Investigações internas corporativas: limites e contornos para acesso e compartilhamento de dados

Maria Beatriz Campos Rodrigues de Moura

1. Identificação e apresentação do(s) problema(s) da pesquisa individual

Um relato anônimo foi registrado no canal de denúncias de uma empresa, descrevendo condutas de corrupção que teriam sido praticadas por um de seus diretores. A empresa iniciou uma investigação interna para apurar as eventuais infrações.

Durante o procedimento investigativo, o computador corporativo utilizado pelo diretor foi acessado sob a justificativa de que o dispositivo pertenceria à empresa, o que, inclusive, implicaria na ausência de expectativa de privacidade, conforme estabelecido no Código de Conduta e no Aviso de Privacidade aos Colaboradores. Embora o diretor utilizasse o e-mail corporativo exclusivamente para questões profissionais, ele também acessava seu e-mail pessoal e o aplicativo *WhatsApp* por meio do navegador.

A equipe de investigação interna acessou remotamente a máquina corporativa do diretor e, ao vasculhar seu e-mail pessoal e seu *Whatsapp Web*, identificou evidências robustas das práticas ilícitas.

Diante do envolvimento de diversos membros da alta liderança, a empresa optou por não notificar as autoridades públicas e comprometeu-se com o desligamento dos colaboradores[1] envolvidos. No entanto, foi expedido um ofício policial solicitando todos os relatórios – substanciados e não substanciados – de investigações internas registradas pelo departamento de compliance desde sua criação.

---

[1] Ao longo da pesquisa, para fins didáticos, a terminologia utilizada será "*colaboradores*", posto que "*funcionários*" poderia remeter a funcionários públicos e "*trabalhadores*" àqueles inseridos no regime CLT. Como alguns membros da alta administração compõem a organização por meio de contratos como Pessoa Jurídica, o termo "*colaboradores*" abarcariam eles também.

Dessa situação, extraem-se as perguntas: quais são os limites para o acesso, pela equipe de investigação interna, aos dispositivos corporativos na posse de seus colaboradores? É permitido acessar contas pessoais, como e-mails e aplicativos de mensagens?

Em um segundo momento, caso uma autoridade pública solicite acesso aos dados e às provas obtidas em investigação interna, a empresa é obrigada a compartilhá-los? Qual autoridade pública está apta a fazer tal pedido? O pedido pode ser indeterminado? O relatório de investigação interna é protegido por sigilo entre advogado e cliente?

Um cenário alternativo que pode ser demonstrado seria: a empresa optou por registrar um boletim de ocorrência e compartilhar com as autoridades públicas o que foi coletado durante a investigação interna, sob a justificativa de que se trataria de "*legítimo interesse*"[2]. De acordo com a previsão disposta em sua Política Interna de Law Enforcement, com intuito de colaborar com as autoridades públicas e subsidiar sua defesa criminal, a empresa compartilhou os dados de pessoas envolvidas em suspeitas de cometimento de delitos.

Questiona-se: a empresa pode compartilhar dados de terceiros, coletados em investigações internas, ainda que seja em seu interesse, para subsidiar eventual defesa criminal?

2. Concepções dogmáticas para a abordagem dos problemas

O que se pretende explorar, especialmente, são os limites impostos aos integrantes das equipes de investigação corporativa, em empresas brasileiras, durante a apuração de condutas denunciadas internamente. Para isso, o emprego de meios invasivos[3] na obtenção de material probatório será examinado para sua posterior delimitação, em atenção à vulnerabilidade dos direitos de privacidade. O objetivo é desenvolver os contornos dessas medidas invasivas no âmbito extrajudicial – investigações internas – para entender o que essas equipes podem acessar.

---

[2] Art. 10 c/c art. 37 da Lei Geral de Proteção de Dados (LGPD).

[3] Divisão em (i) medidas invasivas permitidas: aquelas em que não há expectativa de privacidade; (ii) medidas invasivas condicionadas: aquelas em que há autorização do empregado e (iii) medidas invasivas vedadas: há expectativa de privacidade imutável ainda que por autorização do empregado. (ZACLIS, Daniel. *Investigação interna corporativa…*, p. 226 e ss.)

Se pretende iniciar a pesquisa abordando a comunicação que a empresa deve realizar sobre a ausência de expectativa de privacidade, seus requisitos e contornos. Para que a privacidade de um trabalhador seja considerada limitada, parece fundamental que a empresa tenha estabelecido uma proibição explícita de uso pessoal dos dispositivos corporativos e que os colaboradores tenham sido informados, de forma clara e detalhada, sobre as políticas de monitoramento e as possíveis consequências de sua violação[4].

Superado esse ponto, os parâmetros da proporcionalidade[5], da necessidade e da finalidade nas ações de monitoramento também serão trazidos à baila, pois, embora o consentimento expresso e as políticas internas da empresa desempenhem papéis cruciais na avaliação da expectativa de privacidade, a amplitude e a natureza do monitoramento devem respeitar os referidos princípios[6], evitando excessos e garantindo que a coleta de provas ou dados pessoais não seja desproporcional ao inicialmente pretendido.

A ausência de expectativa de privacidade não implica, portanto, a autorização para práticas de monitoramento ou ingerências ilegítimas. Ainda que subsista a devida comunicação quanto à ausência de expectativa de privacidade, será examinado se todo e qualquer conteúdo encontrado de maneira fortuita poderá ser utilizado para fins de investigação interna.

Na segunda parte do trabalho, alguns dispositivos legais, como o art. 4º, inciso III, alínea *d,* o §1º da Lei Geral de Proteção de Dados, a Constituição Federal, por meio do 5º, incisos XII e LXXIX, tal qual o art. 7º do Marco Civil da Internet, serão abordados. Isso porque algumas discussões que giram em torno da exigibilidade de determinações judiciais[7] para acesso aos dados, em virtude de persecuções penais, merecem aprimoramento. Os princípios da necessidade, da proporcionalidade e da finalidade na coleta e no uso dos dados, além do consentimento para seu fornecimento, também serão aludidos nesse momento.

---

[4] GUIRAO, *Dimensiones constitucionales…,* p.27 e ss.
[5] GRECO, *Investigaciones internas…*, p. 118.
[6] GUIRAO, *Dimensiones constitucionales…,* p.59 e ss.
[7] O art. 7º, III, da Lei nº 12.965/14 ("Marco Civil da Internet") prevê a inviolabilidade do conteúdo de comunicações privadas armazenadas, salvo por ordem judicial.

O que se pretende elucidar é o que pode e/ou deve ser compartilhado com autoridades, quais são as autoridades que podem solicitar o conteúdo e qual a forma de solicitação legítima (ofício, determinação judicial, pedido amplo, específico etc). Ainda, se tal conteúdo poderia ser utilizado em eventual processo penal subsequente e o que seria protegido pelo sigilo entre cliente e advogado. Para tanto, dois cenários serão abordados: quando a empresa é incitada a entregar o conteúdo e quando é interesse da empresa entregá-lo.

À vista disso, a General Data Protection Regulation (GDPR) será estudada para fins comparativos, tal qual o Anteprojeto da Lei Geral de Proteção de Dados e suas recomendações.

Essas reflexões esbarram nas seguintes questões: quando solicitado, o que prevê a lei? O conteúdo deve ser compartilhado? Um simples ofício policial seria suficiente ou é necessária uma determinação judicial? Nesse caso, todo e qualquer conteúdo coletado pela equipe de investigação interna pode e deve ser compartilhado, ou parte dele seria considerado nulo devido à coleta desproporcional? O conceito de nulidade no processo penal teria o mesmo peso na investigação interna? Quem seria o responsável por fazer essa seleção antes da entrega às autoridades? O que está protegido pelo sigilo entre advogado e cliente?

Por fim, se os dados não forem solicitados, mas a empresa tiver o interesse de compartilhá-los, seria possível que o fizesse? Esse conflito[8] entre o direito de defesa e o direito do trabalhador também será objeto de análise.

3. Manifestação do problema na jurisprudência nacional (e estrangeira, se o caso)

Como se trata de tema recente, não há tantos julgados brasileiros. Porém, alguns merecem destaque, como o HC nº 674.185/MG, julgado pela Sexta Turma do Superior Tribunal de Justiça, no qual restou definido que é ilícita a tomada de dados, bem como das conversas de

[8]GUIRAO, *Dimensiones constitucionales…,* p. 83 e ss.

Whatsapp, obtidas diretamente pela autoridade policial em aparelho celular apreendido no flagrante, sem prévia autorização judicial[9].

Ainda sobre os direitos fundamentais que o colaborador permanece ostentando, já decidiu o Tribunal Regional do Trabalho da 9ª Região[10] que a realização de auditagem na estação de trabalho fere o direito ao sigilo de comunicação (CF/88, art. 5º, XII) e o parágrafo único do art.1º da Lei 9.296/96 equipara as comunicações em sistema de informática e telemática, via e-mail, às comunicações telefônicas, em relação às quais cabe a quebra do sigilo somente por determinação judicial. Portanto, seria ilegal a imposição de cláusula autorizadora de realização de auditagem na estação de trabalho dos usuários.

Na jurisprudência estrangeira encontramos delimitações sobre a comunicação a respeito da expectativa de privacidade. O Tribunal Europeu de Direitos Humanos (TEDH), ao interpretar o artigo 8.1 do Convênio Europeu dos Direitos Humanos, afirma que os colaboradores têm uma expectativa razoável de que a sua vida pessoal e familiar será respeitada quando do uso dos meios produtivos disponibilizados pela empresa, desde que o empregador não tenha expressamente proibido tais usos[11].

Na mesma oportunidade, o TEDH definiu que, uma vez desrespeitado o *nemo tenetur*, os documentos coletados em investigações internas não poderiam ser levados ao processo penal como se provas fossem.

Quanto à exclusão da prova por obtenção de atividade privada, ao serviço do Estado, condenou o Tribunal Supremo Espanhol[12] um grupo de pessoas por lavagem de dinheiro a partir de informações fornecidas por um colaborador da entidade bancária. A Sala Segunda

---

[9] BRASIL. Superior Tribunal de Justiça. HC n. 674.185/MG. Sexta Turma. Relator Ministro Sebastião Reis Júnior, julgado em 17/08/2021, publicado em 20/08/2021.

[10]TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO. TRT-PR-02822-2001-660-09-00-8 (RO05568-2002) – Acórdão -06845-2003. Rel. Juíza Janete do Amarante. Diário da Justiça Paraná, XLIX, Edição digitalizada N.6343, Curitiba, 6ª feira, 04 de abril de 2003. p.397. Disponível em: <https://www.tjpr.jus.br/diario-da-justica>. Acesso em: 05 de novembro de 2024.

[11] EUROPEAN COURT OF HUMAN RIGHTS. Case of Copland V. The United Kingdom.Application n.º 62617/00. Strasbourg, 03/04/2007. Disponível em: <https://www.juridice.ro/wp-content/uploads/2016/07/1531450.pdf >. Acesso em: 05 de novembro de 2024. Tradução livre da autora.

[12] STS 725/2020, de 3 de marzo {ECLI:ES:TS:2021:1489} D. Juan Ramón Berdugo Gómez de la Torre.

invocou a doutrina Falciane[13] para concluir que o colaborador do banco atuou sozinho, sem que sua atuação tivesse sido dirigida por forças do Estado, pois o colaborador estava desvinculado de estruturas estatais.

O Tribunal Supremo[14] também efetuou a condenação de dois diretores de uma empresa por apropriação indébita a partir da obtenção de determinados documentos por parte da própria empresa, em revisão documental interna. O Tribunal rechaçou a nulidade das provas, pois teriam sido obtidas de maneira casual e descartou também a presença de intermediação do Estado. Não se tratava de provas obtidas com objetivo direto e indireto de valer em um processo penal, segundo os magistrados.

De acordo com o Tribunal Supremo[15], a empresa não pode acessar conteúdo inequivocamente íntimo e que seja de antemão irrelevante para a finalidade da investigação. A inexistência de uma expectativa de privacidade não legitimaria a empresa a realizar uma supervisão ilimitada e desproporcional ao fim que se persegue. Portanto, é preciso informar ao trabalhador os fins, os meios e o alcance que pode ter a monitoração, por meio de protocolos de investigação internos e regulamentações do uso dos meios. Ainda, estipulou-se que é preciso, na supervisão, que se respeite o princípio da proporcionalidade.

4. Soluções propostas e zonas cinzentas

O equilíbrio entre a eficácia das investigações internas e o respeito às garantias do indivíduo merece estudo aprofundado, tanto em razão do escasso debate sobre o tema, quanto pela utilização do fenômeno da *criminalidade na empresa* como justificativa para a usurpação de todo e qualquer direito do indivíduo – neste caso, na figura do colaborador.

No Brasil, há uma lacuna legislativa a respeito e, as poucas diretrizes internacionais existentes, conflitam entre si. Enquanto os guias[16] emitidos pelo Departamento

---

[13] GUIRAO, *Dimensiones constitucionales…,* p. 38/39 e ss.
[14] STS 546/2019, de 11 de noviembre {ECLI:ES:TS:2019:3689} Dña. Carmen Lamela Díaz.
[15] STS 328/2021, de 24 de abril {ECLI:ES:TS:2021:1486} D. Manuel Marchena Gómez.
[16] U.S. Department of Justice Criminal Division: Guideline Evaluation of Corporate Compliance Programs (Updated September 2024), Acesso em: 06/12/2024. https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl.

de Justiça dos Estados Unidos incentivam o acesso pelas equipes de investigação interna, cada vez mais rápido e infindo aos dados dos colaboradores, as diretrizes européias resguardam o direito à privacidade do colaborador com relevante intensidade[17].

Diante desse panorama, a pesquisa visa explorar a tensão entre a necessidade das empresas de proteger seus interesses e as garantias dos indivíduos.

As consequências da violação às garantias também serão abordadas, a fim de apurar se tais provas obtidas – sem a cientificação ao trabalhador sobre a ausência de expectativa de privacidade ou coletadas de maneira desproporcional – poderão ser utilizadas em futuro processo penal[18]. Isso porque, a depender do meio invasivo e desproporcional utilizado pela equipe de investigação interna, a prova não estará apta a compor acervo probatório em processo penal, regido por regras e princípios diversos.

As investigações corporativas e o devido processo legal não sustentam o mesmo grau de garantia às pessoas submetidas a eles, já que essa aliança estratégica entre empresa e Estado gera, inicialmente, uma vulnerabilidade aos direitos e garantias processuais das pessoas físicas, pois está à margem do processo penal e, portanto, sem controle judicial[19].

Essa diferenciação de *standards* probatórios parece ocorrer diante das diferentes consequências entre um procedimento de investigação interna corporativa e um processo penal. Enquanto naquele a mais gravosa medida disciplinar seria o desligamento com justa causa, neste há possibilidade de pena privativa de liberdade, razão pela qual os seus requisitos probatórios seriam mais rígidos.

Não nos parece irrazoável que existam diferentes requisitos probatórios, na medida em que as equipes de investigação internas corporativas não possuem "*poder de polícia*", mecanismos e prerrogativas para realizar investigações aprofundadas, tampouco

---

[17] Na Espanha há um tipo penal (Artigo 197 do Código Penal Espanhol) que prevê a criminalização da revelação de segredos.
[18] ZACLIS, Daniel. *Investigação interna corporativa…*, p. 232 e ss.
[19] GUIRAO, *Dimensiones constitucionales…,* p. 08.

podem aplicar medidas como cerceamento de liberdade. O objetivo dos departamentos de compliance é, por natureza, prevenir cometimentos de delitos e, portanto, parece ser possível se valer de medidas mais invasivas para desligar colaboradores suspeitos. Do contrário, empresas seriam impelidas a manter possíveis detratores dentro de suas organizações privadas, pois não gozam das mesmas prerrogativas dos órgãos públicos para investigações aprofundadas. Nesse ponto, inicialmente nos parece que são dois ambientes diversos – investigações internas e ação penal – que merecem requisitos de licitude probatória também diversos.

O que não poderia ocorrer[20], todavia, é a utilização dessas provas – por meio de medidas mais invasivas – no âmbito judicial, à luz dos direitos e garantias que fundamentam o processo penal. A única razão que permitiria o uso de meios mais invasivos seria a baixa gravidade da consequência eventualmente imposta ao indivíduo.

Em posição contrária, alguns autores[21] entendem que se tratam de informações que são propriedade da empresa e, portanto, ela poderia dispor do seu sigilo. A priori, o argumento utilizado para fundamentar a posição não parece acertado. Na visão dos autores, as provas poderiam ser utilizadas em processo trabalhista e, portanto, também no processo penal. Contudo, as sanções entre a esfera trabalhista e penal são absolutamente desiguais, razão pela qual se exigiria *standards* probatórios diversos.

Uma das soluções propostas seria incumbir ao Data Protection Officer (DPO) a responsabilidade de diferenciar quais conteúdos poderiam ser compartilhados com as autoridades públicas. As suas atribuições legais serão exploradas para entender se a proposta seria viável.

Ao longo da pesquisa, seria utilizada a metodologia dedutiva, com estudo de casos e, se necessário, a metodologia indutiva para realização de entrevistas com especialistas

---

[20]GRECO, *Investigaciones internas…*, p. 110/111. Também em: GUIRAO, *Dimensiones constitucionales…,* p. 43/44 e ss.
[21]ZACLIS, Daniel. *Investigação interna corporativa…*, p. 237.

que atuam diariamente em procedimentos que envolvem o tema, pois entende-se que poderia trazer robustez à pesquisa.

5. Proposta preliminar de roteiro para a abordagem do problema

A proposta preliminar de sumário é:

Resumo

Introdução

1. Casos

1.1. Variáveis

2. Investigações internas: auto regulação corporativa

2.1. Conceito

2.2. Etapas

2.3. Ausência de expectativa de privacidade e máquinas corporativas

2.4. Incentivos normativos para investigações e acesso a dados

2.5. Síntese parcial

3. Regulamentações das investigações internas: limites e consequências

3.1. Diretrizes norte-americanas

3.1.1. U.S. Department of Justice Criminal Division: Evaluation of Corporate Compliance Programs (Guidelines)

3.2. Diretrizes européias

3.2.1. General Data Protection Regulation (GDPR)

3.3. Diretrizes brasileiras

3.3.1. Lei Geral de Proteção de Dados

3.3.2. Marco Civil da Internet

3.3.3. Anteprojeto da Lei Geral de Proteção de Dados

3.4. Síntese parcial

4. Sigilo advogado-cliente

4.1. Conceito

4.2. *Nemo tenetur*

4.3. Síntese parcial

5. Compartilhamento com autoridades públicas

5.1. Lei Geral de Proteção de Dados e determinações judiciais

5.2. Pedidos indeterminados: *fishing expedition*

5.3. Reaproveitamento da documentação em processo penal

5.3.1. Doutrina Falciani

5.3. Síntese parcial

6. Soluções dos casos

Conclusão

4. Bibliografia

ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. Revista de Investigações Constitucionais, Curitiba, vol. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280

ABREU, Jaqueline de Souza. Proteção da privacidade e cooperação jurídica internacional. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 156-169.

ABREU, Jaqueline. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel Ferreira; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). Tratado de proteção de dados pessoais. Rio de Janeiro, RJ: Editora Forense, 2021. p. 583–603.

ABREU, Jacqueline de Souza, ANTONIALLI, Dennys. Vigilância Sobre as Comunicações no Brasil. INTERNETLAB, São Paulo, 2017.

ALVES, Sérgio Garcia. Fechando um ciclo: do término do tratamento de dados pessoais (arts. 15 e 16 da LGPD). In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ivo Wolfgang e RODRIGUES JR., Otávio Luiz (coord.). Tratado de proteção de dados pessoais – 2ª ed. – Rio de Janeiro: Forense, 2023. ARAS, V. . O congelamento de dados informáticos para fins de prova no processo penal. Delictae - Revista de Estudos Interdisciplinares sobre o Direito , v. 8, p. 180-222, 2024.

AZEVEDO, Y. (2017). A importância da cadeia de custódia das provas para o devido processo legal. In Prado, G.; & Malan, D. (orgs.). Ensaios sobre a cadeia de custódia das provas no processo penal brasileiro, p. 106. Empório do Direito.

BADARÓ, Gustavo. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 51-69.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. Boletim IBCCRIM, ano 29, n. 343, p. 7-9, jun./2021.

BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo - 8. ed. - São Paulo: Saraiva, 2019.

BRASIL. Constituição da República Federativa do Brasil. Promulgada em 5 de outubro de 1988. Disponível em: 80 . Acesso em: 01 ago. 2024.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: . Acesso em: 24 set. 2024.

BRASIL. Superior Tribunal de Justiça. HC n. 674.185/MG. Sexta Turma. Relator Ministro Sebastião Reis Júnior, julgado em 17/08/2021, publicado em 20/08/2021.

COCA VILA, Ivó. ¿Programa de Cumplimiento como forma de autorregulación regulada? In: SILVA SÁNCHEZ, Jesús-María. Criminalidad de Empresa y Compliance. Barcelona: Atelier, 2013.

COFFEE JR., John. Corporate Crime and Punishment. The crisis of underenforcement. Oakland: Berrett-Koheler Publishers, 2020.

CORRÊA DA LUZ, Yuri. Bancos de dados públicos e o compartilhamento com agencias penais. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 170-181.

EUROPEAN COURT OF HUMAN RIGHTS. Case of Copland V. The United Kingdom.Application n.º 62617/00. Strasbourg, 03/04/2007.

FRAGOSO, Alexandre; FRAGOSO; Fernanda. A responsabilidade penal do compliance officer nas organizações. Belo Horizonte: São Paulo: D' Plácido, 2020.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. Rio de Janeiro: Marcial Pons, 2021.

GRECO, Luís; CARACAS, Christian. Investigaciones internas y la prohibición de la autoincriminación. Buenos Aires: En Letra Derecho Penal, Año VII, número 14, 2022, pp. 98-120.

GUIRAO, Rafael Alcácer. Dimensiones constitucionales de las investigaciones internas corporativas: expectativas de privacidad en la empresa e ilicitud de la prueba obtenida por particulares. Madrid: Revista de Responsabilidad Penal de Personas Jurídicas y Compliance, 2024.

ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. Direito Público, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5991. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5991. Acesso em: 12 set. 2023.

FERRAZ JUNIOR, Tércio Sampaio. O alcance da proteção do sigilo das comunicações no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 97-105.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública - 1ª ed. - Rio de Janeiro: Marcial Pons, 2021.

GLEIZER, Orlandino. A dogmática dos métodos ocultos de investigação no processo penal. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 119-129.

LUZ, Yuri. Bancos de dados públicos e o compartilhamento com agências penais. In: CRUZ, Francisco Brito; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital [livro eletrônico]. São Paulo: InternetLab, 2021, p. 170-181.

MACHADO, Eloísa. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 38-49.

MALAN, Diogo. Notas sobre a investigação e prova da criminalidade econômico-financeira organizada. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 2, n. 1, p. 213 - 238, 2016. http://dx.doi.org/10.22197/rbdpp.v2i1.2.

PRADO, Geraldo. Prova penal e sistema de controles epistêmicos: A quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons,
2014.

SILVA SÁNCHEZ, Jesús-María. La expansión del Derecho penal: Aspectos de la política criminal en las sociedades postindustriales. 2. ed. Montevideo: Editorial B de f, 2008.

ZACLIS, Daniel. Investigação interna corporativa: reflexos no Processo Penal. São Paulo: Thomson Reuters Brasil, 2023.