

ISSN 2526-0774

HomaPublica

REVISTA INTERNACIONAL DE
**DERECHOS HUMANOS
Y EMPRESAS**

Vol. X | Nº. 01 | Jun- Out 2026

Recebido: 10.06.2026 | Aceito: 08.08.2026 | Publicado: 08.10.2026

Os NOVOS SENHORES DA PROVA: COMPLIANCE DE PRIVACIDADE E O DEVER CORPORATIVO DE TUTELA DE DIREITOS FUNDAMENTAIS NAS REQUISIÇÕES CRIMINAIS

THE NEW LORDS OF EVIDENCE: PRIVACY COMPLIANCE AND THE CORPORATE DUTY TO PROTECT
FUNDAMENTAL RIGHTS IN CRIMINAL REQUESTS

Gustavo Henrique de Andrade Cordeiro¹

UNIVEM|São Paulo, Brasil| ORCID-ID0000-0002-4035-1628

Resumo

A prova digital encontra-se, hoje, majoritariamente sob a guarda de provedores e plataformas, de modo que a investigação penal depende de requisições dirigidas a entes privados. Ao recebê-las, a empresa ocupa posição de garante dos direitos fundamentais dos titulares dos dados, terceiros ausentes da relação requisitória. Este artigo investiga os limites do dever de colaboração e o papel do compliance de privacidade na tutela desses direitos. Adota-se o método dedutivo, com pesquisa bibliográfica, documental e jurisprudencial. Conclui-se que o dever de colaboração é limitado pela legalidade, pela reserva de jurisdição, pela proporcionalidade e pela minimização, que a observância dessas balizas reclama um compliance de privacidade estruturado e que a entrega excessiva de dados gera a ilicitude da prova, a quebra da cadeia de custódia e a responsabilização administrativa, civil e penal da empresa.

Palavras-chave

Compliance criminal. Proteção de dados. Prova digital. Reserva de jurisdição. Cadeia de custódia.

Abstract

Digital evidence is now mostly held by providers and platforms, so criminal investigation depends on requests addressed to private entities. Upon receiving them, the company acts as guarantor of the fundamental rights of data subjects, third parties absent from the requesting relationship. This article examines the limits of the duty to cooperate and the role of privacy compliance in safeguarding those rights. It adopts the deductive method, with bibliographical, documentary and case-law research. It concludes that the duty to cooperate is limited by legality, judicial reservation, proportionality and minimization, that observing these limits requires structured privacy compliance and that the excessive disclosure of data produces the unlawfulness of the evidence, the breaking of the chain of custody and the administrative, civil and criminal liability of the company.

Keywords

Criminal compliance. Data protection. Digital evidence. Judicial reservation. Chain of custody.

¹ Doutor e Mestre em Direito. Pró-Reitor Acadêmico e Professor da Graduação e do Mestrado no UNIVEM. Promotor de Justiça no Ministério Público do Estado de São Paulo.

1. INTRODUÇÃO

A investigação criminal contemporânea mudou de foco. Os vestígios do crime deixaram de estar apenas na cena física e passaram a residir em servidores, aplicativos e plataformas operados por empresas privadas. Mensagens, registros de conexão, metadados de localização, históricos de navegação e conteúdos armazenados em nuvem tornaram-se as provas mais cobiçadas da persecução penal, e quase todas elas estão sob a guarda de provedores. O resultado é uma dependência estrutural: para investigar, o Estado precisa pedir, e quem detém a chave do acervo probatório é a corporação.

Essa mudança coloca a empresa em uma posição inédita e delicada. Ao receber uma requisição estatal de dados, o provedor não decide apenas sobre interesses próprios; ele decide sobre direitos fundamentais de terceiros, os titulares dos dados, que sequer participam da relação entre a autoridade e a plataforma. O usuário cujos registros são solicitados raramente é ouvido – sequer tomando, muitas vezes, conhecimento do pedido –, e depende inteiramente de que a empresa avalie a legalidade da requisição e resista ao que for excessivo. O provedor torna-se, queira ou não, um garante de direitos fundamentais alheios.

A quebra do sigilo de dados é um gênero, que pode abranger o acesso a: 1) Dados bancários: informações privadas contidas em transações e transferências bancárias; 2) Dados fiscais: informações econômico-financeiras prestadas às Receitas Federal, Estadual ou Municipal; 3) Dados telefônicos: registros de operadoras de telefonia, abrangendo os números de telefone para os quais a pessoa realizou ou recebeu ligações, inclusive a data, o horário e a duração; ou 4) Dados informáticos: armazenadas em arquivos eletrônicos.

Em regra, para que a quebra do sigilo de dados seja lícita, é preciso a presença cumulativa de dois pressupostos: 1) Material: devida justificação constitucional; e 2) Formal: autorização por autoridade competente - ou seja, as autoridades judiciárias, o Corregedor Nacional de Justiça (em processo regularmente instaurado para apuração de infração por sujeito determinado, mediante decisão fundamentada e baseada em indícios concretos) ou as Comissões Parlamentares de Inquérito (estaduais ou federal – art. 58, § 3º, da Constituição de 1988).

Assim, há uma tensão estrutural entre dois deveres. De um lado, o dever de colaborar com a persecução penal, que decorre do interesse público na apuração de infrações penais, podendo o violador incorrer na prática do crime de desobediência ou, até mesmo, no delito previsto no artigo 2º, § 1º, da Lei nº 12.850/2013. De outro, o dever de proteger os direitos fundamentais dos titulares, que decorre da privacidade, do sigilo e da

proteção de dados pessoais². Entre colaborar e proteger, a empresa precisa decidir, e essa decisão não é técnica nem neutra: ela define quem terá seus direitos preservados e quem os terá sacrificados.

Daí o problema que orienta esta investigação: quais são os limites do dever de colaboração da empresa diante das requisições criminais, e de que modo o compliance de privacidade³ medeia a tutela dos direitos fundamentais de terceiros, especialmente quando a requisição é excessiva?

A questão é relevante porque a prática brasileira convive com requisições amplas, genéricas e por vezes desprovidas de ordem judicial, cujo atendimento acrítico pela empresa pode converter o provedor em instrumento de violação de direitos e contaminar a própria prova produzida.

O objetivo geral consiste em analisar os limites do dever de colaboração empresarial nas requisições criminais de dados e o papel do *compliance* de privacidade na tutela dos direitos fundamentais dos titulares. Para alcançá-lo, estabelecem-se três objetivos específicos: caracterizar a posição de garante da empresa na investigação mediada por provedores; examinar os limites jurídicos do dever de colaboração e as consequências da entrega excessiva sobre a licitude da prova; e investigar o compliance de privacidade e os regimes de responsabilização aplicáveis, propondo parâmetros de atuação.

Quanto à metodologia, adota-se o método dedutivo, partindo de premissas gerais sobre proteção de dados, legalidade e prova penal para alcançar conclusões específicas sobre o dever de colaboração empresarial. O método de procedimento combina o monográfico e o comparativo, com recurso pontual a parâmetros estrangeiros. As técnicas são a pesquisa bibliográfica, a documental e a jurisprudencial, de natureza exploratória e explicativa, mobilizando doutrina nacional e estrangeira, atos normativos e decisões dos tribunais superiores sobre o acesso a dados na investigação criminal.

O percurso organiza-se em três eixos. O primeiro caracteriza a empresa como garante de direitos fundamentais na investigação mediada por provedores, situando a privacidade e a proteção de dados como direitos dos titulares ausentes da relação requisitória. O segundo examina o dever de colaboração e seus limites, distinguindo os

² Sobre o tema, o art. 5º, XII, da Constituição de 1988, dispõe ser inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

³ O compliance de privacidade se relaciona com a proteção aos dados pessoais, envolvendo práticas de adequação às legislações de privacidade, com destaque para a Lei Geral de Proteção de Dados Pessoais (LGPD).

regimes de acesso e analisando a entrega excessiva como causa de ilicitude e de quebra da cadeia de custódia. O terceiro investiga o compliance de privacidade e a responsabilização corporativa, propondo um protocolo de atuação à luz da experiência comparada.

2. DA EMPRESA COMO GARANTE DE DIREITOS FUNDAMENTAIS NA INVESTIGAÇÃO MEDIADA POR PROVEDORES

2.1 A INVESTIGAÇÃO PENAL NA ERA DAS PLATAFORMAS E A GUARDA PRIVADA DA PROVA

A digitalização da vida transferiu para o setor privado o controle sobre os rastros que as pessoas deixam. Cada interação on-line gera dados que ficam armazenados nos sistemas de provedores de conexão e de aplicações, e é nesse acervo que a investigação criminal contemporânea busca seus elementos. Ferguson (2017) descreve a ascensão de um policiamento de dados, no qual a atividade investigativa se reorganiza em torno da coleta, do cruzamento e da análise de informações, deslocando o foco do trabalho de campo para o acesso a bases de dados mantidas por terceiros.

Brayne (2021), a partir de pesquisa empírica, demonstra como essa lógica se infiltra nas práticas cotidianas das instituições de segurança, ampliando o alcance da vigilância e tornando-a menos visível. A autora evidencia que a dependência de dados privados confere às empresas que os detêm um papel central, ainda que discreto, na investigação. A polícia e o Ministério Público passam a depender da colaboração das plataformas, e o ponto de acesso ao acervo probatório transfere-se, na prática, para o domínio corporativo.

Essa transferência tem consequências profundas no equilíbrio entre o Estado e o indivíduo. O acervo de dados de uma pessoa, espalhado por múltiplos serviços, permite reconstruir sua rotina, suas relações, suas opiniões e seus deslocamentos com um grau de detalhe que nenhuma investigação tradicional jamais alcançou. O'Neil (2016) alerta que sistemas que operam sobre grandes volumes de dados produzem efeitos de larga escala e difícil reversão, e que a aparência de objetividade técnica encobre escolhas e riscos que merecem escrutínio.

A concentração desse poder informacional em provedores privados cria uma assimetria estrutural. De um lado, o Estado, dotado de poder de requisição; de outro, o titular dos dados, frequentemente alheio ao que ocorre; e, no meio, a empresa, que detém a informação e processa o pedido. A posição intermediária do provedor não é uma circunstância acidental, mas o traço definidor da investigação penal contemporânea, e é dela que decorre o conjunto de deveres que este estudo procura delimitar.

Convém ressaltar que a dependência estatal em relação aos dados privados não é, em si, ilegítima. A apuração de crimes graves frequentemente depende do acesso a registros que só as plataformas possuem, e seria irrealista pretender que a investigação ignorasse essa realidade. O problema não está no acesso, mas nas condições, nos limites e nos controles para que a colaboração não se converta em devassa.

Assim, a dependência de dados privados redefine a própria noção de local do crime. Se antes a investigação se dirigia a um espaço físico determinado, hoje ela se dirige a servidores que podem estar em qualquer lugar do mundo, sob a gestão de empresas transnacionais. Essa desterritorialização da prova adiciona uma camada de complexidade, pois envolve questões de jurisdição e de cooperação que o pedido dirigido a um provedor nem sempre resolve, mas que tampouco autorizam o atalho da requisição irregular. Sobre o tema, o STF decidiu, inclusive, ser constitucional a requisição de dados e comunicações eletrônicas, por autoridades judiciárias brasileiras, a empresas de tecnologia (ex. Facebook e Google), ainda que os dados estejam armazenados em servidores localizados em outros países⁴.

Brayne (2021) observa que a integração de múltiplas bases de dados multiplica o poder de quem a elas tem acesso, pois a combinação de informações antes dispersas revela padrões que cada fonte isolada não revelaria. Essa capacidade de agregação, aplicada à investigação, torna ainda mais sensível a decisão sobre o que entregar, já que a soma de dados aparentemente desconexos pode produzir um retrato devassador da vida do titular, o que reforça a exigência de cautela no atendimento das requisições.

Convém registrar que essa realidade não é transitória, mas tende a se aprofundar. À medida que mais serviços migram para a nuvem e mais objetos se conectam à rede, amplia-se o volume e a variedade dos dados sob guarda privada. A investigação penal do futuro será, ainda mais do que a atual, uma investigação de dados, e isso torna urgente a definição de parâmetros claros para o acesso, antes que a prática consolide rotinas incompatíveis com as garantias.

A guarda privada da prova, portanto, é o pano de fundo de todo o debate. Ela explica por que a empresa se tornou um ator incontornável da persecução penal e por que a sua conduta, diante das requisições, adquiriu relevância jurídica de primeira ordem. Compreendida essa moldura, é preciso identificar quais são os direitos fundamentais que se encontram em jogo quando uma requisição é dirigida ao provedor, tarefa do subtópico seguinte.

⁴ ADC nº 51, Relator Min. Gilmar Mendes, julgada em 23/02/23, publicada em 28/04/2023.

2.2 PRIVACIDADE, SIGILO E PROTEÇÃO DE DADOS COMO DIREITOS FUNDAMENTAIS DOS TITULARES

A requisição de dados a um provedor incide diretamente sobre um feixe de direitos fundamentais do titular.

O primeiro deles é a privacidade, compreendida não apenas como o direito de estar só, mas como o poder de controlar a circulação das próprias informações. Atualmente, o direito à privacidade é vislumbrado enquanto gênero, tendo como espécies 1) a intimidade, 2) a vida privada, 3) a honra/imagem das pessoas e, para aqueles que o admitem, o direito ao esquecimento. Doneda (2019) descreve a evolução que conduziu da privacidade, concebida em termos individualistas, à proteção de dados pessoais, entendida como um instrumento de tutela da pessoa diante do tratamento automatizado de suas informações, com fundamento na dignidade e na autodeterminação informativa.

A proteção de dados consolidou-se como direito fundamental autônomo. Mendes (2014) demonstra que esse direito não se reduz à privacidade clássica, mas possui contornos próprios, voltados a assegurar transparência, finalidade e controle sobre o tratamento das informações pessoais. Bioni (2019) aprofunda essa construção ao analisar a função e os limites do consentimento, evidenciando que a autodeterminação informativa pressupõe que o titular saiba quem acessa seus dados, para qual finalidade e com quais garantias, exigências que a requisição estatal sigilosa tende a frustrar.

No plano constitucional, o sigilo dos dados e das comunicações encontra proteção expressa no art. 5º, incisos X e XII, da Constituição, e a inviolabilidade somente pode ser excepcionada nas hipóteses e na forma previstas em lei, mediante decisão fundamentada. A inclusão da proteção de dados pessoais entre os direitos fundamentais, pelo art. 5º, inciso LXXIX, acrescentado pela Emenda Constitucional 115, de 2022, reforçou esse patamar de tutela e conferiu assento constitucional a um direito que a jurisprudência já vinha reconhecendo, como evidenciou o Supremo Tribunal Federal, na Ação Direta de Inconstitucionalidade 6.387 MC/DF, ao suspender a medida provisória que determinava o compartilhamento de dados telefônicos para fins estatísticos, por configurar transferência massiva de informações sem salvaguardas adequadas. Não bastasse, o artigo 22 da Constituição foi acrescido do inciso XXX, que dispõe competir privativamente à União legislar sobre a proteção e tratamento de dados pessoais.

No âmbito infraconstitucional, o Código de Defesa do Consumidor regulamenta a matéria, especialmente no que concerne ao direito de acesso à informação, ao direito de retificação e ao limite temporal para manutenção dos dados.

Ademais, a Lei nº 12.414/2011, também conhecida como “Lei do Cadastro Positivo”, veda o armazenamento de dados sensíveis e excessivos, dispondo, ainda, sobre o acesso aos principais elementos da análise de risco.

Não bastasse, a Lei nº 12.527/2011, conhecida como “Lei de Acesso à Informação”, disciplina de forma geral o tratamento de informações pessoais.

A Lei nº 12.965/2014, conhecida como “Marco Civil da Internet”, contempla inúmeras disposições sobre a proteção de dados.

Por fim, a Lei Geral de Proteção de Dados (Lei 13.709/2018) estruturou o regime infraconstitucional dessa tutela, fixando, em seu art. 6º, princípios como a finalidade, a adequação, a necessidade e a transparência. Embora o tratamento de dados para fins de segurança pública e persecução penal tenha sido excluído de seu âmbito direto pelo art. 4º, inciso III, remetido a legislação específica ainda pendente, os princípios que a inspiram irradiam-se sobre todo o ordenamento e oferecem parâmetros interpretativos para o exame das requisições criminais, sobretudo no que tange à minimização e à proporcionalidade do que é solicitado.

Esses direitos pertencem ao titular dos dados, e não ao provedor. Essa observação, aparentemente óbvia, é decisiva, pois significa que a empresa, ao decidir sobre uma requisição, dispõe sobre direitos alheios. Pasquale (2015) adverte que o poder de controlar informações alheias, quando exercido sem transparência, converte-se em poder sobre as próprias pessoas, e que a opacidade desse exercício é incompatível com a tutela efetiva dos direitos envolvidos.

Importa distinguir os diferentes tipos de dados quanto à sua sensibilidade. Há informações meramente identificadoras e há dados que revelam aspectos íntimos da personalidade, como convicções, deslocamentos e relações. Doneda (2019) adverte que o regime de proteção deve ser proporcional à sensibilidade da informação, de modo que quanto mais reveladores os dados, mais rigorosas devem ser as exigências para o seu acesso, lógica que se projeta diretamente sobre o exame das requisições criminais⁵.

A proteção de dados, ademais, não é um obstáculo à segurança, mas uma condição da confiança que a sustenta. Mendes (2014) sublinha que um regime sólido de proteção é o

⁵ A título de exemplo, as conversas travadas através do WhatsApp ou SMS (textos, áudios, dentre outros) são resguardadas pelo sigilo das comunicações, de modo que terceiros somente podem ter acesso mediante: a) consentimento dos participantes ou b) autorização judicial. Caso ocorra o compartilhamento em grupos de WhatsApp ou a mensagem seja levada a conhecimento público, “além da quebra da confidencialidade, estará configurada a violação à legítima expectativa, bem como à privacidade e à intimidade do emissor, sendo possível a responsabilização daquele que procedeu à divulgação se configurado o dano.” (STJ. 3ª Turma. REsp 1.903.273-PR, Rel. Min. Nancy Andrighi, julgado em 24/08/2021)

que permite às pessoas participarem do ambiente digital sem o temor de uma vigilância indiscriminada. Quando o acesso estatal a dados ocorre sem limites, erode-se essa confiança, e o custo dessa erosão recai sobre a própria legitimidade das instituições, inclusive das de persecução penal.

A jurisprudência constitucional acompanhou essa evolução. Ao reconhecer a proteção de dados como direito fundamental autônomo, o ordenamento brasileiro conferiu a essa tutela um peso que condiciona a interpretação de todas as normas de acesso. Disso resulta que as hipóteses de quebra do sigilo devem ser interpretadas restritivamente, e que a dúvida sobre a legitimidade do acesso deve resolver-se em favor da proteção do titular - e não da conveniência do investigador.

Há, ainda, uma dimensão coletiva da proteção de dados que o debate sobre requisições costuma negligenciar. Quando o acesso a dados se torna prática rotineira e ampla, o efeito não recai apenas sobre os indivíduos diretamente investigados, mas sobre a coletividade de usuários, que passa a viver sob a expectativa difusa de vigilância. Bioni (2019) observa que a proteção de dados tutela também um interesse social, ligado à preservação de um ambiente informacional livre, cuja erosão afeta a todos, e não apenas aos titulares pontualmente atingidos.

A consequência dessa configuração é que a proteção dos direitos do titular, no momento da requisição, depende de quem detém os dados. Como o titular está ausente e o Estado é o requerente, resta ao provedor a função de anteparo. Compreender a natureza dos direitos em jogo é, portanto, o passo necessário para compreender a posição de garante que a empresa ocupa, tema do subtópico final deste eixo.

2.3 A POSIÇÃO DE GARANTE DO PROVEDOR E O TITULAR COMO TERCEIRO AUSENTE

O traço mais singular da requisição criminal de dados é a ausência do principal interessado. Quando a autoridade dirige o pedido ao provedor, o titular dos dados não é parte, não é notificado e não tem oportunidade de se manifestar. A relação estabelece-se entre o Estado e a empresa, mas seus efeitos recaem sobre um terceiro que dela não participa. Essa estrutura triangular, em que o afetado é o ausente, é o que confere ao provedor a sua peculiar posição de garante.

Leonardi (2011), ao analisar a tutela da privacidade na internet, já apontava que os provedores ocupam posição central na proteção dos dados de seus usuários, pois são eles que detêm tecnicamente a informação e que executam, ou recusam, as solicitações de acesso. Essa centralidade técnica converte-se em responsabilidade jurídica: a empresa que

detém os dados é a única em condições de avaliar, no momento do pedido, se a requisição observa os limites legais e de resistir ao que os ultrapassa.

A posição de garante não é uma construção retórica, mas uma decorrência da estrutura da relação. Bioni (2019) observa que a autodeterminação informativa do titular só é efetiva se houver, ao longo de todo o fluxo de dados, atores comprometidos com a sua proteção. Quando o titular está ausente, esse compromisso recai sobre o provedor, que passa a exercer uma espécie de tutela em favor de quem não pode se defender, função que o aproxima da figura do garantidor de direitos alheios.

Essa função impõe deveres que vão além do simples cumprimento mecânico de ofícios. O provedor que atende a qualquer requisição sem examinar a sua legalidade, que entrega mais do que o solicitado ou que deixa de exigir a ordem judicial cabível não é um colaborador diligente da justiça, mas um agente que falha no seu dever de proteção. A posição de garante, portanto, exige uma postura ativa de verificação e, quando necessário, de recusa fundamentada.

Pasquale (2015) reforça que a concentração de informações em entes privados, sem mecanismos de transparência e controle, transfere a esses entes um poder que precisa ser disciplinado. No contexto das requisições criminais, isso significa que a discricionariedade do provedor não pode ser absoluta nem arbitrária: ela deve orientar-se pelos direitos do titular e pelos limites legais, sob pena de a empresa se tornar coautora da violação que deveria evitar.

A posição de garante do provedor encontra paralelo na ideia dos deveres de proteção que o direito atribui a quem detém o controle sobre bens jurídicos alheios. Assim como determinados agentes respondem por não impedir um resultado que tinham o dever de evitar, o provedor que detém os dados de terceiros assume o dever correlato de não permitir o seu acesso indevido. A omissão diante de uma requisição manifestamente ilegal não é neutralidade, mas participação na lesão.

Contudo, é preciso ponderar que, na dogmática penal clássica, o garantidor responde pela omissão de um dever de agir para evitar um resultado lesivo. No ambiente digital, todavia, essa relação ganha novos contornos a partir da eficácia horizontal direta dos direitos fundamentais⁶, de modo a mitigar as assimetrias de poder informacional. O

⁶ Sobre o tema, o STF já decidiu que “[...] A autonomia privada, que encontra claras limitações de ordem jurídica, não pode ser exercida em detrimento ou com desrespeito aos direitos e garantias de terceiros, especialmente aqueles positivados em sede constitucional, pois a autonomia da vontade não confere aos particulares, no domínio de sua incidência e atuação, o poder de transgredir ou de ignorar as restrições postas e definidas pela própria Constituição, cuja eficácia e força normativa também se impõem, aos particulares, no âmbito de suas relações privadas, em tema de liberdades fundamentais.” (STF, RE 201.819/RJ, rel. p/ acórdão: Min. Gilmar Mendes, rel. Originária: Min. Ellen Gracie, Segunda Turma, j. 11/10/2005, DJ 27-10-2006).

provedor deixa de ser um mero destinatário passivo de ordens estatais e assume deveres de proteção (*Schutzpflichten*)⁷ originariamente atribuídos ao Estado, mas cuja eficácia prática foi materialmente transferida a quem detém o controle técnico dos dados.

Não se trata, portanto, de aplicação de função de garante por analogia, mas de atentar para o fato de que a privacidade e o compliance de dados constituem a face corporativa do dever de proteção dos direitos fundamentais na era digital.

Indo além, é possível falar em garantismo informacional corporativo. Diferente dos deveres de proteção tradicionais, em que a omissão privada pressupõe um nexo de causalidade puramente naturalístico com o dano, a custódia de dados na era das plataformas exige uma nova forma de atuação.

Desse modo, o garantismo informacional corporativo exige um dever de blindagem procedimental pela empresa, transformando o fluxo do compliance em uma extensão das garantias constitucionais. Ao receber a requisição, a plataforma opera uma filtragem de constitucionalidade que impede o arbítrio antes mesmo que este ingresse no processo penal. A responsabilidade corporativa, portanto, tona-se indispensável para mitigar a erosão silenciosa de garantias constitucionais.

Essa responsabilidade, contudo, não transforma o provedor em juiz da causa. Não se espera que a empresa decida sobre o mérito da investigação, mas que verifique a regularidade formal e a legalidade do pedido, exigindo a via adequada e a ordem judicial quando cabível. O papel do garante é de filtro de legalidade, não de árbitro do litígio, e essa delimitação é importante para que o dever de proteção não se confunda com indevida ingerência na atividade investigativa legítima.

Essa função de garante, fundada no dever de proteção, não é incompatível com a colaboração leal com a justiça. O provedor que filtra a legalidade dos pedidos e atende ao que é regular contribui para uma persecução penal adequada, pois assegura que as provas produzidas resistam ao controle judicial. Proteger o titular e colaborar com a justiça, longe de serem posições divergentes, convergem na produção de uma prova lícita, confiável e apta a sustentar a responsabilização dos culpados.

Reconhecida a posição de garante, abre-se a questão central deste estudo: até onde vai o dever de colaborar e onde começa o dever de proteger? A resposta depende da

⁷A dimensão objetiva dos direitos fundamentais aparece, inicialmente, na sentença do caso Lüth, decisão histórica do Tribunal Federal Constitucional Alemão, proferida em 1958, em que se reconheceu os contornos do “dever de proteção estatal” (*Schutzpflicht des Staates*) e, posteriormente, da “proibição de proteção insuficiente” (*Untermaßverbot*) e da “proibição de excesso” (*Übermaßverbot*).

análise dos limites jurídicos do dever de colaboração, dos regimes diferenciados de acesso a dados e das consequências da entrega excessiva, temas que o eixo seguinte enfrenta de modo sistemático.

3. O DEVER DE COLABORAÇÃO E SEUS LIMITES: LEGALIDADE E LICITUDE DA PROVA

3.1 O REGIME DO MARCO CIVIL: DADOS CADASTRAIS, REGISTROS E CONTEÚDO

O ordenamento brasileiro não trata todos os dados do mesmo modo, e essa diferenciação é a chave para compreender os limites do dever de colaboração⁸.

O Marco Civil da Internet estabeleceu um regime escalonado, no qual a intensidade da proteção varia conforme a natureza da informação solicitada. Distinguem-se, de um lado, os dados cadastrais e, de outro, os registros de conexão e de acesso a aplicações, bem como o conteúdo das comunicações privadas, cada categoria submetida a um regime próprio de acesso.

Os dados cadastrais, que informam a qualificação pessoal, a filiação e o endereço do usuário, podem ser requisitados diretamente por autoridades administrativas que detenham competência legal, sem necessidade de ordem judicial, conforme o art. 10, §3º, da Lei 12.965/2014, em previsão que dialoga com o art. 17-B da Lei 9.613/1998 e com o art. 15 da Lei 12.850/2013. Trata-se de uma exceção pontual, justificada pelo caráter identificador e menos sensível dessas informações, e que não autoriza, por si, o acesso a qualquer outro tipo de dado.

Os registros de conexão e de acesso a aplicações, bem como o conteúdo das comunicações privadas, submetem-se a regime distinto e mais rigoroso. A sua disponibilização depende de ordem judicial, nos termos do art. 10, §§1º e 2º, e dos arts. 22 e 23 da Lei 12.965/2014, e a requisição deve observar os requisitos do parágrafo único do art. 22, entre os quais os fundados indícios da ocorrência do ilícito, a justificativa motivada da utilidade dos registros para a investigação e a indicação do período a que se referem. O Decreto 8.771/2016, que regulamenta a lei, reforça esse rigor ao vedar pedidos coletivos genéricos ou inespecíficos.

Leonardi (2011) sublinha que essa diferenciação cumpre a função de equilibrar o interesse na investigação com a proteção da privacidade, evitando que o acesso a

⁸ A quebra do sigilo de dados é um gênero, que pode abranger o acesso a: 1) Dados bancários: informações privadas contidas em transações e transferências bancárias; 2) Dados fiscais: informações econômico-financeiras prestadas às Receitas Federal, Estadual ou Municipal; 3) Dados telefônicos: registros de operadoras de telefonia, abrangendo os números de telefone para os quais a pessoa realizou ou recebeu ligações, inclusive a data, o horário e a duração; ou 4) Dados informáticos: armazenadas em arquivos eletrônicos (COSTA, 2024, p. 654).

informações sensíveis ocorra sem o crivo do juiz. A reserva de jurisdição, nesse ponto, não é uma formalidade, mas uma garantia substancial: ela interpõe, entre o desejo de acesso e a obtenção do dado, a avaliação de um terceiro imparcial sobre a necessidade e a proporcionalidade da medida.

Para o provedor, esse regime escalonado é o primeiro parâmetro de conduta. Atender a uma requisição administrativa direta de conteúdo de comunicações, por exemplo, significa entregar, sem ordem judicial, aquilo que a lei expressamente reservou ao juiz. O cumprimento acrítico de um pedido que extrapola a categoria de dados legalmente acessível por aquela via configura, da parte da empresa, descumprimento do seu dever de proteção, e não exercício do dever de colaborar.

Contudo, a previsão de acesso direto a dados cadastrais comporta limites que não podem ser ignorados. O regulamento da lei exige que a autoridade indique o fundamento legal de sua competência e a motivação do pedido, e veda solicitações coletivas, genéricas ou inespecíficas. Disso decorre que mesmo a requisição direta de dados cadastrais, supostamente menos sensível, não autoriza pedidos em massa nem dispensa a individualização, sob pena de converter uma exceção pontual em instrumento de vigilância ampla.

A interpretação dessas categorias deve ser restritiva, e não expansiva. A dúvida sobre a natureza do dado solicitado deve resolver-se em favor da maior proteção, exigindo-se ordem judicial quando não for inequívoco tratar-se de simples dado cadastral. Essa diretriz hermenêutica protege o titular contra a erosão das garantias constitucionais por meio da reclassificação conveniente dos dados, prática que esvaziaria a reserva de jurisdição ao rotular como cadastral aquilo que, na verdade, revela conteúdo ou comportamento.

A prática forense, contudo, frequentemente ignora essa distinção. Não são raras as requisições que, sob o rótulo de pedido de dados cadastrais, buscam na verdade registros de acesso ou conteúdo, ou que dirigem a provedores exigências amplas sem a correspondente ordem judicial. Cabe à empresa, no exercício de sua função de garante, recusar a confusão entre as categorias e exigir, para cada tipo de dado, a via de acesso que a lei lhe reserva, independentemente da forma como o pedido se apresenta.

A correta classificação do dado solicitado é, portanto, o ponto de partida de qualquer decisão diligente. Antes de entregar, o provedor precisa identificar de que categoria se trata, qual o regime de acesso aplicável e se a autoridade requerente detém competência para o pedido naquela forma. Essa triagem inicial conduz à questão seguinte,

relativa aos princípios que governam o acesso mesmo quando a via adequada é observada: a reserva de jurisdição, a proporcionalidade e a minimização.

3.2 RESERVA DE JURISDIÇÃO, PROPORCIONALIDADE E OS LIMITES DA REQUISIÇÃO DIRETA

A reserva de jurisdição é a pedra angular do regime de acesso a dados sensíveis. Ela traduz a exigência de que a quebra do sigilo seja autorizada por decisão judicial fundamentada, e não decidida unilateralmente pela autoridade interessada na investigação⁹. Ferrajoli (2002), ao formular a teoria do garantismo, sustenta que o poder punitivo só se legitima quando estritamente vinculado à lei e submetido a controles, e a reserva de jurisdição é precisamente um desses controles, voltado a impedir o acesso arbitrário à esfera privada.

A jurisprudência brasileira tem trabalhado essa fronteira com nuances importantes. No julgamento do Tema 990 da repercussão geral (Recurso Extraordinário 1.055.941/SP), relativo ao compartilhamento de dados financeiros, o Supremo Tribunal Federal admitiu a transmissão, aos órgãos de persecução penal e sem prévia autorização judicial, dos relatórios de inteligência financeira e da íntegra dos procedimentos fiscalizatórios, desde que resguardado o sigilo e formalizado o procedimento. A decisão, contudo, referiu-se ao compartilhamento espontâneo pelos órgãos de controle, e não autorizou a requisição direta dos dados pelos órgãos de investigação.

Estellita (2022) explora justamente os limites dessa transmissão, alertando para a distinção entre o compartilhamento espontâneo, admitido, e a solicitação direta, que pressupõe controle judicial. Essa distinção tornou-se centro de importante debate atual. O Superior Tribunal de Justiça firmou, em sua Terceira Seção, ao julgar o Agravo Regimental no Recurso em Habeas Corpus 174.173/RJ, o entendimento de que a polícia e o Ministério Público não podem solicitar relatórios diretamente aos órgãos de inteligência financeira sem prévia autorização judicial, e a Segunda Turma do Supremo Tribunal Federal, no Recurso Extraordinário 1.393.219 AgR/SP, decidiu, no mesmo sentido, que o Ministério

⁹ Sobre o tema, o STF já decidiu que “O postulado da reserva constitucional de jurisdição importa em submeter, à esfera única de decisão dos magistrados, a prática de determinados atos cuja realização, por efeito de explícita determinação constante do próprio texto da Carta Política, somente pode emanar do juiz, e não de terceiros, inclusive daqueles a quem se haja eventualmente atribuído o exercício de ‘poderes de investigação próprios das autoridades judiciais’. A cláusula constitucional da reserva de jurisdição - que incide sobre determinadas matérias, como a busca domiciliar (CF, art. 5º, XI), a interceptação telefônica (CF, art. 5º, XII) e a decretação da prisão de qualquer pessoa, ressalvada a hipótese de flagrância (CF, art. 5º, LXI) - traduz a noção de que, nesses temas específicos, assiste ao Poder Judiciário, não apenas o direito de proferir a última palavra, mas, sobretudo, a prerrogativa de dizer, desde logo, a primeira palavra, excluindo-se [...] a possibilidade do exercício de iguais atribuições, por parte de quaisquer outros órgãos ou autoridades (...)” (MS n. 23.452/RJ, Segunda Turma, Rel. Min. Celso de Mello, DJe de 12/5/2000).

Público não pode requisitar diretamente dados à administração fazendária sem o crivo do juiz.

A controvérsia permanece viva, com o Tema 1.404 da repercussão geral (Recurso Extraordinário 1.537.165/SP) pendente de julgamento pelo Plenário sobre o alcance da requisição direta, o que revela a delicadeza do equilíbrio entre eficiência e garantia. Para os fins deste estudo, importa o princípio que dela emerge: a iniciativa de acesso a dados sigilosos por parte do órgão investigador tende a exigir autorização judicial, ao passo que o compartilhamento espontâneo por órgãos de controle, em procedimento formal e sigiloso, recebe tratamento distinto.

Esse mesmo princípio governa as requisições dirigidas a provedores. A proporcionalidade exige que o acesso seja adequado, necessário e proporcional em sentido estrito, e a minimização impõe que se solicite apenas o estritamente indispensável à investigação, pelo período estritamente necessário. Uma requisição que pede tudo sobre alguém, sem recorte temporal ou material, é o oposto da minimização e não pode ser atendida como se fosse um pedido legítimo, ainda que revestida da aparência de um ofício regular.

A controvérsia sobre a requisição direta tem fundamento constitucional. A exigência de autorização judicial para o acesso a dados sigilosos decorre da proteção da intimidade e do sigilo, que só podem ceder mediante decisão fundamentada de autoridade imparcial. Ferrajoli (2002) recorda que a interposição do juiz entre o poder investigativo e a esfera privada é uma garantia contra a confusão entre acusar e decidir, confusão que se reproduziria se o próprio órgão interessado pudesse determinar o acesso aos dados.

A proporcionalidade, por sua vez, opera em dois momentos. No momento do pedido, exige que a autoridade demonstre a necessidade e a adequação da medida; no momento do atendimento, exige que o provedor verifique se a requisição respeita esses limites. A dupla incidência da proporcionalidade reforça a posição de garante da empresa, que não pode escudar-se na mera existência de um ofício para entregar dados cujo acesso não foi adequadamente justificado nem judicialmente autorizado, quando esta era a via exigível.

A tendência de contenção observada na jurisprudência recente sinaliza um amadurecimento institucional. Ao restringir a requisição direta e reafirmar a reserva de jurisdição, os tribunais superiores reconhecem que a eficiência da investigação não pode ser obtida pela supressão de garantias, e que o atalho do acesso direto, embora mais cômodo, fragiliza-as e expõe a prova à invalidação. Essa orientação oferece ao provedor um respaldo para resistir a pedidos que ignorem o crivo judicial.

Assim, a distinção entre compartilhamento espontâneo e requisição direta, embora sutil, é juridicamente decisiva. No primeiro, a iniciativa parte de um órgão que, no exercício de sua competência fiscalizatória, identifica indícios e os comunica; no segundo, é o órgão de persecução que, movido pelo interesse na prova, vai buscar o dado. A diferença não é meramente procedimental, pois toca a imparcialidade do acesso: admitir que o investigador determine sozinho a quebra do sigilo seria conferir-lhe um poder que a Constituição de 1988 reservou ao juiz.

O caso do congelamento de contas eletrônicas decidido pelo Supremo Tribunal Federal, no Habeas Corpus 222.141 AgR/PR, ilustra a consequência do desrespeito a esses limites. Ao anular provas obtidas a partir da preservação e do acesso ao conteúdo de contas sem prévia autorização judicial, a Corte deixou claro que a inobservância da reserva de jurisdição contamina a prova. A lição para o provedor é direta: atender a um pedido que ignora a reserva de jurisdição não é colaborar com a justiça, mas participar da produção de uma prova ilícita, tema do subtópico seguinte.

3.3 ENTREGA EXCESSIVA, PROVA ILÍCITA E CADEIA DE CUSTÓDIA DA PROVA DIGITAL

A entrega excessiva de dados pelo provedor produz consequências que vão muito além da violação da privacidade do titular. Quando a empresa fornece mais do que foi requisitado, ou atende a um pedido que ultrapassa os limites legais, a prova assim obtida nasce viciada. Lopes Jr. (2020) enfatiza que a licitude é condição de admissibilidade da prova no processo penal democrático, e que provas obtidas com violação de direitos fundamentais devem ser desentranhadas, por força da vedação do art. 5º, inciso LVI, da Constituição de 1988 e do art. 157 do Código de Processo Penal.

A ilicitude, nesse caso, decorre tanto da ausência de fundamento adequado para o acesso quanto do excesso na coleta. Uma requisição autorizada para um período ou um conjunto específico de dados não legitima a entrega de um acervo mais amplo, e o que exceder o autorizado é prova obtida por meio ilícito. O provedor que entrega demais não apenas viola o direito do titular, mas injeta no processo um elemento contaminado, cuja utilização compromete a validade da persecução.

A questão articula-se de modo decisivo com a cadeia de custódia da prova digital. A reforma processual de 2019 incorporou ao Código de Processo Penal a disciplina expressa da cadeia de custódia, nos arts. 158-A a 158-F, incluídos pela Lei 13.964/2019, definindo as etapas de rastreamento do vestígio desde a sua coleta até o seu descarte, com o objetivo de assegurar a integridade e a autenticidade da prova. Prado (2019) sustenta que a cadeia de custódia é condição epistêmica de confiabilidade do material probatório, e que a sua quebra compromete o valor da prova e o próprio direito de defesa.

No ambiente digital, a cadeia de custódia adquire complexidade adicional. A facilidade de alteração, duplicação e manipulação dos dados exige rastreabilidade rigorosa de cada etapa, desde a extração pelo provedor até a juntada aos autos. A entrega excessiva ou desordenada, sem documentação adequada da origem e do método de obtenção, fragiliza essa rastreabilidade e abre espaço para a contestação da autenticidade, comprometendo a própria utilidade do material para a investigação.

O provedor, nesse contexto, é o elo inicial da cadeia. A forma como a empresa coleta, seleciona e transmite os dados condiciona a integridade de toda a prova subsequente. Uma coleta excessiva, além de ilícita, introduz ruído e dificulta a delimitação do que é efetivamente pertinente, ao passo que uma coleta documentada preserva tanto os direitos do titular, quanto a higidez probatória. A diligência da empresa, portanto, é simultaneamente uma garantia de direitos e uma garantia de qualidade da prova.

A doutrina da quebra da cadeia de custódia tem ganhado densidade na jurisprudência, que passou a reconhecer que a ausência de rastreabilidade compromete a confiabilidade da prova. Prado (2019) sustenta que a cadeia de custódia integra o direito à prova e o direito de defesa, pois sem ela a parte não tem como verificar a autenticidade e a integridade do material, ficando à mercê de uma fonte cuja idoneidade não pode controlar. No ambiente digital, essa vulnerabilidade é potencializada pela facilidade de manipulação.

A entrega excessiva também produz um efeito processual menos evidente, mas relevante: a dificuldade de delimitar o objeto da prova. Quando o provedor fornece um acervo amplo e indiferenciado, a defesa e o próprio juízo enfrentam o desafio de separar o pertinente do impertinente, e a investigação corre o risco de transformar-se em uma pesca probatória, na qual se vasculha tudo à procura de qualquer coisa. Lopes Jr. (2020) adverte que essa lógica é incompatível com um processo penal de garantias, orientado por imputações determinadas.

A consequência prática dessa articulação é que a diligência na coleta deixa de ser um ônus e passa a ser um investimento na solidez da prova. Uma extração minimizada, documentada e rastreável produz material robusto, capaz de resistir às impugnações da defesa, ao passo que a coleta excessiva e desordenada gera prova frágil, vulnerável à anulação. A boa técnica, nesse campo, coincide com o respeito aos direitos, e a empresa que a observa serve simultaneamente à justiça e à pessoa investigada.

Essa exigência de rastreabilidade impõe deveres concretos ao provedor no momento da extração. A empresa deve registrar a origem dos dados, o método de coleta, a data e o responsável, de modo a permitir a reconstituição posterior do caminho percorrido pela prova. A ausência desses registros, ainda que a coleta tenha sido regular quanto ao

mérito, fragiliza a prova ao impedir a verificação de sua integridade, o que demonstra que a forma, no tratamento da prova digital, é parte indissociável da substância.

Constata-se, assim, que a proteção dos direitos do titular e a licitude da prova caminham juntas. A entrega excessiva fere o titular e contamina o processo, ao passo que a colaboração diligente, limitada ao estritamente requisitado e devidamente documentada, serve simultaneamente à justiça e às garantias constitucionais. Resta examinar como a empresa pode estruturar-se para cumprir esse papel de modo consistente, o que conduz ao eixo final, dedicado ao compliance de privacidade e à responsabilização corporativa.

4. COMPLIANCE DE PRIVACIDADE E RESPONSABILIZAÇÃO CORPORATIVA

4.1 CRIMINAL COMPLIANCE E O DEVER EMPRESARIAL DE PROTEÇÃO DE DADOS DE TERCEIROS

O cumprimento adequado dos deveres da empresa diante das requisições criminais não pode depender da sensibilidade individual de quem atende ao pedido. Ele exige estrutura, e essa estrutura é precisamente o objeto do *compliance*.

A expressão "*compliance*" designa um conjunto de medidas adotadas por pessoas jurídicas públicas ou privadas visando a garantir o cumprimento do ordenamento jurídico e de princípios de ética e integridade. Tradicionalmente, os programas de *compliance* foram aplicados no âmbito das corporações (*corporate compliance*), com o intuito de garantir o cumprimento do ordenamento jurídico no âmbito negocial (Junqueira, 2019).

Mais recentemente, contudo, muito se tem falado em *criminal compliance*. A ideia consiste em abandonar a perspectiva meramente reativa na esfera penal, para alcançar uma concepção preventiva de combate à criminalidade e evitar, assim, a ocorrência de delitos (Silva Sánchez, 2013). Silveira e Saad-Diniz (2015) descrevem o *criminal compliance* como o conjunto de mecanismos de organização interna voltados a prevenir a prática de ilícitos no âmbito empresarial, deslocando a responsabilidade do plano meramente individual para o plano da organização e de seus deveres de cuidado.

Nieto Martín (2015) sistematiza os elementos dos programas de cumprimento, entre os quais a identificação e a avaliação de riscos, a definição de procedimentos, a designação de responsáveis, os canais de comunicação e os mecanismos de controle e revisão. Transposto para o tratamento de requisições de dados, esse arcabouço implica que a empresa disponha de políticas claras sobre como receber, avaliar e responder aos pedidos estatais, de modo a assegurar que cada requisição seja submetida a um crivo de legalidade antes de qualquer entrega.

O *compliance* de privacidade é, nesse sentido, a tradução desses princípios para o campo da proteção de dados. Ele compreende a existência de um encarregado de dados, a documentação dos fluxos de tratamento, a definição de critérios para a triagem das requisições e a previsão de procedimentos de resposta que contemplem a verificação da competência da autoridade, da via adequada e da existência de ordem judicial quando exigível. Saad-Diniz (2019) observa que a efetividade do *compliance* depende menos da existência formal de programas e mais da sua incorporação real à cultura e às decisões da empresa.

Um elemento central desse compliance é a capacidade de resistência fundamentada, por vezes designada como *push-back*. Diante de uma requisição excessiva, genérica ou desprovida de base legal, a empresa diligente não deve simplesmente cumprir, mas questionar, exigir esclarecimentos, requerer a ordem judicial cabível ou, se necessário, recusar o atendimento e submeter a questão ao crivo do juiz. Essa resistência não é obstrução à justiça, mas exercício do dever de proteção que decorre da posição de garante.

Impende destacar que a imposição de um dever generalizado de repúdio (*push-back*) a requisições pode retardar o tempo de resposta da persecução penal. Se o retardamento no fornecimento de dados inviabilizar a elucidação de crimes graves e de alta lesividade social, a proteção da privacidade individual pode reduzir a eficácia do sistema persecutório. Para solucionar esse problema, a oposição deve atentar para hipóteses em que o pedido estatal evidenciar contornos de uma pescaria probatória (*fishing expedition*), em que o benefício da produção da prova para o Estado é amplamente superado pela necessidade de proteção da privacidade.

Ademais, o *compliance* de privacidade também impõe transparência possível. Na medida em que a lei e o sigilo da investigação permitam, a empresa deve manter registros das requisições recebidas e atendidas, publicar relatórios de transparência e, quando cabível, informar o titular sobre o acesso aos seus dados. Essa prestação de contas funciona como mecanismo de controle e como incentivo à diligência, pois expõe ao escrutínio público a conduta da empresa diante do poder estatal.

A avaliação de riscos, elemento nuclear do *compliance*, aplica-se de modo específico às requisições de dados. A empresa deve mapear os tipos de pedidos que costuma receber, as autoridades que os formulam e as categorias de dados envolvidas, identificando os pontos de maior exposição a violações. Nieto Martín (2015) destaca que a identificação prévia dos riscos é a condição para que os controles sejam desenhados de modo proporcional, evitando tanto a leniência quanto a burocratização que paralisa a atividade legítima.

A formação dos responsáveis é igualmente decisiva. De nada adianta uma política bem redigida se os profissionais que atendem às requisições não compreendem os regimes diferenciados de acesso nem sabem reconhecer um pedido irregular. Silveira e Saad-Diniz (2015) ressaltam que a efetividade dos programas de *compliance* depende da sua internalização pelos agentes que tomam as decisões cotidianas, o que exige capacitação contínua e canais de consulta para os casos de dúvida.

O *compliance* de privacidade deve, ademais, articular-se com as demais áreas de cumprimento da empresa. As requisições criminais tocam questões de proteção de dados, de direito penal e de relações institucionais, o que exige uma atuação coordenada entre o encarregado de dados, o departamento jurídico e a alta administração. Saad-Diniz (2019) observa que a fragmentação dos esforços de *compliance* compromete a sua eficácia, razão pela qual a resposta às requisições deve integrar-se a uma política coerente de gestão de riscos.

A existência de um programa de *compliance* não isenta a empresa de responsabilidade, mas funciona como elemento de aferição da sua diligência. Um programa meramente formal, de fachada, que não se traduz em práticas reais de triagem e de resistência, não cumpre a sua função e não afasta a censura. Nieto Martín (2015) adverte que a efetividade, e não a mera existência documental, é o critério que distingue um *compliance* genuíno de um simulacro destinado a produzir uma aparência de cuidado sem alterar as condutas.

A estruturação de um *compliance* de privacidade robusto, portanto, é a condição prática para que a empresa cumpra a sua função de garante. Sem políticas, procedimentos e responsáveis claramente definidos, a proteção dos direitos do titular fica entregue ao acaso. Com eles, a empresa converte um dever abstrato em uma prática verificável. Resta examinar, porém, o que ocorre quando esse dever é descumprido, ou seja, quais as consequências da entrega excessiva no plano da responsabilização corporativa.

4.2 RESPONSABILIZAÇÃO POR ENTREGA EXCESSIVA: DAS SANÇÕES ADMINISTRATIVAS À ESFERA PENAL

A entrega excessiva de dados não é uma conduta juridicamente neutra para a empresa. Além de contaminar a prova, ela pode gerar responsabilização em múltiplas esferas. No plano administrativo, o tratamento de dados em desconformidade com os princípios da finalidade, da necessidade e da minimização sujeita a empresa à fiscalização e às sanções da autoridade competente, nos termos do regime de proteção de dados, ainda que o tratamento ocorra em contexto de colaboração com a investigação criminal.

No plano civil, a violação dos direitos do titular pode ensejar a obrigação de reparar danos, inclusive de natureza coletiva, quando o vício atinge um número indeterminado de pessoas. Bioni (2019) destaca que a proteção de dados, por seu caráter

de direito de personalidade, tutela interesses que transcendem o patrimônio, de modo que a sua violação produz danos que não se medem apenas em prejuízos econômicos, mas na própria perda de controle sobre a informação pessoal, bem jurídico em si.

A dimensão da vulnerabilidade dos afetados agrava o quadro. Eubanks (2018) demonstra que ferramentas de coleta e tratamento de dados recaem com peso desproporcional sobre os mais pobres e vulneráveis, que dispõem de menos meios para resistir e reparar a violação. Transposta para as requisições criminais, essa constatação revela que a entrega excessiva tende a penalizar justamente quem já é mais exposto à ação estatal, o que reforça a gravidade da falha empresarial e o dever de cautela.

No plano penal, a questão é mais delicada, mas não inexistente. A entrega de dados em violação ao sigilo legalmente protegido, sem a devida ordem judicial, pode configurar ilícito penal por parte de quem a realiza, e a empresa que estrutura suas práticas de modo a facilitar ou tolerar tais entregas pode ver-se exposta a responsabilização. Saad-Diniz (2019) observa que a omissão de deveres de organização, no campo do *compliance*, pode fundamentar a imputação de responsabilidade, deslocando o foco do ato individual para a falha estrutural da empresa.

A responsabilização administrativa ganha contornos próprios no contexto das requisições. A autoridade de proteção de dados pode avaliar se a empresa adotou as salvaguardas exigíveis e se a entrega observou os princípios da finalidade e da minimização, independentemente de a coleta ter sido motivada por um pedido estatal. A existência de uma requisição não funciona como salvo-conduto automático, pois cabe à empresa demonstrar que agiu nos limites do que era legalmente exigível e adequado.

Há, ainda, o risco reputacional, que opera como sanção difusa. A revelação de que uma empresa entrega dados de seus usuários de modo indiscriminado compromete a confiança do público e pode produzir efeitos econômicos significativos. Esse risco, embora extrajurídico, reforça os incentivos para a adoção de práticas diligentes, e converte a proteção dos direitos dos titulares em um interesse convergente com a sustentabilidade do próprio negócio, alinhando ética e estratégia empresarial.

A responsabilização da empresa, por fim, não exclui a das pessoas físicas envolvidas. O agente que, conhecendo a ilegalidade do pedido, ainda assim determina ou executa a entrega excessiva pode responder individualmente, e a estrutura de *compliance* serve precisamente para identificar o agente e evitar que decisões dessa natureza sejam tomadas de modo isolado e acrítico. A clara atribuição de responsabilidades, longe de proteger os indivíduos a qualquer custo, distribui os deveres de modo a tornar a conduta da organização mais cuidadosa.

Convém observar que a responsabilização não visa a desencorajar a colaboração legítima, mas a entrega indevida. A empresa que atende corretamente a requisições regulares não tem o que temer; o que se censura é a entrega excessiva, a omissão de cautelas e a indiferença diante de pedidos manifestamente ilegais. O regime de responsabilização, nesse sentido, é um incentivo à diligência, e não um obstáculo à cooperação, pois recompensa a conduta cuidadosa e penaliza apenas o descuido e a leniência.

E mais: o *compliance* de privacidade não pode limitar-se a um exame meramente formal da existência de assinatura do juiz na decisão judicial. A empresa deve incorporar em sua matriz de risco uma auditoria de impacto. Detectado o risco de instrumentalização da plataforma, o dever de proteção impõe à empresa a obrigação de provocar o Poder Judiciário, exigindo a estrita demonstração da justa causa individualizada.

A multiplicidade de esferas de responsabilização revela que a diligência no atendimento às requisições não é apenas um imperativo ético, mas um interesse jurídico concreto da própria empresa. A corporação que entrega demais expõe-se a sanções administrativas, a condenações civis e, em hipóteses graves, a consequências penais, além de comprometer a prova que pretendia ajudar a produzir. O risco, portanto, não recai apenas sobre o titular, mas também sobre o provedor que falha no seu dever.

Essa convergência de responsabilidades fornece o fundamento para a construção de parâmetros de atuação. Se a entrega excessiva é prejudicial sob todos os ângulos, então a empresa tem razões jurídicas, e não apenas morais, para adotar uma postura criteriosa. O subtópico final examina como a experiência comparada pode inspirar um protocolo de *compliance* requisitório capaz de orientar essa postura de modo consistente e verificável.

4.3 PARÂMETROS COMPARADOS E UM PROTOCOLO DE COMPLIANCE REQUISITÓRIO

A experiência estrangeira oferece referências úteis para o desenho de um protocolo de atuação. No espaço europeu, a disciplina das ordens europeias de produção e de preservação de provas eletrônicas, consolidada no Regulamento (UE) 2023/1543, estabeleceu procedimentos, requisitos e garantias para o acesso transfronteiriço a dados, com atenção à proporcionalidade e à proteção dos direitos dos afetados. O modelo evidencia a preocupação em equilibrar a eficácia da cooperação com a tutela das garantias, em vez de tratar o acesso como um fluxo livre.

Nos Estados Unidos, a legislação sobre comunicações armazenadas (*Stored Communications Act*) e a disciplina do acesso a dados mantidos por provedores, incluindo o regime de alcance extraterritorial do CLOUD Act de 2018, ilustram tanto as possibilidades quanto os riscos do acesso estatal a acervos privados. O debate norte-americano sobre os limites desse acesso, marcado por intensa litigância entre o Estado e as plataformas,

demonstra que a resistência fundamentada da empresa é parte legítima e funcional do sistema, e não um desvio a ser suprimido.

Ferguson (2017) adverte que a aparência de objetividade e a retórica da eficiência frequentemente servem para blindar práticas de acesso contra o escrutínio, e que a contenção depende de regras claras e de instituições dispostas a aplicá-las. Pasquale (2015), por sua vez, insiste em que a transparência é condição de legitimidade do poder informacional, de modo que qualquer protocolo de atuação precisa incorporar mecanismos de documentação e de prestação de contas, sob pena de permanecer no plano simbólico.

A partir dessas referências, é possível esboçar um protocolo de *compliance* requisitório com alguns pilares. O primeiro é a triagem de legalidade, que submete cada requisição à verificação da competência da autoridade, da via adequada e da existência de ordem judicial quando exigível.

O segundo é a minimização, que limita a entrega ao estritamente requisitado, pelo período estritamente necessário, vedando o atendimento a pedidos genéricos.

O terceiro é a documentação rigorosa, que preserva a cadeia de custódia e permite o controle posterior.

O quarto pilar é a resistência fundamentada, que autoriza e mesmo impõe à empresa questionar, exigir esclarecimentos e, se necessário, recusar o atendimento de pedidos ilegais, submetendo a questão ao juiz.

O quinto é a transparência possível, que compreende registros, relatórios e, quando cabível, a comunicação ao titular.

Esses pilares não obstruem a investigação legítima, mas a depuram, assegurando que a colaboração se faça dentro dos limites do Estado de Direito.

Um protocolo de *compliance* requisitório deve prever, ainda, a gradação das respostas conforme a natureza do pedido. Requisições de simples dados cadastrais, formuladas por autoridade competente, podem ser atendidas por fluxo mais célere; pedidos de registros ou de conteúdo exigem a verificação da ordem judicial e dos seus requisitos; e requisições genéricas ou desprovidas de base legal devem acionar o mecanismo de resistência, em uma verdadeira reserva de jurisdição escalonada. Essa gradação evita tanto a obstrução das investigações legítimas quanto a entrega automática do que não poderia ser entregue.

A interlocução entre empresas e instituições de controle também merece institucionalização. Canais de diálogo, protocolos padronizados e parâmetros públicos de atuação reduzem a incerteza e profissionalizam a relação entre o poder estatal e os provedores. Pasquale (2015) sustenta que a transparência das regras do jogo é condição de legitimidade, e a definição clara dos procedimentos de requisição beneficia todos os

envolvidos, ao substituir a improvisação e a pressão informal por um regime previsível e controlável.

A construção desse regime, por fim, é uma tarefa compartilhada. Não cabe apenas às empresas estruturar o seu *compliance*, nem apenas ao Estado disciplinar as requisições, mas a ambos, em diálogo, definir um equilíbrio que preserve a eficácia da investigação e a integridade dos direitos. A experiência comparada demonstra que esse equilíbrio é possível, e que o seu alcance depende menos de soluções tecnológicas e mais de uma decisão institucional de subordinar o acesso a dados aos valores do Estado de Direito.

A adoção desses parâmetros, por fim, beneficia a própria persecução penal. Uma investigação amparada em provas obtidas com observância dos limites legais é mais sólida, menos sujeita a anulações e mais legítima aos olhos da sociedade. O protocolo de *compliance* requisitório, longe de ser um entrave, é um aliado da eficácia, pois substitui a fragilidade das provas obtidas por atalhos pela robustez daquelas produzidas no respeito às garantias, em benefício de uma justiça criminal ao mesmo tempo eficiente e legítima.

Nesse arranjo, o Ministério Público e o controle judicial desempenham papel decisivo. Cabe a essas instituições formular requisições proporcionais e fundamentadas, recusar a utilização de provas obtidas com excesso e fiscalizar a regularidade do acesso a dados, valorizando, e não penalizando, a empresa que resiste a pedidos ilegais. A construção de uma cultura de colaboração diligente, em que a proteção de direitos é parte do próprio dever de colaborar, é o horizonte que este protocolo procura desenhar.

5. CONCLUSÃO

Este estudo dedicou-se a examinar os limites do dever de colaboração da empresa diante das requisições criminais de dados e o papel do *compliance* de privacidade na tutela dos direitos fundamentais de terceiros. O tema impõe-se pela transformação que deslocou a prova penal para o domínio privado, convertendo os provedores em atores incontornáveis da persecução e em guardiões, ainda que involuntários, dos direitos dos titulares de dados que não participam da relação requisitória.

Buscou-se responder até onde vai o dever de colaborar e onde começa o dever de proteger, e qual a consequência da entrega excessiva. Para tanto, articularam-se a teoria da proteção de dados, o regime normativo do acesso a informações na investigação criminal e a literatura sobre prova penal e *compliance*, mediante pesquisa bibliográfica, documental e jurisprudencial. O exame permitiu compreender que colaboração e proteção não são inconciliáveis, mas dimensões que a diligência empresarial deve harmonizar.

No primeiro eixo, constatou-se que a guarda privada da prova confere ao provedor uma posição de garante dos direitos fundamentais dos titulares. Verificou-se que a privacidade, o sigilo e a proteção de dados, reforçados por sua inscrição constitucional,

pertencem ao titular ausente, e que a estrutura triangular da requisição faz da empresa o único anteparo desses direitos no momento do acesso.

No segundo eixo, evidenciou-se que o dever de colaboração é escalonado e limitado. O regime do Marco Civil distingue os dados cadastrais, acessíveis por requisição direta, dos registros e do conteúdo, submetidos à reserva de jurisdição. A jurisprudência sobre o compartilhamento de dados financeiros confirmou a distinção entre o compartilhamento espontâneo e a requisição direta, e a anulação de provas obtidas sem autorização judicial demonstrou que a inobservância dos limites contamina a prova.

No terceiro eixo, analisou-se que a entrega excessiva fere o titular e compromete a própria prova, ao gerar ilicitude e ao quebrar a cadeia de custódia da prova digital, da qual o provedor é o elo inicial. Constatou-se que a observância dos deveres da empresa reclama um *compliance* de privacidade estruturado, com triagem de legalidade, minimização, documentação, resistência fundamentada e transparência, e que a falha nesses deveres expõe a empresa à responsabilização administrativa, civil e penal.

Diante do exposto, conclui-se que o dever de colaboração da empresa é limitado pela legalidade, pela reserva de jurisdição, pela proporcionalidade e pela minimização, e que a sua observância depende de um *compliance* de privacidade efetivo. A entrega excessiva de dados não é colaboração legítima, mas violação que contamina a prova e responsabiliza a empresa. O provedor diligente é aquele que colabora dentro dos limites e resiste fora deles, exercendo a função de garante que a sua posição lhe impõe.

Reconhece-se que o debate comporta posições divergentes. De um lado, sustenta-se que a fluidez no acesso a dados é indispensável à eficácia da investigação diante da criminalidade tecnológica, e que exigências excessivas de formalidade comprometeriam a persecução. De outro, argumenta-se que, sem limites rigorosos, a colaboração se converte em devassa e a empresa em instrumento de violação de direitos. Ambas as perspectivas apresentam fundamentos legítimos e devem ser consideradas na construção do regime aplicável.

Ao término desta investigação, entende-se que a colaboração e a proteção, longe de se excluírem, integram um mesmo dever de atuação responsável. A empresa que protege os direitos do titular não obstrui a justiça, mas a qualifica, ao assegurar provas lícitas e confiáveis. Sugere-se, para estudos futuros, o exame da legislação específica de proteção de dados na segurança pública, ainda pendente, e o desenvolvimento de modelos de auditoria das práticas requisitórias. O desafio é fazer da colaboração um exercício de garantia, e não de sacrifício de direitos fundamentais.

REFERÊNCIAS BIBLIOGRÁFICAS | REFERENCES | REFERENCIAS

- BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.
- BRAYNE, Sarah. Predict and surveil: data, discretion, and the future of policing. New York: Oxford University Press, 2021.
- COSTA, Rafael de Oliveira. Direito Constitucional. Rio de Janeiro: Editora Método, 2024.
- DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.
- 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, Brasília, v. 18, n. 100, 2022. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5991>. Acesso em: 4 jun. 2026.
- EUBANKS, Virginia. Automating inequality: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2018.
- FERGUSON, Andrew Guthrie. The rise of big data policing: surveillance, race, and the future of law enforcement. New York: New York University Press, 2017.
- FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. Tradução de Ana Paula Zomer Sica et al. São Paulo: Revista dos Tribunais, 2002.
- JUNQUEIRA, Gabriel Marson. A prevenção da corrupção na Administração Pública: contributos criminológicos, do corporate compliance e public compliance. Belo Horizonte: D'Plácido, 2019.
- LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2011.
- LOPES JR., Aury. Direito processual penal. São Paulo: Saraiva, 2020.
- MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.
- NIETO MARTÍN, Adán (dir.). Manual de cumplimiento penal en la empresa. Valencia: Tirant lo Blanch, 2015.
- O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. New York: Crown, 2016.
- PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.
- PRADO, Geraldo. A cadeia de custódia da prova no processo penal. São Paulo: Marcial Pons, 2019.
- SAAD-DINIZ, Eduardo. Ética negocial e compliance: entre a educação executiva e a interpretação judicial. São Paulo: Thomson Reuters Brasil, 2019.

SILVA SÁNCHEZ, Jesús-Maria. Deberes de vigilancia y compliance empresarial. In: KUHLEN, L.; MONTIEL, J. P.; GIMENO, I. O. U. (Org.). Compliance y teoría del Derecho Penal. Madrid: Marcial Pons, 2013, p. 79-106.

SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. Compliance, direito penal e lei anticorrupção. São Paulo: Saraiva, 2015.

Jurisprudência

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso em Habeas Corpus 174.173/RJ. Terceira Seção. Relator: Ministro Messod Azulay Neto. Julgamento em 14 maio 2025.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6.387 MC/DF. Tribunal Pleno. Relatora: Ministra Rosa Weber. Julgamento em 7 maio 2020.

BRASIL. Supremo Tribunal Federal. Habeas Corpus 222.141 AgR/PR. Segunda Turma. Relator: Ministro Ricardo Lewandowski. Julgamento em 6 fev. 2024.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 1.055.941/SP (Tema 990 da repercussão geral). Tribunal Pleno. Relator: Ministro Dias Toffoli. Julgamento em 4 dez. 2019.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 1.393.219 AgR/SP. Segunda Turma. Relator: Ministro Edson Fachin. Julgamento em 1 jul. 2024.

Instagram & Twitter | @HomaPublicaDHE
periodicos.ufjf.br/index.php/homa/