reitera que todos os direitos e princípios de tutela de dados são plenamente aplicáveis, garantindo-se, assim, a tutela da pessoa humana independentemente da natureza e acessibilidade de seus dados pessoais, pois integrantes de sua personalidade. Por esse motivo, o art. 18, §2º da LGPD determina que, nos casos de violação à legislação, o titular pode se opor ao tratamento realizado por hipótese de dispensa de autorização, como a presente hipótese de dados pessoais públicos. É perfeitamente possível equilibrar publicidade com privacidade, desde que resguardadas as garantias fundamentais do microssistema como freio ao abuso do direito.

3.3 O uso de dados privados

Em simples comparação com os dados pessoais públicos, os dados pessoais privados possuem maior valor ao processo de tratamento em razão de sua escassez e acessibilidade reduzida, garantindo resultados mais objetivos e compreensíveis no controle interno. Entre os diversos meios disponíveis para a coleta desses dados em sede de investigação interna, podem-se mencionar, entre outros: *e-mail*, telefone e veículo corporativos, histórico de acesso na internet, *keylogger*,[59] *spyware*,[60] câmeras e microfones.

Tanto os dados públicos quanto os privados estão sujeitos ao regime do microssistema de tutela de dados, de modo que os agentes de tratamento deverão

[58] Nesse sentido, confira-se lição de Anderson Schreiber: "A tolerância com essa coleta não implica, contudo, em alienação do dado pessoal. Vale dizer: os dados pessoais não põem ser tratados como bens patrimoniais, que, uma vez fornecidos, podem ser livremente utilizados pelo destinatário ou retransmitidos para quem quer que seja" (SCHREIBER, Anderson. *Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014. p. 141).

[59] *Keylogger* é um programa (ou aplicativo) oculto instalado para identificar e registrar tudo o que é digitado no teclado de um computador e demais dispositivos, a fim de transmitir todas essas informações a fontes externas.

[60] *Spyware* é um programa (ou aplicativo) oculto para espionagem de computadores e outros dispositivos, a fim de coletar dados sobre histórico e atividades *on-line* para posteriormente transmitir tais informações a fontes externas.

observar a finalidade e necessidade do tratamento, bem como respeitar a privacidade de seus titulares. Por outro lado, os dados privados aumentam a relevância da privacidade diante de sua acessibilidade restrita para coleta e tratamento, os quais dependerão, como regra, do consentimento dos titulares.

Nesse sentido, o respeito à privacidade, além de ser considerado como direito fundamental no art. 5º, X da CF/88, é elencado no microssistema como: (i) dever do investigador no art. 11, II da LDP; (ii) fundamento da proteção de dados pessoais no art. 2º, I da LGPD; (iii) condição para o pleno exercício do direito de acesso à internet no art. 8º do MCI e (iv) direto inviolável no art. 21 do CC. Além disso, considerando que o art. 60, §1º da Lei de Telecomunicações prevê a transmissão e recepção de informações como telecomunicação, bem como o art. 69, parágrafo único aponta a comunicação de dados como forma de telecomunicação, seria possível também aplicar às investigações internas por análise de dados seu art. 3º, IX, o qual garante ao titular de dados não só o respeito à sua privacidade, como também transparência na utilização de seus dados pessoais.

Apesar da questionável redação do art. 11 do CC,[61] a privacidade como direito da personalidade encontra fundamento legal no microssistema para sua limitação voluntária por meio do consentimento. Apesar de o art. 7º, I da LGPD fazer menção apenas ao consentimento para o tratamento de dados, tal dispositivo deve ser interpretado conjuntamente com o art. 7º, IX do MCI que também o exige para coleta, uso e armazenamento. Dessa forma, o consentimento deve ser considerado como regra em toda a cadeia de valor do *big data*.

Na forma dos arts. 5º, XII e 8º da LGPD, o consentimento pode ser escrito ou não e deve constituir manifestação livre, informada, inequívoca e direcionada a uma finalidade determinada, sendo nulas as autorizações genéricas; se realizado por escrito, deve estar destacado das demais cláusulas contratuais. Além disso, deve ser reservado ao titular o direito de revogar seu consentimento a qualquer tempo via simples manifestação expressa.

Ocorre que, em uma primeira análise, a atividade investigativa de controle interno deve ser realizada com a discrição e sigilo necessários a uma coleta e tratamento de dados corretos e objetivos, uma vez que a ciência do investigado sobre uma inspeção contra si provocaria uma mudança de comportamento atípica e apta a comprometer toda a efetividade do procedimento. Por isso, seria questionável

[61] O art. 11 do CC classifica os direitos da personalidade como irrenunciáveis, sendo permitida sua limitação voluntária apenas nos casos previstos em lei; mas a doutrina civilista tende a amenizar a literalidade do dispositivo, garantindo a livre limitação dos direitos por seus titulares, desde que não se dê de forma permanente ou geral. Por todos, confira-se: TEPEDINO, Gustavo; BARBOZA, Heloisa Helena; MORAES, Maria Celina Bodin. *Código Civil interpretado conforme a Constituição da República*. 3. ed. Rio de Janeiro: Renovar, 2014, v. 1, p. 34.

exigir que a sociedade empresária dependesse de constante autorização dos investigados para análise de seus dados, especialmente pelo fato de o tratamento estar voltado para fins éticos e de integridade exigidos (ou incentivados) pela legislação nacional e internacional.

Nesse sentido, o art. 7º, IX da LGPD dispensa o consentimento no tratamento de dados (e não na coleta) quando for necessário ao atendimento de interesses legítimos do controlador, salvo se prevalecerem direitos e liberdades fundamentais no caso concreto. A noção de o que seriam "interesses legítimos" não é aprofundada pelo legislador, que se limita a trazer um rol exemplificativo de apenas duas atividades no art. 10, quais sejam: (i) apoio e promoção de atividades do controlador e (ii) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem.

O controle por investigação interna dos programas de *compliance* pode ser considerado como hipótese do art. 10, I da LGPD como atividade que apoia e promove a função social da empresa ao prevenir e coibir atos fraudulentos, sendo inclusive reconhecida nas já mencionadas Lei Anticorrupção, Estatuto das Estatais e Lei de Prevenção à Lavagem de Dinheiro, além de incentivadas pela Administração Pública via decretos ou atos administrativos de agências reguladoras e outros órgãos.

A expressão "interesses legítimos" pode ainda ser encontrada nos Considerandos nºs 47 a 50 do Regulamento Geral sobre a Proteção de Dados da União Europeia (Regulamento 2016/679), legislação essa que teve impacto significativo na redação da LGPD brasileira.[62] A legislação europeia também não delimita o conceito do termo, mas elenca como exemplo no Considerando nº 47 a hipótese em que titular dos dados está ao serviço do responsável pelo tratamento e, mais especificamente, quando o tratamento for necessário aos objetivos de prevenção e controle de fraude.[63]

Essa ponderação de interesses pode ser diretamente extraída do mencionado art. 7º, IX na medida em que condiciona a validade do legítimo interesse ao não prevalecimento de direitos e liberdades fundamentais. Para Ricardo Bioni, essa regra interpretativa deve passar por quatro etapas essenciais: (i) verificação da legitimidade do interesse e inexistência de vedação legal expressa; (ii) necessidade do tratamento de dados e inexistência de fundamento legal que não a do

[62] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 324-325.

[63] No mesmo sentido: (i) BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 331-334; (ii) BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 277 e (iii) MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 9, 2016. p. 40.

interesse legítimo; (iii) consideração das legítimas expectativas do titular dos dados e dos impactos em sua privacidade; (iv) transparência e minimização de riscos no procedimento.[64] Ao mesmo tempo, esse exercício de proporcionalidade pode ser atingido a partir da perspectiva do abuso do direito, considerando-se também a boa-fé, os princípios e os fins sociais e econômicos envolvidos no exercício do direito subjetivo.[65]

Dentro desse exercício de ponderação, o consentimento informado deve ser compreendido como a regra do microssistema de tutela de dados, a fim de garantir maior transparência ao procedimento. É preciso que aqueles que elaboram e executam o programa de *compliance* levem em consideração que os dados coletados integram a autodeterminação informativa de seus titulares, de modo que somente devem ser colhidos, armazenados, tratados e usados os dados estritamente relacionados com a finalidade de prevenir e identificar ilícitos e em quantidade necessária para tal fim. Com isso, resgata-se a tutela existencial como fundamento da proteção de dados, ao revés de uma leitura estritamente patrimonial e aquém da função social.

Esse é o motivo da relevância do já mencionado art. 50 da LGPD, o qual sugere que os controladores e operadores estabeleçam regras de boas práticas e de governança sobre tratamento de dados e privacidade. A prevenção e combate a atos ilícitos não é de interesse restrito da companhia, mas também de toda a sociedade e principalmente daqueles que são diretamente impactados pela atividade econômica exercida, como trabalhadores, administradores, sócios e acionistas, terceiros contratantes. A atividade de controle interno não é um fim em si mesmo e, por isso, não deve privilegiar o interesse da companhia ao sacrifício de direitos e garantias fundamentais. Um programa de investigação interna somente será completo se as práticas de governança corporativa também incorporarem práticas de governança de privacidade, garantindo maior transparência e participação no procedimento.

É importante ressaltar que existe outra hipótese no art. 7º, II da LGPD que pode permitir a supressão do consentimento no tratamento de dados: cumprimento de obrigação legal ou regulatória pelo controlador. Ao contrário da dispensa por interesses legítimos, essa hipótese também abrange o tratamento de dados pessoais sensíveis sem consentimento na forma do art. 11, II, "a" da LGPD. Cumpre

[64] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 327-330.

[65] BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 276.

ressaltar que essa hipótese pode gerar distorções na avaliação de riscos e, inclusive, na concorrência.

Isso, porque não são todas as atividades econômicas que têm como obrigação legal ou regulatória a adoção de programas de *compliance* e controle interno. Como já mencionado, as empresas estatais são obrigadas por lei a adotar boas práticas de governança corporativa, assim como as instituições financeiras e companhias por determinação do Bacen e da CVM, respectivamente. Enquanto isso, às demais sociedades empresárias aplicam-se as Leis Anticorrupção e de Prevenção à Lavagem de Dinheiro, que apenas incentivam a adoção de integridade como medidas atenuantes a ilícitos praticados. Admitir que uma companhia aberta ou empresa estatal tenham maiores ferramentas para análise e controle de riscos via controle de dados pessoais (inclusive os de natureza sensível) em detrimento de outras sociedades empresárias atuantes no mesmo mercado importaria em desequilíbrio injustificado na concorrência.

Dessa forma, é necessário que o art. 7º, II seja interpretado em favor da liberdade econômica e dos investimentos, conforme preceitua o art. 1º, §2º da Lei de Liberdade Econômica, sem desconsiderar a natureza existencial dos titulares de dados. Assim, é possível adotar uma das seguintes interpretações: (i) o dispositivo é aplicável a todas as sociedades empresárias, vez que o incentivo da Lei Anticorrupção se considera como obrigação legal à luz da função social da empresa e dos preceitos éticos envolvidos; (ii) o dispositivo não é aplicável às obrigações legais ou regulatória de adoção de programas de integridade, uma vez que a legislação não comina obrigação de investigação via análise de dados pessoais.

Independentemente da incidência do art. 7º, II ou IX da LGPD, é recomendável que seja colhido consentimento dos titulares dos dados diante da incerteza na eventual interpretação judicial ou arbitral, ou, ao menos, que seja dada ciência inequívoca ao titular por meio da implementação dos códigos internos de governança corporativa (e de privacidade). É preciso que todos os titulares saibam que seus dados podem ser coletados e tratados para uso de controle interno e, mais do que isso, deve-se trabalhar com o máximo de informações que esclareçam as finalidades do procedimento, bem como os direitos e garantias legais e institucionais envolvidos.

A premissa ora colocada sobre a potencial perda de eficiência da investigação pelo conhecimento do investigado não se sustenta, pelo simples motivo de que as autorizações deverão ser dadas no momento da formação do contrato, seja ele com empregado, administrador ou terceiros. Ou seja, estabelece-se o pressuposto de que todas as relações institucionais poderão ser monitoradas para fins de investigações de controle interno. Um consentimento colhido no início da relação jurídica não pode ser equiparado àquele colhido mediante informação de que

existem suspeitas de ilícitos contra o titular. É imprescindível que todos os titulares tenham ciência de que seus dados podem ser coletados e tratados para fins específicos e predeterminados, do contrário ocorreria violação à privacidade por inexistência de limitação voluntária na forma do art. 11 do CC.

Com isso, é preciso que o ambiente corporativo seja estabelecido como tal pelos programas de integridade, de modo a separar o ambiente de trabalho da noção de vida privada. Eventual fornecimento de *e-mail*, telefones e veículos corporativos deve ser acompanhado de diretrizes internas claras e objetivas que estabeleçam seu uso estritamente para o trabalho. O mesmo se aplica em relação aos servidores de internet, cabendo ao empregador informar sobre eventual monitoramento e que somente será admitido o uso dos computadores da companhia para atividades estritamente corporativas.

Cumpre apontar que a LGPD é silente em relação ao tratamento de dados na relação de emprego, os quais seguirão suas normas gerais. O Regulamento Geral Europeu também não regulamenta o tema, limitando-se a permitir em seu art. 88 que os Estados-Membros elaborem normas específicas que resguardem a transparência do tratamento de dados e regulem a transferência de dados pessoais dentro de grupo empresarial.

A Alemanha pode ser apontada como país que regulamenta o tratamento de dados na relação de trabalho. Segundo sua Lei de proteção de dados (*Bundesdatenschutzgesetz* – BDSG), o tratamento de dados de empregados em sede de investigação interna somente se dará quando sobre eles recair suspeita fundada e documentada. Ademais, seu livre consentimento ao tratamento deve ser analisado de acordo com as circunstâncias do caso, vez que a relação de trabalho estaria pautada por uma dependência em face do empregador. Esse tema foi, inclusive, discutido no Processo AZR 681/16 pelo Tribunal Federal do Trabalho alemão (*Bundesarbeitsgericht* – BAG), o qual entendeu ser vedado que empregadores monitorem empregados com programas de *keylogger* se não houver suspeita fundada de ilícito, sob risco de afronta à sua autodeterminação informativa.

Apesar de coerente, referida decisão do BAG alemão aparenta não se atentar aos avanços tecnológicos nos métodos de investigação. Isso, porque não necessariamente o monitoramento será realizado por uma pessoa ou grupo de pessoas em face de um suspeito específico, mas também por meio de inteligência artificial e algoritmos que coletam e analisam dados pessoais indiscriminadamente, com o fim de prevenir ilícitos e identificar comportamentos suspeitos (*red flags*).

A investigação por meios automatizados garante uma maior objetividade e imparcialidade na colheita dos dados, ao mesmo tempo em que elimina potenciais enviesamentos na escolha do alvo, já que todos serão monitorados. Em caso de erro ou dúvida nas conclusões da inteligência artificial, o investigado poderá

solicitar revisão das decisões tomadas com base no tratamento de seus dados, bem como obter informações sobre os critérios e procedimentos utilizados na forma do art. 20, *caput* e §1º da LGPD.

De qualquer modo, as atividades de controle interno encontram fundamento nos denominados poderes diretivo e fiscalizatório, os quais constituem conjunto de prerrogativas do empregador para organizar, acompanhar e fiscalizar a estrutura do estabelecimento empresarial por meio da especificação e orientação cotidianas relativas à prestação do trabalho.[66] Trata-se de ato legítimo do empregador, especialmente diante de sua responsabilidade por ato de seus empregados contra terceiros (art. 932, III do CC), mas que não possui caráter absoluto e precisa fundamentar seu legítimo interesse a partir de um equilíbrio proporcional com a autodeterminação informativa dos seus titulares.[67]

É recomendável que as diretrizes dos poderes diretivos e fiscalizatórios na investigação interna sejam incorporadas ao contrato de trabalho desde sua formação ou, ao menos, sejam objeto de convenção coletiva ou acordo coletivo de trabalho (art. 611-A, VI da Consolidação das Leis do Trabalho – CLT). Do contrário, essas novas práticas de controle interno podem ser configuradas como alteração contratual que exigirão mútuo consentimento e prova de inexistência de prejuízos diretos ou indiretos ao empregado na forma do art. 468 da CLT. Mesmo que se decida por não incorporar as normas do programa de *compliance* ao contrato de trabalho, estas poderão ser interpretadas como alteração contratual conforme Súmula nº 51, I do TST. Por isso, apesar de se tratar de prerrogativa do empregador, é imprescindível que seja maximizada a transparência no procedimento.

O Tribunal Superior do Trabalho (TST) vem se mostrando favorável ao exercício do poder diretivo e fiscalizatório do empregador no monitoramento de seu estabelecimento, desde que estritamente relacionado aos fins corporativos. Em relação ao *e-mail* corporativo, a 1ª Turma já reconheceu que sua fiscalização não afronta a inviolabilidade do sigilo de correspondência ou de comunicações telegráficas, desde que declaradamente destinado apenas para assuntos afetos ao trabalho, uma vez que o servidor e os computadores constituem propriedade do empregador.[68] O Superior Tribunal de Justiça possui

[66] DELGADO, Mauricio Godinho. *Curso de direito do trabalho*. 18. ed. São Paulo: LTr, 2019. p. 792; 795.

[67] LION, Maurício Pepe. Condução de investigações internas sob o ponto de vista trabalhista. *In*: DEL DEBBIO, Alessandra; MAEDA, Bruno Carneiro; AYRES, Carlos Henrique da Silva (Coord.). *Temas de Anticorrupção & Compliance*. Rio de Janeiro: Elsevier, 2013. p. 306-308.

[68] "PROVA ILÍCITA. 'E-MAIL' CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO. [...] 4. Se se cuida de 'e-mail' corporativo, declaradamente destinado somente para assuntos e matérias afetas ao serviço, o que está em jogo, antes de tudo, é o exercício do direito de propriedade do empregador sobre o computador capaz de acessar à INTERNET e sobre o próprio provedor. [...] 5. Pode o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em 'e-mail' corporativo, isto é,

entendimento semelhante em relação aos funcionários públicos e à Administração Pública.[69]

O *e-mail* corporativo é parte integrante do estabelecimento empresarial da sociedade empresária e, conforme diretrizes de governança corporativa interna, precisam ser utilizados exclusivamente para o desempenho do trabalho. O mesmo raciocínio pode ser aplicado à fiscalização de telefones corporativos, ao monitoramento georreferenciado de veículos corporativos e à instalação de *spywares* e *keyloggers* nos computadores do empregador, desde que haja ciência inequívoca de seu uso para fins privados. Dessa forma, prioriza-se o interesse legítimo do empregador e afasta-se qualquer argumentação sobre privacidade e intimidade na prestação de serviços, resguardados os direitos e garantias dos titulares e respeitados os princípios da finalidade e necessidade do tratamento.

A 1ª e 2ª Turmas do TST também possuem julgado no sentido de considerar a gravação ambiental das atividades dos empregados por meio de câmera como inseridas no poder diretivo e fiscalizatório do empregador. Para tanto, seria necessário que houvesse ciência e autorização específica por parte dos empregados, bem como não houvesse monitoramento em locais de repouso que expusessem sua privacidade e intimidade, como banheiros e vestiários.[70] A princípio, também seria permitida a investigação por câmeras com reconhecimento facial e microfones para fins exclusivamente necessários ao controle interno, desde que a tecnologia não seja utilizada como ferramenta discriminatória – como pressupor personalidades e comportamentos por expressão facial e etnia.

Por fim, existem situações em que não é tão fácil separar o ambiente corporativo do privado, como quando o empregado trabalha com seus próprios dispositivos no ambiente de trabalho (prática conhecida como *bring your own device* – BYOD ou *wear your own device* – WYOD) ou quando presta seus serviços a partir de sua residência em *home office*. Nessas situações, o empregador continua assumindo exclusivamente o risco da atividade, mas o juízo de proporcionalidade

checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5º, incisos X, XII e LVI, da Constituição Federal" (TST, 1ª T. RR nº 61300-23.2000.5.10.0013. Rel. Min. João Oreste Dalazen, j. 18.5.2005).

69 Confira-se trecho da ementa: "Não configura prova ilícita a obtenção de informações constantes de e-mail corporativo utilizado pelo servidor público, quando atinentes a aspectos não pessoais, mas de interesse da Administração Pública e da própria coletividade; sobretudo quando há expressa menção, nas disposições normativas acerca do seu uso, da sua destinação somente para assuntos e matérias afetas ao serviço, bem como advertência sobre monitoramento e acesso ao conteúdo das comunicações dos usuários para fins de cumprir disposições legais ou instruir procedimento administrativo" (STJ, 2ª T. RMS nº 48.665. Rel. Min. Og Fernandes, j. 15.9.2015).

70 Confira-se: (i) TST, 1ª T. RR nº 21162-51.2015.5.04.0014. Rel. Min. Hugo Carlos Scheuermann, j. 28.8.2020 e (ii) TST, 2ª T. RR nº 44900-19.2012.5.17.0012. Rel. Min. Delaíde Miranda Arantes, j. 23.8.2019.

tende à privacidade do empregado a partir do momento em que um mesmo aparelho é usado para fins privados e corporativos.

Não é razoável que o empregador tenha acesso irrestrito aos aparelhos de seus empregados, pois isso significaria investigar atos privados sem qualquer relação com o ambiente de trabalho como histórico da internet e *e-mail* particular. Além disso, eventual consentimento fornecido pelo empregado (e inclusive por administradores, diretores e outros *stakeholders* sob regime de direito empresarial ou civil) seria absolutamente questionável, pois patente o impacto da dependência econômica e subordinação na livre manifestação de vontade – afinal, a negativa poderia ensejar a rescisão contratual.

O InterGuard é um exemplo de várias outras ferramentas disponíveis *on-line* para acesso remoto de aparelhos privados, permitindo a coleta de dados a partir de histórico de acesso, fotos, mensagens de texto, histórico de chamadas, geolocalização e monitoramento de aplicativos como Skype, WhatsApp, Tinder e Instagram.[71] Contudo, trata-se de atividade que extrapola os limites razoáveis do legítimo interesse e dos poderes diretivos do empregador, podendo, inclusive, configurar conduta típica do crime de invasão de dispositivo informático (art. 154-A, *caput* e §3º do Código Penal).[72]

Os programas de *compliance* precisam regulamentar o uso de aparelhos próprios na prestação do serviço antes de autorizar sua prática, considerando aspectos de transparência e segurança. Por exemplo, seria possível que o empregador condicionasse o BYOD ou *home office* ao *download* de *softwares* ou aplicativos de coleta remota de dados e que permitissem o acesso do empregado ao servidor do ambiente de trabalho. Recomenda-se também a previsão de que a conexão à internet se dê por meio de rede virtual privada (*virtual private network* – VPN), a fim de evitar que terceiros maliciosos invadam dados pessoais e corporativos, visto que os aparelhos pessoais podem não possuir o mesmo nível de segurança daqueles do empregador.[73]

[71] Disponível em: https://www.interguardsoftware.com/employee-cell-phone-monitoring/.

[72] "Art. 154-A do Código Penal. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. [...] §3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave".

[73] MAVRETICH, Robert. Legal issues within corporate "bring your own device" programs. *SANS Institute*, 2012. Disponível em: https://www.sans.org/reading-room/whitepapers/legal/legal-issues-corporate-bring-device-programs-34060. Acesso em: 2 jul. 2020.

Cumpre observar que, caso se decida pela implementação de *softwares* e aplicativos, estes precisam atender a padrões aceitáveis de segurança no armazenamento de dados, além de utilizar métodos lícitos e previamente informados de coleta dos dados necessários às finalidades do programa de integridade. Dessa forma, não pode ser admitido que essas ferramentas estejam constantemente ativas no dispositivo para monitorar acesso à internet, *e-mail* privado e outras atividades da vida privada desenvolvidas fora do contexto da prestação de serviços.

Conclusão

A investigação interna por coleta e análise de dados pessoais é uma importante ferramenta na implementação dos programas de integridade em sociedades empresárias. Conhecer melhor o perfil de *stakeholders* como funcionários e administradores permite uma melhor avaliação dos riscos, de modo a saber sobre a existência de um desvio de conduta ou probabilidade de ele acontecer na prática. Com isso, além de evitar as duras sanções legais como aquelas previstas na Lei Anticorrupção, o empresário fortalecerá sua confiança e reputação no mercado em que está inserido.

Ocorre que, ao mesmo tempo em que a investigação via análise de dados proporciona grandes benefício e eficiência, também pode abrir margem ao desrespeito a direitos da personalidade dos investigados. O fato de os dados pessoais estarem amplamente acessíveis não significa que os investigadores possuam legitimidade para analisá-los de forma irrestrita e sem prazo determinado, tampouco que um excesso de informações trará resultados melhores e mais precisos.

É preciso reconhecer que cada um dos elementos coletados diz respeito não apenas à vida privada de um indivíduo, mas também à sua autonomia sobre o controle de suas próprias informações enquanto autodeterminação informativa. A discussão não pode se encerrar na máxima simplista de que o que é acessível é necessariamente público. Deve-se superar a presente fase de consentimento desinformado, em que usuários aceitam longos termos e condições de privacidade sem realmente conhecer as condições às quais está se submetendo, principalmente em situações em que há nítida dependência econômica na relação jurídica.

Por isso, é necessário que as sociedades empresárias repensem seus programas de *compliance* para neles incluírem aspectos de governança sobre proteção de dados. Com isso, é garantida uma maior transparência no ciclo de valor dos dados com uma regulamentação precisa sobre o procedimento de investigação e os respectivos direitos dos titulares, de modo a maximizar a figura do consentimento informado na prática. A integridade da sociedade empresária é um

aspecto fundamental no exercício da empresa, mas não pode ser tomada como um fim em si mesmo, ao arrepio de sua função social e dos direitos da personalidade das pessoas investigadas.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

GONÇALVES, Vitor Gabriel de Moura; Leonardo da Silva Sant'Anna. Aspectos legais da investigação interna por análise de dados nos programas de compliance. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 33, n. 1, p. 17-50, jan./mar. 2024. DOI: 10.33242/rbdc.2024.01.002.

Recebido em: 07.01.2021
Aprovado em: 28.04.2021