DIREITO & TI
ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Risco ou trust and safety? Balizas jurídicas no enfrentamento a fraudes digitais no Brasil

Risk or trust and safety? Legal guidelines when addressing digital fraud in Brazil

Paulo Ricardo Aguiar de Deus[1]

Recebido em: 19.01.2025
Aprovado em: 15.04.2025

RESUMO

O artigo analisa os mecanismos jurídicos que sustentam o enfrentamento do crescente problema das fraudes digitais no Brasil, abordando também os meios pelos quais os controladores de dados agem para se prevenir e investigá-las, consoante a Lei Geral de Proteção de Dados nacional. Por meio de metodologia exploratória e técnica de interpretação dedutiva e indutiva, foi possível apresentar uma definição normativa de fraude, suas características jurídicas e implicações no direito brasileiro. A partir disso, foi distinguida a atuação nas empresas da emergente área de Trust and Safety, que visa proteger usuários e garantir a segurança no seu uso de plataformas digitais, em contraste com a tradicional área de gerenciamento de risco, que foca na proteção dos ativos corporativos. Além disso, a pesquisa discute a importância da incidência da correta hipótese de tratamento de dados pessoais, inclusive sensíveis, no combate a fraudes, o que pode variar a depender da natureza da equipe atuando no caso concreto. A pesquisa contribui para o campo jurídico ao propor uma análise integrada da incidência legislativa e das práticas e necessidades empresariais no combate a fraudes digitais no Brasil.

Palavras-chave: Gerenciamento de risco; investigação; prevenção a fraude; Trust and Safety.

ABSTRACT

The paper examines the legal mechanisms that support the fight against the growing issue of digital fraud in Brazil, also exploring how data controllers respond to prevent and investigate such fraud under the national General Data Protection Law. Through an exploratory methodology and deductive and inductive interpretation techniques, it was possible to present a normative definition of fraud, its legal characteristics, and implications in Brazilian law. Based on this, the study distinguishes the work of the emerging area of Trust and Safety in companies, which aims to protect users and ensure their safe use of digital platforms, from the traditional area of risk management, which focuses on safeguarding corporate assets. Furthermore, the research discusses the importance of applying the appropriate legal basis for processing personal data, including sensitive data, in combating fraud, which may vary depending on the nature of the team handling the specific case. This research contributes to the legal field by proposing an integrated analysis of legislative application and the business practices and needs in combating digital fraud in Brazil.

Keywords: Risk management; investigation; fraud prevention; Trust and Safety.

[1] Advogado, bacharel e especialista em direito pela UniProcessus. Doutorando em direito digital e mestre em direito processual penal pelo UniCEUB. ORCID: https://orcid.org/0000-0002-9695-7186. prdeus@gmail.com. Lattes: http://lattes.cnpq.br/2396711142206387.

1 INTRODUÇÃO

De maneira geral, o sentimento de preocupação com a criminalidade sempre está em alta na sociedade. Uma pesquisa continuada conduzida há mais de dez anos pela Ipsos (2024) em 29 países indica que criminalidade e violência é a terceira maior preocupação de mais de 20 mil adultos em todo o mundo (pontuando 29%), antecedido apenas pelas preocupações com a pobreza e desigualdade social, em segundo lugar (com 31%), e pela inflação, em primeiro (com 32%). No Brasil, segundo uma pesquisa semelhante conduzida pela Quaest (Martins, 2024), a violência encontra-se em uma tendência crescente, ocupando o segundo lugar (19%), apenas perdendo para a economia (21%). Os resultados de ambas as pesquisas são do ano de 2024.

Com o rápido desenvolvimento da tecnologia, é possível perceber uma migração paulatina da criminalidade do mundo real para o mundo virtual, de maneira que os estelionatos virtuais já superam, em números, os crimes de roubo (FBSB, 2024, p. 96-99). Essa migração sofreu uma aceleração exponencial durante a pandemia, e continua crescendo gradualmente, segundo a TransUnion (2023) em seu Relatório Global sobre Tendências de Fraude Digital Omnichannel 2023. Nesse relatório foi identificado um aumento de 80% na tentativa de fraudes de 2019 a 2022, enquanto no Brasil o índice foi de 144% para transações digitais.

Para se ter uma noção concreta desse impacto no Brasil, num outro relatório produzido pelo Visa (2023), e baseado em dados de mais de 2,7 bilhões de transações globalmente, apontou que o índice de risco de fraudes no Brasil atingiu 14,24%, posicionando o país em segundo lugar, pouco atrás da China com 14,93%. O alento é saber que o sucesso nessas tentativas é baixo, pontuando 2,44% em todas as indústrias. Bons processos e equipes bem treinadas no combate a fraudes são fundamentais para manutenção desse resultado, em especial quando se constata que o aumento de crimes digitais não é transitório, mas uma verdadeira tendência.

Nesse sentido, o tratamento de dados é indubitavelmente uma questão da maior importância quando o assunto são as fraudes no atual mundo globalizado e digital. Dados

têm se tornado objeto de interesse tanto dos criminosos quanto de empresas em suas operações legítimas, e são o novo campo de batalha das relações econômicas. A preocupação com esse tema é tão grande que há 40 anos tem sido objeto de regulações cada vez mais sofisticadas e complexas em todo o mundo (Greenleaf, 2011). No Brasil, o tema foi abordado pela Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados – LGPD, com franca inspiração no Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR) da União europeia (Lorenzon, 2021).

Dessa forma, esta pesquisa se propõe a responder a seguinte pergunta: quais são fundamentos jurídicos em que as equipes de investigação a fraudes podem se apoiar em sua atividade? O tema é da maior importância não apenas pelo que foi possível apresentar no que tange à dimensão desse tipo de crime nacionalmente, mas também porque não é uma perspectiva comumente explorada academicamente no Brasil, mesmo apesar do seu impacto e relevância tanto no país quanto internacionalmente.

A pesquisa traçará em linhas gerais como esse enfrentamento se dá no Brasil, bem como será possível explorar o arcabouço jurídico que apoia legalmente essas ações. Para percorrer tais questões, será empregue metodologia exploratória em livros, artigos e pareceres produzidos no Brasil e União Europeia, como dito, inspiração primeira para a LGPD. Serão empregados, ainda, os métodos dedutivos e indutivos para analisar e cotejar diferenças entre a LGPD e a GDPR.

Para tanto, a primeira parte desta pesquisa conceituou termos elementares para seu desenvolvimento, definindo normativamente as chamadas fraudes e suas características. A segunda parte se focou em apresentar as diferentes formas pelas quais as empresas costumam enfrentar o problema das fraudes. Finalmente, na terceira e última parte, abordou as particularidades dos usos de dados pessoais durante o enfrentamento a fraudes, incluindo reflexões sobre quando de fato dados devem ser objeto de proteção jurídica e como as regras previstas nas hipóteses de tratamento se amoldam a cada caso.

2 DEFININDO “FRAUDE” NA NORMA BRASILEIRA

Como ponto de partida, parece razoável ter certeza que o debate a ser desenvolvido cobre adequadamente conceitos que podem facilmente se confundir e comprometer uma mensagem clara por uma abordagem pouco, quiçá nada explorada na produção jurídica nacional. Como será possível ser visto mais à frente, o conceito de fraude impactará diretamente alguns desdobramentos que surgem da confirmação da existência de uma fraude.

Sendo assim, o que seriam as fraudes? Não há qualquer definição objetiva sobre o termo na legislação vigente no Brasil, de forma que para chegar a tal resultado, será necessário passar por um processo hermenêutico. Segundo o dicionário online Michaelis, fraudes podem ser entendidas como "1) Ato de má-fé que tem por objetivo fraudar ou ludibriar alguém; cantiga, engano, sofisticação. 2) Mentira ardilosa; sicofantia. 3) Entrada ilegal de produtos estrangeiros, sem o pagamento dos tributos alfandegários. 4) Ato de falsificar documentos, marcas e produtos." Apesar de fornecer um ponto de partida, juridicamente não basta uma definição lexical, que até pode auxiliar mediante a técnica de interpretação gramatical, mas é necessário um aprofundamento do tema, investigando as normas nacionais para delas extrair um conceito adequado ao direito brasileiro.[2]

Antes de prosseguir, cabe aqui uma digressão para explicar a metodologia que será empregada na definição normativa de fraude que será utilizada ao longo da pesquisa. No direito positivo tem-se que a completude normativa depende de uma estrutura lógico-normativa que viabilize a identificação dos requisitos fáticos condicionantes da sua aplicação, bem como a descrição abstrata de sua consequência jurídica (Bisol, 2016, p. 54-57). Dispositivos legais que tenham ausentes qualquer das duas proposições são considerados incompletos, de maneira que para sanar essa incompletude, é necessário integrá-las a outros dispositivos para finalmente formar aquilo que pode ser chamado de norma jurídica. Assim, dado que nosso esforço está concentrado na definição normativa de fraude, para além de sua identificação particular, cada dispositivo legal que isoladamente considere esse conceito é um fragmento da norma.

[2] O direito brasileiro adota a escola de *Civil Law*, na qual a lei é fonte primária do sistema jurídico (Tartuce, 2018, p. 2).

Dos dispositivos fragmentários que compõem a norma relacionada à fraude, podem ser extraídas quatro características descritivas, que afinal, irão propiciar uma conceituação jurídica do termo compondo finalmente a norma dirigida à fraude. São elas: i) o vício no ato de vontade do fraudado (vítima); ii) a invalidade no ato do fraudador (agente); iii) a anulabilidade das consequências ou resultados da fraude; iv) a reclassificação do fato, enquadrando-se em alguma tipificação penal, gerando repercussões criminais para o agente.

A fim de ilustrar as características indicadas, e com o intuito de tornar essa investigação mais concreta, serão explorados alguns dispositivos representativos que podem ser encontrados na norma nacional. Esse caminho foi escolhido para evitar excessiva redundância em alguma tentativa fútil e desnecessária de abordar todas as incidências da fraude na norma brasileira, ao mesmo tempo em que se cumpre a proposta de definir fraude por meio do método indutivo a partir do nosso sistema normativo fragmentário.

- Vício no ato de vontade do fraudado

Na esfera cível, o vício de vontade causado pela fraude não necessariamente torna nulo o negócio jurídico, mas anulável (art. 171, II, Código Civil – CC). Por outro lado, na esfera criminal, o vício do consentimento da vítima da fraude ou torna um fato que seria legítimo em crime (exemplo: a conjunção carnal voluntária entre adultos é legítima, mas devido à fraude que vicia a vontade da vítima, se torna em uma conjunção sem sua vontade, portanto, estupro - art. 215, Código Penal – CP).

- Invalidade no ato do fraudador

Na Seção VI do Código Civil – CC, entre os artigos 158 e 165 bem como o art. 171, prescreve uma série de nulidades e suas consequências em atos e contratos firmados com a intenção de fraudar credores que possuam legítimo interesse sobre coisa ou direito que tenha sido vulnerabilizado ou mesmo lesado em definitivo pelo fraudador. A convenção de Viena sobre o Direito dos Tratados, definiu em seu art. 49 que a fraude é

motivação suficiente para invocar a invalidade do consentimento de um Estado consoante outro Estado negociador, desobrigando-se de seu cumprimento.

- Anulabilidade das consequências ou resultados da fraude

A Constituição Federal ao tratar de direitos políticos em seu art. 14, §10, possibilita a impugnação de mandato eletivo perante a Justiça Eleitoral em até quinze dias da diplomação do mandatário na ocorrência de fraude. Caso esse prazo preclua, a diplomação poderá ocorrer mesmo apesar da fraude comprovada.

- Reclassificação do fato

A fraude potencialmente pode qualificar um fato já tipificado como crime (exemplo: furto mediante fraude – art. 155, §4º-B, CP). Interessantemente, durante as pesquisas sobre a reclassificação do fato, não foram encontrados tipos que agravassem a conduta, apenas que as qualificam, o que denota uma disposição de aumentar o poder punitivo em relação a esse tipo penal, portanto, uma maior reprovação de quem age deliberadamente violando a boa-fé.

É importante estabelecer que a fraude é dolosa. Não há espaço para erro ou culpa. Há algum tipo de vontade por trás da ação da pessoa que comete uma fraude, normalmente de beneficiar ou prejudicar alguém. Os sujeitos passivos da fraude podem ser privados, públicos ou mesmo abstratos, como a opinião pública. Reconhecida a existência de fraude, na esfera privada é típico que sejam previstas multas contratuais ou o desfazimento de contratos e, na esfera pública, a tipificação de crimes decorrentes da fraude pública. De todo fato revestido, de fraude, nasce uma pretensão pública de persecução penal decorrente da tipicidade do fato a ela diretamente relacionada, ou de alguma qualificadora de outros tipos penais, bem como uma pretensão indenizatória do privado por ele afetado ou prejudicado.

Destaque-se que a fraude possivelmente cruza transversalmente todas as matérias jurídicas, de maneira que dispositivos que tipificavam ou prescreviam algum tipo de consequência quando da sua incidência nas seguintes áreas: direito dos tratados e

internacional (público e privado), direito constitucional, legislação eleitoral, legislação comercial, direitos de nacionalidade, legislação penal e processual penal (inclusive militar), legislação civil e processual civil, legislação trabalhista, direitos autorais, regulações administrativas, legislação tributária, legislação consumerista, direito ambiental, proteção de dados pessoais, legislação de apoio à cultura, direito do esporte, lei da magistratura, legislação de registros públicos, legislação de fornecimento de educação e saúde, legislação afeta à administração pública direta e indireta, além de ser tratada em súmulas de tribunais superiores, sendo eles o STF, STJ e TST.

3 DA NATUREZA DO ENFRENTAMENTO À FRAUDE

Uma vez identificada a *ratio legis* por trás da fraude, os inúmeros danos que ela pode causar e os inequívocos interesses tanto público quanto privado em combatê-la nacional e internacionalmente, finalmente é possível abordar os meios pelos quais se pode fazer isso. Não há mistério ou novidades a respeito da atuação pública na repressão de fraudes, que deve se dar por qualquer agente público e pela administração pública por dever de ofício.[3] Essa atuação ocorre dentro dos próprios órgãos por meio de corregedorias ou por outros órgãos, como controladorias, tribunais de contas e mesmo pelas polícias civis, e federal quando investigando os crimes de fraude. Em âmbito privado, o enfrentamento a fraudes é realizado por áreas especializadas, com a literatura normalmente se concentrando nos processos de auditoria (Pinheiro, 2003), *compliance,* também chamado de integridade (Santos, 2011), e governança (Medeiros; Codignoto, 2023).

Para além dessas importantes áreas, nas quais o combate a fraudes não é sua função principal, mas uma consequência de sua atividade, existem outras estruturas inteiras de gerenciamento de risco que tem no enfrentamento a fraudes sua função

[3] Tal dever decorre acima de tudo de mandamentos constitucionais que podem ser encontrados no art. 37 da Constituição Federal, mais precisamente no princípio da moralidade, que impõe ao agente público o dever de praticar somente atos ilibados, éticos e probos (Gandra; Mendes; Nascimento, 2012, p. 1132-1134)

precípua. Esse enfrentamento pode ser de natureza preventiva, quando se busca impedir que a fraude sequer ocorra, ou de natureza responsiva, quando a fraude, já ocorrida, é investigada pela empresa que a sofreu, visando detectá-la tanto para aprimorar seu processo preventivo, quanto restituir, na medida do possível, o patrimônio perdido por meio de colaboração com as autoridades de persecução criminal. Naturalmente nada impede que equipes de auditoria, integridade ou mesmo governança acumulem essas funções de prevenção e investigação, de maneira que neste artigo ora serão abordadas as áreas que são dedicadas a fraudes, ora olharemos para a prevenção e investigação a fraudes como atividade e não estritamente como áreas em si. Por certo, equipes dedicadas têm potencial de se especializarem mais, mas essa questão foge ao escopo desta pesquisa.

Tanto a prevenção quanto a investigação a fraudes são não apenas legítimas, como constituem direito e por vezes dever das empresas. Elas são legítimas na medida em que não são proibidas por lei; são direitos enquanto materialização do direito da empresa de zelar e proteger sua propriedade; e são obrigatórias quando assim definido pela norma. Como exemplo disso, a Lei das Sociedades Anônimas (art. 163, IV, Lei 6.404/76) que destaca o dever do conselho fiscal ou na sua inércia, da assembleia geral, de informar aos administradores sobre fraudes que sejam identificadas na administração das empresas e seus balanços.

Os métodos de prevenção a fraude consistem no estabelecimento de rotinas e procedimentos que possibilitem às empresas distinguirem o acesso legítimo do acesso ilegítimo, portanto fraudulento, de seus serviços ou recursos. É instrumentalizada por recursos tecnológicos (Krishnan, 2023) que podem passar desde verificações biométricas, ferramentas, como o duplo fator de autenticação, até produção de inteligência corporativa. Para que seja possível prevenir fraudes, no entanto, é preciso compreendê-la, suas consequências (vítimas, perpetradores e a extensão do prejuízo sofrido) e formas de cometimento. Todas as informações levantadas sobre a fraude devem ser sistematizadas para implementar medidas de prevenção e o monitoramento deve ser feito para evitar que a fraude ocorra novamente. A investigação, também chamada de detecção de fraudes na literatura especializada, ajuda a detectar fraudes e relatá-las à autoridade apropriada (Mangala; Kumari, 2015).

Obviamente o ponto principal não é a investigação da fraude em si, mas o necessário e permanente processo de aprimoramento das barreiras contra a fraude em um primeiro momento e a restituição total ou parcial dos ativos pelas autoridades públicas em um segundo momento. Como exposto na introdução, fraudes digitais têm escalado exponencialmente. Assim, para que realizem seu mister conforme exigido pela lei, pelos acionistas, clientes ou interessados, é fundamental que as empresas estejam ativamente atuando tentando entender as inovações no campo da fraude, notadamente quando seus procedimentos falham, para que seja possível apresentar uma resposta eficaz.

Uma vez identificada a tentativa de fraude ou caso seja consolidada, é necessário que haja alguma comunicação com o poder público, em regra, com a polícia civil para que procedam com investigação criminal buscando eventual responsabilização dos agentes. Ocorre que, para que isso seja feito, não basta apenas a suspeita ou alegação de ocorrência do fato criminoso, é necessário que a empresa consiga apresentar todos os elementos que seja capaz de levantar a respeito do ocorrido. Esse levantamento se dá também pelo processo de investigação, e pode ser desenvolvido de diversas formas ou métodos e em diversos contextos a depender do cenário, como quando se dá em um processo de auditoria.

O tempo de uma investigação de fraudes por parte das empresas costuma ser ágil, mas pode demorar diversos meses a depender de sua complexidade, pois é nele que se angariam os elementos de prova que viabilizarão a investigação policial sobre sua ocorrência. Geralmente, o próprio sucesso das polícias civil ou federal dependerá de levantamentos e dados que estão disponíveis quase exclusivamente às vítimas, sendo uma etapa crucial para o bom desenrolar da investigação policial. Em muitos casos as polícias sequer têm ideia de quais dados são coletados pelas vítimas e que podem estar disponíveis para a investigação policial, de maneira que uma cooperação formalizada pela *notitia criminis*[4] é fundamental para o sucesso das ações de repressão criminal.

[4] Trata-se de um ato de conhecimento de fato entendido como infração penal, que pode decorrer da provocação formal de alguém ou não, e que pode anteceder ou não a ocorrência da infração penal. É por meio da notícia do crime que se viabiliza o início da investigação (Enciclopédia Jurídica da PUC, 2020).

Antes de encerrar este tópico, é importante destacar que a prevenção a fraude não pode se confundir com as medidas de segurança adotadas por empresas com o intuito de preservar a integridade física de seus funcionários ou segurança imediata do seu patrimônio, buscando evitar sua destruição ou perda. Esse campo é reservado à atividade geralmente identificada como segurança patrimonial. Essa área é responsável pela segurança em geral, devendo cuidar, por exemplo, da verificação de acesso às dependências da empresa, controle de saída de patrimônio, coordenação de equipes de segurança privada e acompanhamento de circuito fechado de televisão – CFTV.

No Brasil, muitas vezes essa atividade é inserida na estrutura da diretoria de risco, que acaba concentrando sob sua atuação também a atividade de combate a fraudes. Nessa dinâmica, uma vez que a segurança da empresa seja violada, como por exemplo em um roubo, é comum que a equipe de segurança patrimonial atue acionando as autoridades e cooperando com aquilo que seja necessário para seguimento da investigação criminal. Caso trate-se de um evento em que a segurança seja burlada (não se tratando meramente de uma violação ostensiva), havendo uma estrutura de fraudes na empresa, idealmente deveria haver a comunicação dos fatos para o time de investigação a fraudes. Por sua vez, lhes caberia levantar tudo que fosse possível a respeito do incidente para que seja solicitada a instauração de inquérito policial por meio de *notitia criminis.*

Por certo não é toda empresa que possui porte para tamanha organização (Stone, 2016), sendo comum que a equipe de segurança patrimonial acumule todas essas atividades, incluindo atuação contra fraudes e comunicação com autoridades. Nesses casos é necessário um cuidado redobrado para se evitar potenciais ilegalidades. Ainda que a área de segurança possa atuar no sentido de acumular sua função com a atuação no enfrentamento a fraudes, ambas precisam ser entendidas como coisas distintas, uma vez que o conjunto normativo que viabiliza, ou por vezes até obriga a atividade de enfrentamento a fraudes é distinto daquele que autoriza a atividade de segurança patrimonial.

Em se tratando do enfrentamento a fraudes como um todo, em tempos de revolução digital, é fundamental que essa atividade recorra constantemente ao tratamento sistemático de dados de pessoas jurídicas e naturais. Os direitos e deveres nas relações

entre a empresa responsável pelas ações de enfrentamento a fraudes e dados de outras empresas, portanto, pessoas jurídicas, deve ser regulada sempre a partir de normas do direito civil e contratos que as obriguem mutuamente ou a terceiros interessados quando também forem pessoas jurídicas. Por outro lado, sempre que o uso de dados envolve um titular de dados que seja pessoa natural, automaticamente atrairá a incidência da LGPD (art. 1º), que será objeto de importantes considerações a seguir.

Enquanto o combate a fraudes, inclusive digitais, é voltado à proteção dos ativos da empresa, tradicionalmente será desenvolvido pelos diversos setores da área de gerenciamento de risco, integridade e governança (Hermawan; Novita, 2021). Todavia, quando voltada à proteção dos usuários dos serviços de uma empresa será realizada pelos setores que compõem a novíssima área de *Trust and Safety* – T&S. Trocando em miúdos, T&S é um campo dedicado a investigar como as pessoas abusam da internet para causar danos humanos reais, explorando produtos da maneira como foram projetados para funcionar, mas de forma indevida (Cryst; Grossman; Hancock; Stamos; Thiel, 2023). A função das equipes de T&S é garantir que o ambiente virtual fornecido por certas plataformas seja confiável e seguro para que seus usuários interajam ou façam negócios. Equipes de T&S são as responsáveis por garantir que, em última análise, os usuários confiem que a plataforma que estão utilizando não abusará de seus dados ou violará sua privacidade. Essa divisão ainda é muito incipiente no Brasil e geralmente só é encontrada em multinacionais que já possuem um amadurecimento maior no tratamento de dados de usuários de seus serviços.

Cultivar a confiança do usuário implica que é papel de T&S evitar que esse usuário sofra com vazamentos de seus dados ou exposição desnecessária, garantindo que a empresa tratará seus dados conforme sua própria expectativa em relação a esse serviço (art. 10, II, LGPD). Lhes cabe também construir e cultivar confiança junto ao poder público na medida em que é seu papel zelar pelo cumprimento da lei no que toca ao tratamento e compartilhamento de dados de usuários de seus serviços conforme os princípios nela previstos e a boa-fé (art. 6º, LGPD).

No que toca à segurança do usuário, é dever de T&S garantir que além da segurança de seus dados, a empresa atuará para preservar inclusive sua própria

integridade física (art. 7, VII e art. 11, II, g, ambos da LGPD). Naturalmente a atuação da empresa não pode extrapolar aquilo que tem poder de fazer, tampouco pode agir em contrariedade à lei alegando segurança ou proteção dos titulares dos dados que lhe foram conferidos. Não obstante, há toda uma responsabilidade por parte da empresa em agir uma vez que certas informações lhe são confiadas com exclusividade, e sua inação pode render-lhe responsabilizações de caráter cível ou criminal nas pessoas dos responsáveis que não agirem para evitar danos, quando cabível. Por certo, essa responsabilidade se encerra quando toma todas as medidas possíveis ou que estavam ao seu alcance para fazer frente aos riscos a que pode estar submetido o usuário de seus serviços.

Apesar de um aparente antagonismo entre Risco e T&S, as duas estruturas ao fim a ao cabo necessariamente agem no interesse da empresa, mas agora de uma maneira mais holística, ao incluir como sua preocupação a busca pela proteção de seus clientes para além apenas da sua. Nesse passo, parece inevitável que, por vezes, as áreas de Risco e de T&S atuem juntas para simultaneamente proteger a empresa *e* seus clientes. Não há qualquer problema com essa atuação, mas é responsabilidade da empresa como um todo zelar para que dados regulares ou sensíveis dos clientes não sejam comprometidos para além daquilo que é legítimo ser explorado durante uma atuação como essa.

4 USO DE DADOS PESSOAIS NO COMBATE A FRAUDES DIGITAIS

Antes de aprofundar neste tópico, parece importante trazer alguns conceitos fundamentais do capítulo de definições da LGPD (art. 5º) para evitar confusões terminológicas e a bem da clareza da pesquisa:

- Titular de dados: pessoas físicas cujo interesse surge sempre que há uma atividade de tratamento de seus dados pessoais.

- Dado pessoal: toda informação relacionada a pessoa natural identificada ou identificável.

- Tratamento: engloba praticamente tudo o que pode ser feito com dados pessoais, da coleta, passando pela manipulação e até o descarte das informações.

- Agentes de tratamento: são aqueles que manipulam os dados dos titulares, podendo ser de dois tipos:

    - Controlador: responsável pela coleta e armazenamento dos dados pessoais. Determina as finalidades e as maneiras de tratamento dos dados pessoais.

    - Operador: realiza o tratamento de dados pessoais conforme instruções do controlador

Ao controlador pode ser necessário o tratamento de dados pessoais em distintas hipóteses autorizadas ou mesmo determinadas pelo art. 7º da LGPD. Aquelas que são mais relevantes para as formas de lidar com fraudes digitais incluem o cumprimento de obrigação legal ou regulatória, para a proteção do crédito ou quando presente o legítimo interesse do controlador ou de terceiros.

Em relação ao cumprimento de obrigação legal ou regulatória, muito recentemente ocorreu a assinatura de um acordo de cooperação técnica entre a Federação Brasileira de Bancos – FEBRABAN e o Ministério da Justiça e Segurança Pública (Brasil, 2024), voltado para o enfrentamento de fraudes digitais. O acordo definiu um plano de trabalho visando, entre outras coisas, a capacitação de agentes públicos e parceiros, o mapeamento dos principais casos de fraudes, golpes e crimes cibernéticos. O acordo vem na esteira de outro acordo existente entre a FEBRABAN e a Polícia Federal desde 2007, chamado Projeto Tentáculos (FEBRABAN, 2023), que possibilita centralizar todas as notícias-crime de fraudes em um repositório único de dados.

Quanto à proteção ao crédito podemos citar como exemplo, além do conteúdo das normas já apontadas previamente que também se amoldam a esta hipótese, a Resolução Conjunta nº 6/BACEN, de 2023. Nela, o Banco Central do Brasil – BACEN, e o Conselho Monetário Nacional regularam acerca dos requisitos para compartilhamento de dados e

informações sobre indícios de fraudes por instituições financeiras. A Resolução definiu o dever de que as instituições compartilhem dados e informações com as demais instituições reguladas pelo BACEN com a finalidade de subsidiar seus procedimentos e controles de prevenção a fraudes, mediante alguns requisitos.

Finalmente, a hipótese de legítimo interesse não pode ser compreendida como uma hipótese coringa, a ser utilizada sempre que as demais hipóteses não se apliquem ao desejo do controlador dos dados (Leonardi, 2019), sendo fundamental demonstrar a aplicabilidade do legítimo interesse por meio dos testes de balanceamento (ANPD, 2024), relatório de impacto (art. 10, §3º, LGPD) e registros pertinentes sobre essa operação (art. 37, LGPD). Importante destacar que um dos objetivos principais dos testes de balanceamento é verificar se o interesse legítimo do controlador ou terceiro efetivamente se sobrepõe aos direitos e liberdades fundamentais do titular dos dados enquanto os demais se prestam a verificar se somente os dados estritamente necessários foram tratados.

Merece destaque uma reflexão, que certamente será aprofundada em futuros estudos acadêmicos, sobre como o legítimo interesse (considerado pela perspectiva do controlador de dados) deve ser legitimado. Quando da realização do teste de balanceamento e demais meios de controle e prevenção aos excessos do legítimo interesse, precisa estar claramente descrito o que efetivamente legitima aquele tratamento no contexto do combate a fraude. Ou seja, é necessário estar expresso se o controlador está tratando esses dados para a proteção dos seus recursos e serviços ou se é para a proteção do próprio usuário.

Aqui, mais uma vez, a forma de organização e estruturação dos setores internos, bem como clareza na sua missão e cultura são os principais garantidores de registros adequados para prevenir excessos e ilegalidades, e por consequência uma possível sanção administrativa pela ANPD ou mesmo responsabilização judicial por abuso no tratamento de dados pela empresa.

Até recentemente o uso mais comum do legítimo interesse no tratamento de dados pessoais para combater fraudes se deu no âmbito de proteção da própria empresa e seus ativos, o que envolve a atuação de gerenciamento de risco empresarial. Quase toda

empresa de médio e grande porte possui algum setor dedicado a esse fim, havendo inclusive aquelas que não lidem com usuários, apenas atuando diretamente com outras empresas como clientes. Empresas menores ou que não pretendam investir em equipes internas dedicadas a esse fim, podem trabalhar com empresas terceiras na realização da consultoria em risco ou segurança. Em um ou outro caso, o interesse que legitima o tratamento de dados será o do controlador de dados, que o realiza diretamente ou por meio do agente de tratamento que o faz em seu nome.

De outro lado, sempre que as ações tomadas forem com o intuito de evitar fraudes para proteger os interesses e segurança do próprio usuário, o legítimo interesse não será no interesse do controlador, mas de terceiros, no caso o próprio titular dos dados. Esses terceiros podem também ser entendidos como a própria comunidade de demais usuários dos serviços dessa empresa (ANPD, 2024) ou ainda outros que podem ser impactados por desdobramentos desta fraude.[5] Cabe destacar ainda que, tanto no caso de segurança do titular de dados quanto em casos de fraude que afetem o controlador em si, nos termos da Lei, é possível o tratamento de dados sensíveis (art. 11, LGPD).

Não obstante essas hipóteses em que se pode deduzir sua aplicabilidade ao enfrentamento a fraudes, a LGPD somente é expressa ao se referir a fraudes no art. 11, II, g, dispositivo localizado na seção dedicada ao tratamento de dados sensíveis.[6] Essa escolha legislativa é particularmente interessante, em especial ao se considerar como a regulação europeia, como já dito, fonte de inspiração para a lei nacional, se posicionou a esse respeito. Em 2014 foi apresentada a Opinião 06/2014, escrita pelo grupo de trabalhos da comissão europeia a respeito da interpretação a ser conferida ao teor das hipóteses de tratamento de dados. Cabe destacar que em que pese a opinião ter sido redigida em

[5] Exemplo disso é quando dados reais de um cidadão são utilizados para criar contas bancárias falsas em diversas instituições financeiras que serão utilizadas para lavar dinheiro proveniente de outros crimes, como a venda falsa de produtos a terceiros de boa-fé, utilizando esses dados reais que se apresentam como confiáveis num primeiro momento.

[6] Importante destacar aqui que a terminologia empregada tanto na Opinião 06/2014 do grupo de trabalho da comissão europeia de proteção de dados, quanto no art. 11, II, g, LGPD ao chamar o enfrentamento a fraudes de maneira genérica como "prevenção a fraude", não tinham intenção de excluir a investigação a fraudes, sob pena de tornar a própria prevenção ineficaz. Como foi explicado, há, inclusive, verdadeira dependência dos processos de prevenção dos métodos de investigação e descoberta de fraudes.

referência à então em vigor Diretriz 95/46/EC, primeira norma a sistematizar a questão de dados pessoais na União europeia, seu teor foi endossado durante o primeiro encontro do conselho europeu de proteção de dados por ir ao encontro do que foi previsto na GDPR. Apesar da importância e preocupação com combate às fraudes permear tanto a Opinião 06/2014 quanto a GDPR,[7] não há exceções expressas sobre enfrentamento a fraudes no tratamento de categorias especiais de dados, como foram chamados os dados sensíveis na Diretriz 95/46/EC e na GDPR.

De outro lado, quando da confecção de seu guia orientativo a respeito do legítimo interesse no Brasil, a Autoridade Nacional de Proteção de Dados – ANPD, afirmou expressamente que a despeito da autorização expressa da LGPD de uso de dados sensíveis com a finalidade de prevenir fraudes (art. 11, II, g), isso não exclui o uso de dados não sensíveis também para o mesmo fim na hipótese do legítimo interesse de forma a garantir a segurança dos dados dos titulares. Ou seja, considerando a expressa autorização do uso de dados sensíveis para enfrentamento a fraudes enquanto se quedava silente a respeito do mesmo uso no dispositivo que abordou o legítimo interesse, a ANPD entendeu necessário enfrentar a questão no seu guia dedicado ao legítimo interesse, certamente visando sanar alguma dúvida que pudesse surgir a respeito, como por exemplo, que tal hipótese não fosse hábil para legitimar investigações ou prevenção a fraude por interpretação negativa. Razoável, portanto, a posição da ANPD ao não descartar fraude como hipótese legítima para tratamento de dados no interesse do controlador ou terceiros.

Aparentemente a realidade brasileira se impôs durante o processo legislativo de tal forma, que foi necessário expandir as hipóteses que viabilizem o enfrentamento a fraudes no Brasil, inclusive autorizando o uso de dados sensíveis para tal fim. No entanto, sempre é importante destacar que junto a essa possibilidade, nasce uma responsabilidade redobrada devida ao tratamento de dados sensíveis.

Aqui nasce uma reflexão necessária de ser realizada. Pela própria natureza da fraude, é comum que os fraudadores forjem identidades inteiras, criando verdadeiras

[7] Nos considerandos da GDPR, há menções ao uso de dados para enfrentamento a fraudes em cinco parágrafos: 47, 71, 75, 85 e 88.

personas que frequentemente sequer existem, ou ainda se utilizem de dados de pessoas reais sem seu conhecimento.

Diversos são os casos nos quais fraudadores forjam ou fraudam desde certidões de nascimento ou casamento, passando pela abertura de contas em bancos, plataformas digitais ou em diversos setores de serviço em nome dessa persona inexistente. Criam endereços (muitas vezes igualmente inexistentes), manipulam digitalmente fotos de pessoas reais para gerar imagens de pessoas fictícias, inclusive se passando por eles em contatos com vítimas ou centrais de apoio a clientes. Uma questão parece preponderante nesses casos: se essa persona é absolutamente falsa, inexistente, não lhe são devidos quaisquer direitos ou garantias. São, em realidade, cada um desses dados, foto, endereço, conta bancária e dados de registro civil, materialidade dos crimes de falsidade cometidos pelos fraudadores. Resgatando as características que identificamos ao conceituar a norma atinente a fraude na primeira parte da pesquisa, todos os atos realizados pelo fraudador devem ser reputados inválidos. Ou seja, não há qualquer impedimento legal que as empresas durante seus processos de prevenção ou investigação a fraudes lhes façam verdadeira devassa para que possam proteger clientes reais ou os ativos da empresa.

Situação distinta recai sobre os dados de pessoas reais que de alguma forma chegam às mãos de criminosos, o que demanda maior cautela por parte dos profissionais atuando no enfrentamento a fraudes. Dados legítimos podem ser objeto de tratamento para descoberta e proteção a fraudes, inclusive dados sensíveis, como impressões digitais, mas esses dados precisam ser tratados levando-se em consideração as liberdades e direitos fundamentais do seu titular, cientes ou não do seu mal uso por terceiros (ou talvez, especialmente por desconhecê-lo). Mais uma vez, no que tange à norma relacionada a fraude, outra de suas características é a anulabilidade das suas consequências. Isso implica, por exemplo, que empréstimos realizados em nome de pessoas reais por fraudadores não podem lhe ser cobrados.

Notem, porém, que contas falsas criadas por meio de dados reais de vítimas não usufruem em si da mesma proteção devida a contas reais criadas pelos titulares dos dados. Mais uma vez, no esforço realizado durante a definição normativa de fraude, no que tange aos vícios decorrentes da atividade fraudulenta, há invalidade do ato de criar a conta, bem

como seus resultados são anuláveis: a conta em si pode ser revirada ou mesmo removida pelo prestador de serviço ou pelo próprio titular dos dados sem que lhe acarrete qualquer prejuízo. O desafio sempre vai residir no esforço que envolve essas considerações nos testes de balanceamento, sendo devida cautela e responsabilidade redobradas pelas equipes de enfrentamento a fraudes quando manipulando dados desse tipo.

Finalmente, parece importante abordar a questão dos dados dos chamados laranjas ou testas de ferro. Laranjas ou testas de ferro é como são popularmente conhecidos os criminosos que, na condição de partícipes, voluntariamente fornecem seus dados legítimos para fins criminosos. Nesses casos, ainda que exista o dolo no cometimento de crime, eles ainda são titulares legítimos dos dados, e tanto as equipes de enfrentamento a fraudes quanto as autoridades criminais devem agir na estrita legalidade para não macular o procedimento investigativo e potencialmente a própria ação penal.

5 CONSIDERAÇÕES FINAIS

Ao longo do artigo, foi possível observar que fraudes surgem da ação dolosa do agente de se beneficiar ou prejudicar pessoas naturais, jurídicas (públicas ou privadas) ou a coletividade. Dentre suas características, uma vez detectada, destacam-se a existência do vício no ato da vítima, a invalidade no ato do fraudador, a anulabilidade das suas consequências ou resultados da fraude, e possível reclassificação do fato.

Dentre as pesquisas acadêmicas realizadas no Brasil a respeito dos setores responsáveis por enfrentamento a fraudes, o mais comum são artigos que tratem de auditoria, integridade e governança, escapando-lhes investigações a respeito das atividades exclusivamente dedicadas a esse fim: a atuação preventiva e a detecção ou investigação que se segue ao cometimento da fraude. Nesse sentido, foi abordado a respeito da necessidade de constante atualização e envolvimento dos setores de investigação para manter viável a capacidade de resposta das empresas às fraudes a que estão sujeitas.

Foi apresentado como equipes de gerenciamento de risco se estruturam e atuam ao agirem no interesse das empresas. Em contraste, introduzimos a nova área que está em

formação internacionalmente e começa a deixar suas pegadas no Brasil, chamada *Trust and Safety*, que tem desempenhado um importante papel na garantia de correta segurança do tratamento de dados de titulares. Isso naturalmente impacta diretamente o próprio tratamento de dados durante processos de combate a fraudes. Como vimos, ela se diferencia da atividade de gerenciamento de risco por ter como sua raiz e eixo principal a preocupação com a segurança do usuário de serviços, enquanto o gerenciamento de risco se concentra em proteger os ativos da empresa.

Devido à natureza das equipes que potencialmente atuam no combate à fraude, foi possível observar ao longo da pesquisa que dependendo de qual equipe esteja atuando, a hipótese de incidência legal que autoriza o tratamento de dados no combate a fraudes será alterada. Assim, para responder ao problema proposto, é necessário definir em qual capacidade as equipes estão agindo, de forma que a hipótese de tratamento de dados será distinta em cada atuação.

Dessa forma, auditorias e programas de integridade atuarão sempre que se tratar de fraudes que a empresa tenha obrigação legal de reprimir ou na proteção do crédito. Especificamente no que se refere ao legítimo interesse, enquanto de um lado está o controlador de dados ou seu operador tratando os dados para prevenir ou detectar fraudes no interesse do próprio controlador, do outro está T&S tratando dados no interesse dos usuários ou comunidade, entendidos como terceiros.

Há aí uma particularidade interessantíssima a respeito da atuação prática das equipes de T&S em comparação com as tradicionais e amadurecidas áreas de gerenciamento de risco. Como o foco dessas equipes divergem num primeiro momento, muitas vezes elas podem se chocar em relação aos interesses imediatos da empresa, ainda que se alinhem com interesses mediatos; como a manutenção da base de clientes e usuários de seus serviços, a conformidade legal e equilíbrio em relação ao tratamento de dados dos titulares. Na realidade, essa divergência vem a compor a riqueza e equilíbrio que passa a surgir quando as áreas de gerenciamento de risco e de T&S são bem estruturadas e atuam em harmonia. Nesse sentido, mesmo a preocupação com o tratamento de dados com base no legítimo interesse deve respeitar as particularidades de cada um desses setores.

Por fim, a pesquisa se encerra com considerações a respeito do alcance das proteções legais e constitucionais que permeiam dados forjados por fraudadores, dados reais que fraudadores utilizam para criar contas falsas e dados reais utilizados para criação de contas reais, mas com a finalidade de cometer crimes. Espera-se que com esta provocação, outros trabalhos venham a ser produzidos para aprofundar ainda mais esse importante debate que ora se impõe sobre a norma de proteção de dados doméstica e estrangeira, bem como nos mercados digitais nacional e internacional.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). **Guia orientativo sobre bases legais para o tratamento de dados pessoais:** Legítimo interesse. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-orientativo-sobre-legitimo-interesse Acesso em: 12 jun. 2025.

BISOL, Jairo. **Fundamento normativo**: sobre a norma jurídica geral e a decisão judicial. Curitiba: Juruá, 2016.

BRASIL. Ministério da Justiça e Segurança Pública. **Acordo de Cooperação nº 1/2023/SE/MJSP.** Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/acts/secretaria-executiva/acordo-de-cooperacao-no-1-2023-se-mjsp/sei_mj___26226967___acordo_transparencia.pdf. Acesso em: 29 abr. 2025.

CRYST, Elena.; GROSSMAN, Shelby.; HANCOCK, Jeff.; STAMOS, Alex; THIEL, David. Introducing the Journal of Online Trust and Safety. **Journal of Online Trust and Safety**, *[S. l.]*, v. 1, n. 1, 2023. DOI: 10.54501/jots.v1i1.8. Disponível em: https://tsjournal.org/index.php/jots/article/view/8. Acesso em: 23 jun. 2025.

EDPB. **Endorsed WP29 Guidelines.** Disponível em: https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en. Acesso em: 12 jun. 2025.

ENCICLOPÉDIA JURÍDICA DA PUC. **Notitia criminis**. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/449/edicao-1/notitia-criminis. Acesso em: 12 jun. 2025.

FEBRABAN. **Febraban e Polícia Federal assinam mais um acordo para combater fraudes bancárias digitais.** Disponível em: https://portal.febraban.org.br/noticia/4031/pt-br/ Acesso em: 12 jun. 2025.

GANDRA, Ives da Silva Martins; MENDES, Gilmar Ferreira; NASCIMENTO, Carlos Valder do. **Tratado de direito constitucional**, v. 1. 2. ed. São Paulo: Saraiva, 2012.

Greenleaf, Graham, Global Data Privacy Laws: Forty Years of Acceleration (October 10, 2011). **Privacy Laws and Business International Report**, No. 112, pp. 11-17, September 2011, UNSW Law Research Paper No. 2011-36, disponível em: SSRN: https://ssrn.com/abstract=1946700. Acesso em: 12 jun. 2025.

HERMAWAN, Agung.; NOVITA, Novita. The Effect of Governance, Risk Management, and Compliance on Efforts to Minimize Potential Fraud Based on the Fraud Pentagon Concept. **Asia Pacific Fraud Journal**, *[S. l.]*, v. 6, n. 1, p. 82–95, 2021. DOI: 10.21532/apfjournal.v6i1.196. Disponível em: https://apfjournal.or.id/index.php/apf/article/view/196. Acesso em: 13 set. 2024.

IPSOS. **What Worries the World** – August 2024. Disponível em: https://www.ipsos.com/en/what-worries-world. Acesso em: 12 jun. 2025.

KRISHNAN, K. Sarojini Devi; RANI, Nazatul Shima Abdul; SUDA, Khairul Azizan; CHAHHOUB, Fatimazahra. An Investigation of Business Intelligence Tools and their Effectiveness in Fraud Risk Management. **Asia Proceedings of Social Sciences**, v. 11, n. 1, p. 91-95, 2023. Disponível em: https://readersinsight.net/APSS/article/view/2814. Acesso em: 23 jun. 2025.

LEONARDI, Marcel. Legítimo interesse. **Revista do Advogado,** n. 144, 2019.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. **Revista do Programa de Direito da União Europeia**, v. 1, p. 39-52, 2021. Disponível em: https://periodicos.fgv.br/rpdue/article/view/83423 Acesso em: 23 jun. 2025.

MANGALA, Deepa; KUMARI, Pooja. Corporate Fraud Prevention and Detection: Revisiting the Literature (January 1, 2015). **Journal of Commerce & Accounting Research**, Volume 4, Issue 1, January 2015, pp 35-45, Disponível em: https://ssrn.com/abstract=2678909. Acesso em: 12 jun. 2025.

MARTINS, André. Preocupação do brasileiro com violência cresce em quase um ano e chega a 19%, aponta Genial/ Quaest. **EXAME**. Disponível em: https://exame.com/brasil/economia-violencia-e-questoes-sociais-sao-as-principais-preocupacoes-do-brasileiro-aponta-pesquisa/. Acesso em: 12 jun. 2025.

MEDEIROS, Marcio Lima; CODIGNOTO, Roberta. Governança, integridade e resultados caminham juntos. **Revista Latino-americana de Governança**, Brasília

(DF), v. 3, n. 1, p. e030, 2022. DOI: 10.37497/ReGOV.v3i1.30. Disponível em: https://revistaregov.org/index.php/revista/article/view/30. Acesso em: 24 jun. 2025.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/fraude. Acesso em: 12 jun. 2025.

PINHEIRO, Geraldo José; CUNHA, Luís Roberto Silva. A importância da auditoria na detecção de fraudes. **Contabilidade Vista & Revista**, v. 14, n. 1, p. 31-47, 2003. Disponível em: https://revistas.face.ufmg.br/index.php/contabilidadevistaerevista/article/view/210. Acesso em: 23 jun. 2025.

SANTOS, Renato de Almeida dos. Compliance como ferramenta de mitigação e prevenção da fraude organizacional. 2011. 151 f. **Dissertação** (Mestrado em Administração) – Pontifícia Universidade Católica de São Paulo, São Paulo. Disponível em: https://bdtd.ibict.br/vufind/Record/PUC_SP-1_77dbb3776a66e09e507b17c6d78d0348. Acesso em: 12 jun. 2025.

STONE, Robert. Fraud, security, and controls in small businesses: A proposed research agenda. **Journal of Business**, v. 1, n. 3, p. 15-21, 2016. Disponível em: https://journalofbusiness.us/index.php/site/article/view/44. Acesso em: 23 jun. 2025.

TARTUCE, Flávio. **Manual de direito civil**: volume único. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018.

TRANSUNION. **TransUnion Report Finds Digital Fraud Attempts Spike 80% Globally From Pre-Pandemic Levels**. 13 mar. 2023. Disponível em: https://newsroom.transunion.com/transunion-report-finds-digital-fraud-attempts-spike-80-globally-from-pre-pandemic/. Acesso em: 12 jun. 2025.

VISA. **Biannual Threats Report**, December 2023. Disponível em: https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/pfd-biannual-threats-report-december-2023.pdf. Acesso em: 29 abr. 2025.