

RESERVA DE JURISDIÇÃO E ARQUITETURA DE DADOS: A ADC 91 E O TESTE DE SEPARAÇÃO ESTANQUE NO DIREITO EUROPEU

Gustavo Henrique de Andrade Cordeiro

Doutor em Direito pela Instituição Toledo de Ensino (ITE). Mestre em Direito pelo Centro Universitário Eurípides de Marília (UNIVEM). Promotor de Justiça no Ministério Público do Estado de São Paulo. Pró-Reitor Acadêmico do Centro Universitário Eurípides de Marília (UNIVEM). Coordenador do Grupo de Estudos de Marília 'João Batista de Santana' da Associação Paulista do Ministério Público. Diretor Regional da Escola Superior do Ministério Público. <http://lattes.cnpq.br/6687308419664444>. <https://orcid.org/0000-0002-4035-1628>. E-mail: gustavomqv@hotmail.com

Guilherme Domingos de Luca

Doutorando em Direito pela Universidad Internacional Iberoamericana do México, Mestre em Teoria do Direito e do Estado (UNIVEM) (Bolsista CAPES/PROSUP) e Pós-Graduando em Direito do Trabalho e Previdenciário (PUC-MG) e Marketing e Mídias Digitais (Estácio-RJ) (Be Academy). MBA em Liderança na Nova Economia pela Faculdade Atitude de Educação Continuada. Estudante de tecnologia em Inteligência Artificial pela Uninove - SP. Advogado; Professor de Direito em Curso Superior (IBMR-RJ e Uninassau-RJ), cursos preparatórios e pós-graduações. Palestrante. <http://lattes.cnpq.br/0558315354670819>. <https://orcid.org/0000-0001-8863-8604>. E-mail: guilhermedeluca@gmail.com

Rogério Monteiro de Barros

Mestrando em Direito pela Universidade de Marília (UNIMAR). Especialista em Direito Tributário pela UNIVEM. Possui graduação em Direito pelo Centro Universitário de Adamantina (2000). Atualmente é advogado autônomo. <http://lattes.cnpq.br/8118653073386539>. <https://orcid.org/0009-0003-7530-018X>. E-mail: barros.rogeriomonteiro@gmail.com

Priscila Carolina de Oliveira

Docente titular no Centro Universitário Eurípides de Marília (UNIVEM) na disciplina de Direito Digital (2025 - atual). Mestranda pelo Centro Universitário Eurípides de Marília (2025 - atual). Graduada em Direito pelo Centro Universitário Eurípides de Marília - UNIVEM (2016). Formação como Data Protection Officer - DPO pela Opice Blum Academy (2019). Advogada desde 2017, com atuação predominante na área Direito Digital e Proteção de Dados/LGPD. <http://lattes.cnpq.br/1606194120143879>. <https://orcid.org/0009-0005-7598-1899>. E-mail: prilolivee@gmail.com

Rogério Nascimento Renzetti Filho

Doutor em direito pela Universidade Veiga de Almeida, PPGD/UVA e Mestre em Direito pelo Centro Universitário Eurípides de Marília, UNIVEM/SP. Especialista em Direito e Processo do Trabalho pela Escola de Magistratura da Justiça do Trabalho no Estado do Rio de Janeiro. Bacharel em Direito. Advogado. Master em Programação Neurolinguística (PNL). Professor do curso em Ciências Jurídicas no Centro Universitário IBMR (Grupo Ânima). Advogado Orientador do NPJ e Professor na Uninassau-RJ. Professor do CERS Cursos Online e em cursos preparatórios para concursos públicos na área jurídica, pós-graduação, preparatórios para o Exame de Ordem dos Advogados do Brasil e prática para Advogados na modalidade presencial e online. <http://lattes.cnpq.br/937177420218165>. <https://orcid.org/0009-0005-5503-5440>. E-mail: renzettiprofessor@gmail.com

Rodrigo Murad Vitoriano

Mestrando em Direito Digital pelo Centro Universitário Eurípides de Marília (UNIVEM), graduado em Direito pelo Centro Universitário de Rio Preto (UNIRP) e graduando em Gestão Pública pela Universidade Estácio de Sá - Ribeirão Preto. Possui especializações em Direito Penal, Direito Constitucional, Direito Civil e Direito Processual Civil. Exerce o cargo efetivo de Procurador Jurídico do Poder Legislativo do Município de Jales (SP). <http://lattes.cnpq.br/2051996455632539>. <https://orcid.org/0009-0009-4015-2934>. E-mail: adv.rmv@hotmail.com

João Luís dos Santos

Mestrando em Direito e Estado na Era Digital pela UNIVEM - Marília. Mestre em Letras - Literaturas de Língua Portuguesa pela UNESP de São José do Rio Preto (Ibilce). Graduado em Letras, Pedagogia e Direito. Supervisor de Ensino na URE Penápolis e Professor na Fundação Educacional de Penápolis. Pesquisador em Estudos Literários, Políticas Educacionais e Educação em Direitos Humanos. Advogado. Poeta. Membro-fundador da Academia Penapolense de Letras. <http://lattes.cnpq.br/8261621520380363>. <https://orcid.org/0009-0003-0392-2326>. E-mail: santos.joaoluiz@yahoo.com.br

Cesar Claudio Pinto Ferreira

Formando em Direito (IBMR-12/2026), Pós-graduando em Direito Tributário (UNI LEGALE EDUCACIONAL), Mestre em Economia Empresarial (UCAM-RJ), MBA Gestão de Investimentos (Estácio - RJ), Graduação em Ciências Econômicas (UFF-RJ), Empresário há 20 anos, atuou 15 anos em grandes multinacionais do mercado financeiro, investidor profissional em mercado de capitais. Palestrante. <https://orcid.org/0009-0005-0315-9265>. E-mail: cesarclaudiopf@yahoo.com.br

DOI-Geral: <http://dx.doi.org/10.47538/RA-2026.V5N3>

DOI-Individual: <http://dx.doi.org/10.47538/RA-2026.V5N3-63>

RESUMO: O Supremo Tribunal Federal discute, na ADC 91, se a identificação de usuário de internet a partir de endereço IP depende de autorização judicial. O problema investigado consiste em saber qual é o objeto do controle judicial nessa hipótese: a categoria de dado requisitada ou a operação que vincula registro de conexão e cadastro.

CORDEIRO, G.H.A.; LUCA, G.D.; BARROS, R.M.; OLIVEIRA, P.C.; RENZETTI FILHO, R.N.; VITORIANO, R.M.; SANTOS, J.L.; FERREIRA, C.C.P. Reserva de jurisdição e arquitetura de dados: a ADC 91 e o teste de separação estanque no direito europeu. **Revista Eletrônica Amplamente**, Natal/RN, v. 5, n. 3, p. 1164-1195, jul./set., 2026.

A hipótese sustentada é que o objeto é a operação. Adota-se método hipotético-dedutivo, com análise normativa, jurisprudencial e comparada, apoiada em decisões do Supremo Tribunal Federal, do Superior Tribunal de Justiça, do Tribunal de Justiça da União Europeia, do Tribunal Europeu de Direitos Humanos e da Suprema Corte norte-americana. Examinam-se o regime do art. 10 da Lei nº 12.965/2014, a taxonomia firmada na ADI 4.906 e o teste europeu de separação estanque. Conclui-se pela submissão do ato de correlação a controle judicial, com proposta de redação normativa e critério de admissibilidade probatória.

PALAVRAS-CHAVE: Identificação de usuário. Registros de conexão. Endereço IP. Persecução penal. Admissibilidade probatória.

JUDICIAL AUTHORISATION AND DATA ARCHITECTURE: ADC 91 AND THE WATERTIGHT SEPARATION TEST IN EUROPEAN LAW

ABSTRACT: In ADC 91, the Brazilian Supreme Court is deciding whether identifying an internet user from an IP address requires judicial authorisation. The research problem concerns the object of judicial control in this scenario: the category of data requested or the operation that links connection records to subscriber records. The hypothesis defended here is that the object is the operation. The study follows a hypothetical-deductive method, combining statutory, case-law and comparative analysis, drawing on rulings of the Brazilian Supreme Court, the Superior Court of Justice, the Court of Justice of the European Union, the European Court of Human Rights and the United States Supreme Court. It examines the regime of Article 10 of Law 12.965/2014, the taxonomy established in ADI 4.906 and the European watertight separation test. The conclusion submits the act of correlation to judicial control, with proposed statutory wording and an evidentiary admissibility criterion.

KEYWORDS: User identification. Connection records. IP address. Criminal prosecution. Evidentiary admissibility.

INTRODUÇÃO

Em 27 de agosto de 2026, o Plenário do Supremo Tribunal Federal retomou em sessão presencial o julgamento da Ação Declaratória de Constitucionalidade 91, ajuizada pela Associação Brasileira de Provedores de Internet e Telecomunicações, e o suspendeu no mesmo dia, depois dos votos dos relatores.

Discute-se ali se o art. 10, § 1º, da Lei nº 12.965/2014 é compatível com a Constituição na parte em que condiciona à autorização judicial o fornecimento de registros de conexão e de acesso a aplicações. A pergunta prática que move o processo é menos abstrata do que a formulação sugere.

Quando um órgão de persecução penal informa a um provedor um endereço IP, uma data e um horário, e pede o nome de quem estava conectado naquele instante, essa requisição pode ser cumprida sem ordem judicial? A resposta divide a jurisprudência ordinária e coloca o provedor entre dois riscos simétricos: responder por desobediência se recusa, ou por violação de sigilo se entrega.

O problema jurídico deste artigo tem formulação estreita. Se a lei submete a autorização judicial o fornecimento de registros de conexão e ao mesmo tempo dispensa essa autorização para dados cadastrais de qualificação pessoal, filiação e endereço, qual é o regime da operação que combina os dois conjuntos?

A questão não se resolve pela classificação isolada de cada categoria, porque nenhuma delas, sozinha, produz o resultado que interessa à investigação. Esse resultado é a identificação, e a identificação nasce de um cruzamento executado pelo provedor a pedido do Estado. A tensão constitucional está em decidir se o cruzamento tem regime próprio ou se herda, por contágio, o regime da categoria mais protegida entre as duas que o compõem.

Determinar o objeto do controle judicial na identificação de usuário por endereço IP é o objetivo geral. Quatro objetivos específicos organizam o percurso. O primeiro consiste em reconstruir o regime legal brasileiro da requisição de dados a provedores, com exame do art. 10 da Lei nº 12.965/2014, do Decreto nº 8.771/2016 e da tese firmada na ADI 4.906. O segundo consiste em contrastar a solução em construção no Supremo com a jurisprudência europeia sobre acesso a dados de identidade civil associados a endereço IP. O terceiro consiste em avaliar a consistência da exceção de urgência admitida no voto do relator. O quarto consiste em formular o critério operativo aplicável a casos futuros e a redação normativa que dele decorre.

Quanto ao método de abordagem, a pesquisa é hipotético-dedutiva: parte da hipótese de que o ato de correlação constitui objeto normativo autônomo e a submete a teste contra o material normativo e jurisprudencial disponível. O método de procedimento articula análise normativa, análise de decisões judiciais e comparação funcional.

As fontes utilizadas são a legislação brasileira e europeia, decisões do Supremo Tribunal Federal, do Superior Tribunal de Justiça, do Tribunal de Justiça da União Europeia, do Tribunal Europeu de Direitos Humanos e da Suprema Corte dos Estados Unidos, literatura revisada por pares e documentos institucionais. A comparação não persegue transplante de solução, e sim a identificação dos pressupostos institucionais que sustentam cada arranjo. O corte temporal alcança decisões publicadas até 28 de agosto de 2026.

A reconstrução do regime legal ocupa a abertura do texto, porque dela depende a delimitação do que está efetivamente em disputa. Ali se examinam as três camadas do art. 10 da Lei nº 12.965/2014, os requisitos de motivação e especificidade impostos pelo Decreto nº 8.771/2016 e a contenção conceitual promovida pela ADI 4.906, que reduziu o dado cadastral requisitável a qualificação pessoal, filiação e endereço.

O litígio trazido pela associação de provedores fecha a primeira parte, com atenção ao ponto que a doutrina costuma tratar como periférico: a posição jurídica de quem recebe a requisição e precisa decidir sozinho se cumpre.

Depois de fixado o quadro normativo, a discussão se desloca para o núcleo teórico. A taxonomia da privacidade oferece instrumentos para separar agregação e identificação como atividades distintas, com riscos distintos, e essa separação sustenta o argumento central do artigo.

O percurso europeu comparece em seguida, do julgamento Ministério Fiscal, de 2018, ao acórdão La Quadrature du Net II, de 2024, no qual o Tribunal de Justiça admitiu acesso a dados de identidade civil associados a endereço IP sem controle prévio, sob condição de separação estanque entre bases e verificação periódica independente. Benedik e Carpenter completam o panorama e permitem testar a hipótese contra parâmetros construídos fora do direito da União.

Fornece o ponto de apoio da terceira parte um dispositivo pouco lembrado: o art. 12 do Decreto nº 8.771/2016, que obriga órgãos federais a publicar relatórios estatísticos anuais das requisições de dados cadastrais. Nela se examinam a exceção de perigo atual

admitida pelo relator e suas balizas, a consequência probatória do descumprimento e a lacuna institucional que separa o desenho brasileiro do europeu.

A ausência de autoridade de controle com competência sobre tratamento de dados para fins penais não é detalhe de arquitetura administrativa. É o elemento que torna inviável, no Brasil, a transposição do parâmetro europeu, e é também o que justifica manter o juiz como instância de verificação.

A contribuição pretendida tem nome: construção do ato de correlação como objeto normativo autônomo, com três consequências operativas. Requisitar identificação por endereço IP significa requisitar um processamento, não um registro; o provedor que executa esse processamento age como agente de tratamento a serviço do Estado, com deveres próprios de documentação; e a inobservância do controle judicial gera inutilizabilidade da prova, não simples irregularidade. Ao final, propõe-se redação para novo parágrafo do art. 10 da Lei nº 12.965/2014.

O REGIME LEGAL DA REQUISIÇÃO E A FORMAÇÃO DO LITÍGIO CONSTITUCIONAL

A controvérsia sobre a requisição direta de dados por autoridades investigativas não pode ser adequadamente compreendida se permanecer confinada à distinção formal entre “dado cadastral” e “registro de conexão”. O problema central está menos no nome atribuído à informação e mais na operação necessária para produzi-la.

No Marco Civil da Internet, a guarda e a disponibilização de registros de conexão, registros de acesso a aplicações, dados pessoais e conteúdo de comunicações privadas devem observar a proteção da intimidade, da vida privada, da honra e da imagem das pessoas envolvidas, nos termos do art. 10 da Lei nº 12.965/2014 (Brasil, 2014).

Essa opção legislativa evidencia que a informação digital não é juridicamente neutra: sua coleta, conservação, associação e disponibilização podem afetar direitos fundamentais, ainda que o resultado seja apresentado sob a aparência de simples identificação civil.

O desenho normativo do art. 10 é construído em três camadas. O caput estabelece a regra geral de proteção dos registros, dados pessoais e comunicações privadas. O § 1º condiciona a disponibilização dos registros de conexão e de acesso a aplicações à ordem judicial. O § 3º, por outro lado, permite que autoridades administrativas com competência legal requisitem diretamente dados cadastrais que informem qualificação pessoal, filiação e endereço (Brasil, 2014).

Trata-se de uma arquitetura categorial, na qual cada espécie de informação recebe regime próprio. A dificuldade surge quando a resposta formalmente cadastral somente pode ser obtida mediante consulta a registros de conexão, pois, nesse caso, o dado entregue à autoridade não resulta de mera consulta a cadastro estático, mas de uma operação de correlação entre bases distintas.

O Decreto nº 8.771/2016 reforçou essa lógica ao delimitar os dados cadastrais como filiação, endereço e qualificação pessoal, compreendida como nome, prenome, estado civil e profissão do usuário. O mesmo decreto exigiu que a autoridade indique fundamento legal de competência expressa, motive o pedido, especifique os indivíduos alcançados e indique as informações desejadas, vedando pedidos coletivos genéricos ou inespecíficos (Brasil, 2016).

Esses requisitos são relevantes, mas permanecem voltados à forma e à motivação da requisição. Eles não enfrentam, por si sós, a pergunta decisiva: que tipo de tratamento informacional o provedor precisa realizar para atender ao pedido?

Essa pergunta é essencial porque há diferença jurídica entre recuperar um dado cadastral já existente e produzir uma identificação por correlação. Quando a autoridade solicita o endereço do titular de determinada linha telefônica, o provedor consulta uma base cadastral e informa dado previamente fornecido pelo usuário.

Quando, porém, a autoridade apresenta um endereço IP, uma data, um horário e um fuso, e pede a identificação do usuário correspondente, o provedor deve consultar registros técnicos de conexão, localizar a sessão compatível, vincular essa sessão a um assinante e, somente depois, extrair do cadastro os dados civis correspondentes.

O resultado pode ser nome, filiação e endereço, mas o caminho percorrido revela algo adicional: aquela pessoa esteve vinculada à conexão indicada naquele momento. Por isso, a natureza jurídica da operação não deve ser definida apenas pelo conteúdo final entregue à autoridade.

A doutrina contemporânea sobre proteção de dados há muito demonstra que a informação pessoal adquire significado pela possibilidade de tratamento, cruzamento e contextualização, e não apenas por sua leitura isolada (Doneda, 2021; Bioni, 2021; Mendes, 2014).

A mesma conclusão aparece, sob outro ângulo, nos estudos estrangeiros sobre vigilância e privacidade informacional: dados aparentemente fragmentários podem, quando combinados, reconstruir condutas, relações e padrões de comportamento (Rodotà, 2008; Solove, 2004). A identificação do titular de um IP em determinado instante, portanto, não se reduz a uma ficha cadastral; ela incorpora uma inferência temporal e comportamental.

A questão técnica confirma essa preocupação jurídica. Em razão do compartilhamento de endereços IPv4, especialmente por meio de soluções de tradução de endereços como o Carrier-Grade NAT, diversos usuários podem utilizar o mesmo endereço IP público em intervalos próximos ou simultâneos. Nesses cenários, a identificação confiável depende da indicação da porta lógica de origem associada à conexão (Ford et al., 2011).

A jurisprudência do Superior Tribunal de Justiça também reconheceu que, enquanto persistir a necessidade de individualização em ambientes de compartilhamento de IPv4, a porta lógica de origem é elemento relevante para a correta identificação do usuário (Brasil, 2019).

O Decreto nº 12.975/2026 incorporou expressamente essa preocupação ao prever que o dever de guarda de registros de endereço IP abrange a porta lógica de origem sempre que necessária à identificação inequívoca do terminal de origem ou do próximo enlace de rede (Brasil, 2026a).

A consequência é direta: a requisição baseada apenas em IP, data e hora pode gerar risco de identificação equivocada quando não acompanhada dos elementos técnicos indispensáveis. Esse risco não é meramente operacional. Se o resultado da consulta ingressa em investigação ou processo penal com aparência de dado objetivo, a falha técnica converte-se em problema probatório e constitucional.

A individualização do investigado, nesse contexto, passa a depender de uma cadeia de tratamento informacional que precisa ser controlável, documentada e sujeita à verificação posterior. Sem isso, a defesa fica diante de uma identificação já estabilizada pela autoridade e pelo provedor, mas sem acesso claro aos passos técnicos que permitiram sua produção.

O próprio Marco Civil fornece elementos para essa leitura operacional. Os arts. 13 e 15 da Lei nº 12.965/2014 autorizam autoridade policial, autoridade administrativa ou Ministério Público a requerer cautelarmente a preservação de registros por prazo superior ao legal, mas condicionam a disponibilização efetiva desses registros à autorização judicial (Brasil, 2014).

A distinção entre preservar e acessar foi confirmada pelo Superior Tribunal de Justiça no HC 626.983/PR, no qual se reconheceu a validade do pedido de congelamento de dados telemáticos sem prévia ordem judicial, desde que se trate de simples preservação, e não de acesso ao conteúdo ou aos registros preservados (Brasil, 2022).

A lógica é clara: conservar a possibilidade probatória pode ser ato administrativo; revelar a informação protegida exige controle jurisdicional. Os arts. 22 e 23 do Marco Civil completam essa estrutura ao disciplinar o requerimento judicial de fornecimento de registros. O pedido deve conter fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros para investigação ou instrução probatória e indicação do período a que se referem os registros (Brasil, 2014).

Esses requisitos demonstram que o legislador não tratou o acesso a registros como providência burocrática. Ao contrário, exigiu controle de pertinência, necessidade e delimitação temporal. A lacuna está em permitir que uma requisição formalmente

cadastral, mas materialmente dependente de registro de conexão, escape desse filtro apenas porque o resultado se apresenta como nome, filiação ou endereço.

A ADI 4.906 enfrentou parte desse problema, mas não o resolveu integralmente. Ao examinar o art. 17-B da Lei nº 9.613/1998, o Supremo Tribunal Federal reconheceu a constitucionalidade do acesso direto, por autoridades policiais e Ministério Público, a dados cadastrais de investigados, desde que limitado à qualificação pessoal, filiação e endereço (Brasil, 2024).

A decisão foi importante porque impediu interpretação expansiva da expressão “dados cadastrais”. Sem essa limitação, qualquer informação constante de cadastro poderia ser indevidamente qualificada como cadastral, inclusive elementos mais sensíveis, históricos contratuais, identificadores técnicos ou dados de pagamento.

Ainda assim, a ADI 4.906 respondeu apenas à pergunta sobre quais dados cadastrais podem ser requisitados diretamente. Ela não enfrentou, em profundidade, a situação em que o pedido de dado cadastral funciona como instrumento de acesso a informação de tráfego.

A distinção é sutil na formulação, mas expressiva nos efeitos. Um ofício que solicite “nome, filiação e endereço do usuário vinculado ao IP X, na data Y, às Z horas” parece, à primeira vista, limitado aos três campos admitidos pela jurisprudência constitucional.

Ocorre que a resposta comunica, de modo necessário, que determinada pessoa esteve associada àquela conexão em momento específico. Essa informação não é apenas cadastral; ela deriva de registro de conexão e revela vínculo temporal de uso da rede.

É justamente essa zona de interseção que se encontra no centro da ADC 91. A ação foi proposta pela Associação Brasileira de Provedores de Internet e Telecomunicações com o objetivo de obter declaração de constitucionalidade do art. 10, § 1º, do Marco Civil da Internet, diante de divergências judiciais sobre a exigência de ordem judicial para fornecimento de registros de usuários, especialmente em hipóteses de identificação por endereço IP (Brasil, 2026b).

Até 29 de agosto de 2026, o julgamento ainda não deve ser tratado como concluído: as notícias recentes indicam que os ministros Cristiano Zanin e Dias Toffoli votaram pela preservação da ordem judicial como regra para acesso a dados de tráfego, mas o julgamento foi suspenso para retomada posterior (Brasil, 2026b).

A formulação atribuída ao voto do ministro Cristiano Zanin é relevante porque desloca o debate do rótulo do dado para a operação de correlação. A requisição direta de dados cadastrais básicos não autorizaria, por si só, o acesso a metadados de conexão nem o cruzamento de informações destinado a identificar quem estava por trás de determinado endereço IP.

Nessa hipótese, a exigência de autorização judicial decorreria não do nome civil entregue ao final, mas do itinerário informacional necessário para produzi-lo. A identificação por IP, data e hora é, em termos jurídicos, uma reconstrução de vínculo técnico-temporal, e não mera consulta cadastral.

Essa leitura é mais coerente com a proteção constitucional de dados pessoais. A Emenda Constitucional nº 115/2022 incluiu expressamente a proteção de dados pessoais entre os direitos e garantias fundamentais, reforçando a compreensão de que a tutela constitucional não se limita ao sigilo das comunicações ou à privacidade em sentido clássico (Brasil, 1988).

No mesmo sentido, a jurisprudência do Supremo Tribunal Federal, em casos sobre compartilhamento de dados no setor público, tem associado proteção de dados, finalidade, necessidade, segurança e controle institucional (Brasil, 2022b).

A requisição de identificação por IP deve ser compreendida nesse ambiente constitucional ampliado, no qual o poder estatal de correlacionar dados exige fundamento jurídico, finalidade legítima, necessidade demonstrável e mecanismos de responsabilização.

O argumento contrário não é irrelevante. Investigações de crimes praticados por meio da internet dependem, muitas vezes, de resposta rápida, e os prazos legais de guarda de registros são limitados. O Marco Civil prevê guarda de registros de conexão pelo prazo

de um ano e de registros de acesso a aplicações pelo prazo de seis meses, o que pode pressionar autoridades investigativas a agir com urgência (Brasil, 2014).

Além disso, há situações concretas em que a demora judicial pode comprometer a proteção de bens jurídicos relevantes. O problema é que essa constatação não autoriza converter a exceção em regra nem transformar todo pedido de identificação por IP em requisição administrativa ordinária.

A solução dogmaticamente mais consistente consiste em tratar a correlação entre dado cadastral e registro de conexão como objeto normativo próprio. Não basta perguntar se o resultado é cadastral. É necessário verificar se a autoridade pediu uma consulta que exige acesso, tratamento ou combinação de registros protegidos.

Havendo correlação entre IP, marco temporal e identidade civil, a regra deve ser a autorização judicial, salvo hipóteses excepcionais expressamente justificadas, documentadas e submetidas a controle jurisdicional subsequente. Esse modelo preserva a utilidade investigativa sem esvaziar a garantia constitucional.

A posição jurídica do provedor reforça essa conclusão. Quando recebe requisição direta fundada em IP, data e hora, o provedor é colocado diante de uma decisão que não deveria ser sua: definir se a diligência é simples fornecimento cadastral ou acesso indireto a registro de conexão. Essa transferência de responsabilidade a particulares gera assimetria prática.

Grandes provedores, com departamentos jurídicos estruturados, tendem a resistir a pedidos ambíguos e exigir ordem judicial. Provedores menores, especialmente regionais, podem cumprir requisições para evitar conflito com autoridades. O resultado é uma proteção desigual, determinada não pela Constituição ou pela lei, mas pela capacidade institucional do intermediário.

A discussão conjunta da ADC 91 com as ADIs 5.059 e 5.073 amplia esse quadro. As ações relativas à Lei nº 12.830/2013 discutem o alcance do poder requisitório do delegado de polícia durante a investigação criminal, especialmente quanto à possibilidade de requisitar perícias, informações, documentos e dados de interesse da apuração (Brasil, 2013).

A leitura constitucionalmente adequada desse poder deve reconhecer sua importância para a investigação, mas também seus limites diante de dados protegidos por sigilo, privacidade ou disciplina legal específica. Poder genérico de requisição não pode funcionar como autorização ampla para acessar registros cuja disponibilização a própria legislação condiciona ao controle judicial.

A controvérsia, portanto, não se resume a disputa institucional entre órgãos de investigação, Ministério Público, polícia judiciária e provedores. Seu núcleo é constitucional. Trata-se de saber se o Estado pode obter, sem ordem judicial, uma identificação civil produzida a partir de registros de conexão.

A resposta deve considerar que a correlação entre IP, tempo e pessoa transforma um dado aparentemente cadastral em informação de tráfego contextualizada. Nessa hipótese, a reserva jurisdicional não é formalismo; é mecanismo de controle da proporcionalidade, da necessidade e da rastreabilidade da medida.

Conclui-se, assim, que a distinção relevante não está apenas entre “dado cadastral” e “registro de conexão”, mas entre consulta cadastral simples e correlação identificadora.

A primeira pode, nos limites legais, ser atendida por requisição direta quando envolver qualificação pessoal, filiação e endereço. A segunda, por depender de registros técnicos e produzir vínculo temporal de navegação ou conexão, deve submeter-se à ordem judicial como regra.

Essa interpretação preserva a eficácia investigativa, evita identificações tecnicamente frágeis, protege a igualdade entre usuários submetidos a provedores de portos diversos e impede que garantias constitucionais sejam redefinidas, na prática, por decisões privadas tomadas no balcão da requisição administrativa.

A CORRELAÇÃO COMO OBJETO NORMATIVO

Daniel Solove propôs, em 2006, taxonomia que organiza os danos à privacidade em quatro grupos de atividades, e que trata agregação e identificação como itens separados dentro do grupo do processamento de informações (Solove, 2006).

Agregação é a reunião de dados dispersos sobre a mesma pessoa; identificação é a ligação entre um conjunto de dados e um indivíduo determinado. A distinção parece escolástica até que se observe o efeito de cada uma. Pode haver agregação intensa com baixa identificação, como em bases estatísticas anonimizadas, e identificação intensa com baixa agregação, como em pontos de controle documental.

O caso da ADC 91 combina os dois vetores em uma única operação, e é essa combinação que o desenho legal brasileiro não captura. O registro de conexão isolado tem alta agregação potencial e baixa identificação: revela horários, duração e volume, sem dizer de quem.

O cadastro isolado tem alta identificação e baixa agregação: diz quem é, sem dizer o que fez. Cruzar os dois converte cada conjunto no que faltava ao outro. Adota-se aqui a leitura de que o dano relevante não está em nenhum dos conjuntos, e sim na função que os liga.

Helen Nissenbaum ofereceu, em 2010, formulação complementar ao propor que a proteção da privacidade se mede pela integridade contextual, isto é, pela adequação do fluxo de informação às normas do contexto em que foi originalmente produzida (Nissenbaum, 2010).

O dado cadastral é fornecido pelo usuário no contexto da contratação de um serviço, com finalidade de faturamento e suporte. O registro de conexão é gerado pelo funcionamento técnico da rede, sem ato voluntário do usuário. Unir os dois para fins de persecução penal rompe as normas dos dois contextos ao mesmo tempo, e não apenas as de um deles.

Doutrina brasileira consolidada sustenta o deslocamento da privacidade para a proteção de dados como categoria autônoma, dotada de regime próprio e de função distinta da tutela do segredo (Doneda, 2020). O tratado organizado por Laura Schertel Ferreira Mendes e Bruno Ricardo Bioni sistematizou esse regime e o projetou sobre setores em que o tratamento é executado por agentes públicos (Mendes; Bioni, 2021).

Aplicada ao caso em exame, a distinção produz efeito direto. O problema da identificação por endereço IP não se resolve perguntando se houve quebra de sigilo, e sim

perguntando se a operação de tratamento observou base legal adequada e controle proporcional à sua intensidade.

Assiste razão à literatura brasileira que vem apontando o ponto sob outra chave. Jacqueline de Souza Abreu, em tese defendida na Universidade de São Paulo em 2022, demonstra que a jurisprudência constitucional brasileira sobre sigilo telemático opera com parâmetros herdados do modelo das comunicações telefônicas e precisa de revisão em pontos determinados, entre eles o acesso a dados junto a controladores (Abreu, 2022). A crítica é procedente.

O art. 5º, XII, da Constituição foi pensado para a interceptação de fluxo, e a identificação por correlação não é interceptação de coisa alguma. A coletânea organizada por Dennys Antonialli e pela mesma autora já reunia, em 2018, estudos que anteciparam boa parte da controvérsia hoje submetida ao Supremo (Antonialli; Abreu, 2018).

Jamilla Monteiro Sarkis, em estudo publicado em 2024 na Revista Brasileira de Direito Processual Penal, sustenta a existência de um direito da pessoa imputada ao anonimato digital, com consequências sobre os meios de obtenção de prova (Sarkis, 2024).

Não se adota aqui a construção em toda a sua extensão, porque o anonimato como direito autônomo suscita dificuldades no plano da tutela penal de vítimas. A contribuição da autora é útil, contudo, para o argumento central: se existe interesse juridicamente protegido em não ser identificado, o ato que produz a identificação tem de ter regime próprio, e não pode ser tratado como consequência incidental de uma consulta cadastral.

Marta Saad, Helena Costa Rossi e Pedro Henrique Partata concluíram, em 2024, que a obtenção de provas digitais demanda disciplina jurídica própria, com requisitos mínimos fixados em lei para balizar as decisões judiciais autorizativas (Saad; Costa Rossi; Henrique Partata, 2024).

A conclusão converge com a que se defende neste artigo, embora por caminho distinto: os autores partem das características do objeto probatório, e o argumento aqui desenvolvida parte da operação que produz o objeto. As duas rotas chegam à mesma exigência de lei específica.

Cabe formular a proposição em termos operativos. O ato de correlação é a operação pela qual o provedor, a pedido de autoridade pública, executa consulta cruzada entre base de registros de conexão ou de acesso a aplicações e base de dados cadastrais, com a finalidade de vincular um identificador de rede a uma pessoa determinada.

Três elementos o caracterizam: existência de duas bases distintas, execução de consulta pelo controlador a pedido do Estado e produção de informação inexistente em qualquer das bases isoladamente. Presentes os três, o regime aplicável é o do art. 10, § 1º, e não o do § 3º. Três consequências decorrem da definição.

A primeira é que a autorização judicial deve indicar o parâmetro de consulta e o período, e não apenas o nome do investigado, porque é o parâmetro que delimita o alcance da operação. A segunda é que o provedor assume, ao executar a consulta, posição de auxiliar do juízo, com deveres de documentação equivalentes aos de quem produz prova técnica.

A terceira é que a falta de autorização não se convalida pela obtenção posterior de ordem judicial, ressalvada a hipótese de urgência disciplinada adiante. Nenhuma dessas consequências decorre da qualificação do dado, e todas decorrem da qualificação do ato.

A Lei nº 13.709/2018 oferece, em definição que o Marco Civil não possui, o conceito de tratamento como toda operação realizada com dados pessoais, entre as quais o texto legal enumera a utilização, o processamento, a comunicação e a extração (Brasil, 2018).

Ainda que o diploma exclua de seu âmbito o tratamento voltado à persecução penal, o conceito permanece disponível como categoria dogmática. Vincular duas bases é operação, e operação é tratamento. Reputa-se estranho que o ordenamento defina com precisão a operação para fins civis e administrativos e a ignore justamente quando ela produz o elemento probatório que sustentará uma condenação.

O PERCURSO EUROPEU: DE MINISTERIO FISCAL À SEPARAÇÃO ESTANQUE

O Tribunal de Justiça da União Europeia decidiu, em 2 de outubro de 2018, o caso Ministério Fiscal, originado de investigação espanhola sobre roubo de aparelho telefônico. A polícia pretendia obter a identidade dos titulares dos números ativados com o IMEI do aparelho subtraído, e o juiz de instrução recusou o pedido por entender que o delito não era grave o bastante.

A Corte respondeu que o acesso limitado a dados de identidade civil dos titulares de cartões SIM não constitui ingerência suficientemente grave nos direitos dos arts. 7 e 8 da Carta, de modo que o requisito de gravidade do delito não se aplica (União Europeia, 2018).

A jurisprudência europeia sobre conservação de dados formou-se em etapas conhecidas, a partir da invalidação da diretiva de conservação em Digital Rights Ireland, em 2014, e da recusa da conservação geral e indiferenciada em Tele2 Sverige, em 2016.

A Diretiva 2002/58/CE autoriza, no art. 15, item 1, que os Estados restrinjam direitos de confidencialidade por medidas legislativas necessárias e proporcionadas (União Europeia, 2002).

O ponto de partida do sistema é, assim, uma cláusula de exceção interpretada de modo restritivo, o que explica a preocupação constante da Corte com salvaguardas e com controle por instância independente.

A lógica do julgado de 2018 é escalar. Quanto mais intensa a ingerência, mais exigentes os requisitos de acesso. Identidade civil isolada situa-se no degrau inferior; dados de tráfego e de localização, que permitem conclusões precisas sobre a vida privada, permanecem reservados à criminalidade grave. A fragilidade da construção aparece na hipótese intermediária que a ADC 91 examina.

Em 30 de abril de 2024, reunido em Pleno, o Tribunal enfrentou essa hipótese no caso La Quadrature du Net e outros, relativo ao mecanismo francês de combate à contrafação em ambiente digital.

A Corte admitiu que os Estados imponham aos provedores de acesso a conservação geral e indiferenciada de endereços IP para o combate à criminalidade em geral, desde que a conservação não permita conclusões precisas sobre a vida privada do titular, o que se obtém por meio de separação verdadeiramente estanque entre os endereços IP e as demais categorias de dados pessoais, em especial os dados de identidade civil (União Europeia, 2024). O acórdão de 2024 acrescentou requisitos ao acesso, e não apenas à conservação.

A autoridade que pretende vincular endereço IP a identidade civil deve operar por procedimento técnico que preserve a separação, submetido a verificação periódica de confiabilidade por instância independente, com registro das consultas e salvaguardas contra desvio de finalidade.

Anja Elisabeth Dekhuijzen observou, em análise publicada em 2025 na *European Data Protection Law Review*, que a decisão representa manobra delicada entre a repressão de ilícitos digitais menos graves e a proteção dos direitos fundamentais dos usuários (Dekhuijzen, 2025).

Discorda-se, no ponto, da leitura que apresentá-la *La Quadrature du Net II* como flexibilização generalizada da jurisprudência europeia. O que a Corte fez foi substituir uma garantia processual, o controle prévio por juiz ou autoridade administrativa independente, por uma garantia arquitetural, a separação estanque auditada.

A substituição só é legítima porque a segunda garantia existe e funciona no contexto examinado. Orla Lynskey já havia demonstrado que o direito europeu de proteção de dados se estrutura sobre a existência de autoridades de controle dotadas de independência e poderes efetivos (Lynskey, 2015), e esse pressuposto é o que sustenta a solução de 2024.

Transportar o critério europeu para o Brasil sem o pressuposto que o sustenta seria erro de método. A Lei nº 13.709/2018 exclui de seu âmbito o tratamento de dados realizado para fins exclusivos de segurança pública e de investigação e repressão de infrações penais, remetendo a matéria a legislação específica que até hoje não foi editada (Brasil, 2018).

O anteprojeto elaborado por comissão de juristas e apresentado à Câmara dos Deputados em 2020 previa autoridade de fiscalização, e o Projeto de Lei nº 1.515/2022 alterou o desenho em pontos sensíveis, conforme documentou a nota técnica produzida por Cynthia Pícolo Gonzaga de Azevedo e outros pesquisadores (Azevedo et al., 2022).

A comparação sugere, ademais, que o debate brasileiro tem discutido a pergunta errada. Enquanto se disputa a etiqueta do dado, o direito europeu já se ocupa da arquitetura dos sistemas que o guardam, o que indica maturidade regulatória ainda não alcançada aqui. A falta de lei específica sobre tratamento de dados na persecução penal não é lacuna neutra.

Ela produz, em alguma medida, o efeito de transferir ao processo penal a função de suprir, caso a caso, aquilo que deveria ser resolvido por norma geral e por fiscalização administrativa. Conquanto a solução judicial seja imperfeita, ela é a única que o desenho atual comporta.

Enquanto essa lacuna persistir, o Brasil não dispõe da instância independente que o modelo europeu pressupõe. Sustenta-se, por isso, que a reserva de jurisdição opera aqui como sucedâneo funcional da autoridade de controle, e não como excesso de cautela de um sistema desconfiado.

O juiz não é a solução ideal para verificar arquitetura de bancos de dados, tarefa para a qual falta ao Judiciário estrutura técnica. Ele é a única instância disponível, e retirá-lo sem substituto deixaria a operação sem controle algum.

Divergir da literatura estrangeira nesse ponto é o núcleo da contribuição pretendida. Os autores europeus discutem se o controle prévio judicial pode ser dispensado quando existe separação estanque auditada, e a resposta afirmativa faz sentido no ambiente institucional em que foi formulada.

A pergunta brasileira é outra, e a literatura citada não a considera: o que fazer quando não há autoridade de controle, não há obrigação legal de separação, não há auditoria e não há registro obrigatório das consultas? A resposta que decorre do próprio raciocínio europeu é conservar o controle prévio até que os pressupostos alternativos existam.

BENEDIK, CARPENTER E A QUALIDADE DA LEI COMO PARÂMETRO

O Tribunal Europeu de Direitos Humanos julgou, em 24 de abril de 2018, o caso Benedik contra Eslovênia, no qual a polícia obtivera de provedor, sem ordem judicial, os dados do assinante associados a endereço IP dinâmico registrado por autoridade suíça. Por seis votos a um, a Quarta Seção reconheceu violação do art. 8 da Convenção (Conselho da Europa, 2018).

O fundamento é instrutivo e costuma ser mal reproduzido nas citações brasileiras: a Corte não afirmou que toda identificação por IP exige ordem judicial, e sim que a base legal invocada carecia de clareza, não oferecia proteção contra ingerência arbitrária, não previa salvaguardas contra abuso e não submetia o poder policial a supervisão independente. Os fatos do caso esloveno merecem detalhe, porque a prática brasileira os reproduz com fidelidade incômoda.

A polícia invocou dispositivo do código de processo penal que obrigava operadoras a revelar informações sobre titulares de meios de comunicação não constantes de listas públicas, e o provedor forneceu o nome e o endereço do pai do investigado, assinante do serviço. Somente meses depois a autoridade obteve ordem judicial para acessar os dados do assinante e os dados de tráfego vinculados ao endereço. A sequência coincide com a que se observa em inquéritos brasileiros: requisição direta primeiro, autorização depois, com a identificação já consumada.

A Corte europeia observou que a legislação eslovena não previa regras sobre conservação dos dados e não oferecia salvaguardas contra abuso, o que sugere que o vício não estava na conduta isolada dos policiais. Ainda que se admita boa-fé dos agentes, o resultado seria o mesmo, porque a garantia protege contra a possibilidade de arbítrio e não apenas contra o arbítrio efetivamente praticado.

A lição interessa ao Brasil por razão simples: também aqui inexiste disciplina específica da operação, e a regularidade da requisição depende, não raro, da leitura que cada provedor faz de um dispositivo redigido antes do problema.

A ratio de Benedik é, portanto, de qualidade da lei, e ela reforça o argumento deste artigo por via indireta. Se o vício está na ausência de disciplina específica, de

salvaguardas e de supervisão, o remédio não se esgota em exigir ordem judicial caso a caso. Ele passa por normatizar a operação.

A Suprema Corte dos Estados Unidos decidiu, em 22 de junho de 2018, o caso *Carpenter*, no qual se discutia o acesso a registros históricos de localização celular mantidos por operadoras. Por cinco votos a quatro, a Corte assentou que a obtenção desses registros constitui busca para fins da Quarta Emenda e exige mandado apoiado em causa provável, limitando a aplicação da doutrina do terceiro (Estados Unidos, 2018).

A maioria observou que o fato de a informação estar em poder de terceiro não afasta, por si, a proteção constitucional. É de se questionar a utilidade de *Carpenter* para o caso brasileiro, e a objeção tem fundamento parcial. A decisão norte-americana trata de localização continuada por período prolongado, situação materialmente distinta da identificação pontual de um endereço IP em um minuto determinado.

A própria Corte ressaltou que a maioria das investigações continua a admitir requisição sem mandado. Transportar *Carpenter* como se autorizasse conclusão geral sobre metadados seria uso incorreto do precedente.

O que aproveita de *Carpenter* é o critério de decisão, não o resultado. A Corte perguntou se a informação obtida permitia reconstruir aspectos da vida privada que o titular não expôs voluntariamente, e respondeu que a entrega ao provedor ocorria sem ato afirmativo do usuário.

O mesmo teste, aplicado ao registro de conexão brasileiro, produz resposta análoga: nenhum usuário decide gerar registro de conexão, que é subproduto técnico do funcionamento da rede. A voluntariedade, base histórica da doutrina do terceiro, simplesmente não existe.

Três parâmetros externos convergem sem coincidir. A Corte de Luxemburgo admite dispensa de controle prévio mediante garantia arquitetural auditada; a Corte de Estrasburgo exige qualidade da lei, salvaguardas e supervisão independente; a Suprema Corte norte-americana afasta a doutrina do terceiro quando a produção do dado independe de ato voluntário do titular. Nenhum deles sustenta a requisição direta e desregulada que a prática brasileira consolidou.

CONSEQUÊNCIAS OPERATIVAS DO CRITÉRIO PROPOSTO

O voto do relator da ADC 91 admite exceção à exigência de autorização judicial em situações nas quais a espera comprometeria a resposta a dano grave. Nessas hipóteses, a requisição direta de dados seria admitida como medida de proteção, e não como instrumento de investigação ou de repressão, observadas balizas determinadas: proteção a bens jurídicos de alto valor, perigo atual involuntário, comprovação da imprescindibilidade do acesso imediato, documentação contemporânea aos fatos e submissão posterior da medida à apreciação judicial (Brasil, 2026a).

Sequestro em curso, ataque terrorista e crime cibernético em andamento foram os exemplos mencionados. Convém situar o estado do julgamento com precisão, porque análises divulgadas nas últimas semanas apresentam como resultado aquilo que ainda é voto isolado. Na sessão de 27 de agosto de 2026 votaram apenas os relatores dos três processos, e a apreciação foi suspensa sem data definida para retomada (Brasil, 2026a).

As posições examinadas neste artigo são propostas em discussão, e a tese que vier a ser fixada pode divergir das duas redações aqui confrontadas. A análise se dirige aos argumentos, cuja consistência independe do desfecho.

Prefere-se a solução do relator à alternativa proposta pelo ministro Dias Toffoli, que em voto-vista na sessão virtual de 6 a 13 de março de 2026 acompanhou a constitucionalidade do dispositivo, mas divergiu quanto às exceções, admitindo requisição direta apenas quando houver autorização expressa em lei. A tese que o voto-vista propôs foi assim redigida:

É constitucional o art. 10, § 1º, da Lei nº 12.965/14 (Marco Civil da Internet), que condiciona o compartilhamento de dados de tráfego por provedores, de forma autônoma ou associados a outros dados pessoais, à obtenção de prévia autorização judicial. Consequentemente, a identificação do usuário mediante a correlação, pelo provedor, entre os dados cadastrais e os registros de conexão ou de acesso a aplicações de internet, exige autorização judicial específica, ressalvados apenas os casos previstos em lei formal e proporcional (Brasil, 2026a).

A redação é tecnicamente superior à do relator em um aspecto e inferior em outro. Ela é superior porque nomeia a correlação como o ato que exige autorização, o que aproxima a tese da construção aqui defendida.

Ela é inferior porque remete a exceção à existência de lei formal e proporcional que hoje não existe, criando um vazio: enquanto o Congresso não legislar, casos de sequestro em andamento ficariam sem solução, e a prática responderia por meio de estado de necessidade invocado depois do fato, sem parâmetro.

As balizas do relator resolvem esse vazio, e ainda assim uma delas merece reparo. A exigência de perigo atual involuntário exclui da exceção situações em que a vítima contribuiu para a própria exposição, hipótese frequente em fraudes com engenharia social e em casos de aliciamento de adolescentes.

Objeta-se que o critério da involuntariedade importa, para o direito processual, um juízo sobre a conduta da vítima que não guarda relação com a urgência da proteção. Sugere-se sua substituição por critério de atualidade e de gravidade, sem indagação sobre a origem do perigo.

A documentação contemporânea aos fatos é a baliza de maior rendimento prático e a menos discutida. Ela impede a construção retrospectiva da urgência, que é o modo típico de degradação de qualquer regime excepcional.

Sem registro produzido no momento da requisição, a alegação de imprescindibilidade se torna inverificável, e o controle judicial posterior se converte em homologação. A experiência com outros regimes de urgência no processo penal brasileiro mostra que a exigência documental é o que separa a exceção controlada da exceção nominal.

Propõe-se, em complemento, prazo determinado para a submissão judicial. O voto do relator refere submissão posterior sem fixar prazo, e a omissão tende a produzir dilação indefinida na prática forense. Vinte e quatro horas é intervalo compatível com a lógica das medidas de urgência já disciplinadas no ordenamento e suficiente para a elaboração do requerimento, considerando que os elementos justificadores já estarão documentados por força da baliza anterior.

INUTILIZABILIDADE E ÔNUS DE DEMONSTRAÇÃO DA FONTE INDEPENDENTE

Definido o regime do ato, resta a pergunta sobre a consequência do descumprimento, que os votos até aqui proferidos não enfrentam com profundidade. A tese proposta pelo ministro Dias Toffoli prevê efeitos ex nunc, ressalvadas da modulação as investigações e ações penais em curso nas quais a defesa tenha suscitado a controvérsia até a conclusão do julgamento (Brasil, 2026a).

A modulação resolve o problema de transição, e não o problema de regime. Ela diz o que acontece com o passado, sem dizer o que acontecerá com a violação futura. Rejeita-se a qualificação do vício como mera irregularidade sanável. Violada a reserva constitucional, a prova é ilícita, e a consequência é a inutilizabilidade, com desentranhamento e contaminação das derivadas, salvo demonstração de fonte independente. O que se propõe de novo é a atribuição do ônus dessa demonstração.

O ônus importa mais do que a regra que o precede. Na prática das varas criminais, a alegação de fonte independente costuma ser aceita mediante afirmação genérica de que a identificação teria sido obtida por outros meios, sem indicação de quais meios, de quando teriam sido acionados e de qual resultado teriam produzido.

Esse padrão frouxo esvazia a garantia, porque toda prova ilícita admite, no plano abstrato, alguma rota alternativa imaginável. Sustenta-se, por isso, critério mais exigente, formulado em três requisitos cumulativos.

A acusação deve indicar diligência concretamente existente nos autos, anterior ou contemporânea à correlação impugnada; deve demonstrar que essa diligência produziria a identificação de modo autônomo, e não apenas que poderia produzi-la; e deve apresentar documentação que permita verificar a cronologia. Ausente qualquer dos três, a fonte independente não se configura e a contaminação permanece.

A cronologia é o elemento que o critério proposto torna verificável. Quando a identificação por correlação antecede toda diligência alternativa, a alegação de que outra rota levaria ao mesmo resultado é reconstrução posterior, e reconstrução posterior não constitui fonte independente.

Existindo diligência anterior documentada, o exame se torna simples e a acusação nada perde. O critério não pune a investigação diligente. Ele retira valor probatório da narrativa construída depois do questionamento da defesa.

Gustavo Henrique Badaró demonstrou, ao tratar da cadeia de custódia da prova digital, que a confiabilidade do elemento probatório depende de documentação capaz de reconstituir cada intervenção sobre o objeto (Badaró, 2023).

O raciocínio se aplica com ajuste ao problema aqui examinado. A correlação é intervenção sobre dados, executada por terceiro, em ambiente que o juízo não inspeciona. Sem registro do que foi consultado, em qual base e mediante qual chave, o resultado chega ao processo como afirmação do provedor, insuscetível de verificação pela defesa.

O paralelo tem limite, e convém explicitá-lo. A cadeia de custódia foi pensada para objetos que a autoridade apreende e manipula, ao passo que a correlação ocorre em ambiente de terceiro, sob controle exclusivo dele. Transportar o instituto sem ajuste levaria a exigir do provedor procedimentos incompatíveis com sua atividade.

O que se propõe é mais modesto e provavelmente mais viável: registro estruturado da operação, gerado pelo próprio sistema, com os campos mínimos indicados adiante. Bases de dados comerciais já produzem registros dessa natureza para auditoria interna, de modo que a exigência tende a incidir sobre a conservação e a entrega do registro, e não sobre sua criação. Daí decorre dever de documentação que recai sobre o provedor e cuja imposição depende de norma.

O registro deve conter a identificação do ofício ou da decisão que autorizou a operação, as bases consultadas, os parâmetros de consulta, a data e a hora da execução e o responsável técnico. Falha em qualquer desses itens compromete a possibilidade de contraditório sobre a origem da identificação, e essa falha não pode ser suprida por presunção de regularidade dos atos praticados por particular.

Uma limitação metodológica precisa ser declarada. A afirmação sobre o padrão frouxo de aceitação da fonte independente apoia-se em observação da prática forense e em literatura que trata do tema em termos gerais, sem levantamento sistemático de

decisões. Inexiste, no Brasil, base que permita mensurar a frequência do acolhimento sem demonstração concreta.

A LACUNA INSTITUCIONAL E A PROPOSTA DE REDAÇÃO NORMATIVA

O art. 12 do Decreto nº 8.771/2016 obriga a autoridade máxima de cada órgão da administração pública federal a publicar anualmente relatórios estatísticos das requisições de dados cadastrais, com o número de pedidos, a listagem dos provedores destinatários e informações correlatas (Brasil, 2016).

O mecanismo existe, é conhecido e alcança apenas a esfera federal. Sua extensão às requisições de correlação, e sua replicação nos âmbitos estaduais, resolveria parte do problema de transparência com custo institucional reduzido.

Falta ao arranjo brasileiro, porém, o elemento que o modelo europeu considera indispensável. Não existe autoridade com competência para fiscalizar o tratamento de dados realizado para fins de investigação criminal, porque a Lei nº 13.709/2018 excluiu essa hipótese e remeteu a disciplina a lei específica que permanece pendente desde 2018 (Brasil, 2018).

O anteprojeto de 2020 e o Projeto de Lei nº 1.515/2022 disputam o desenho dessa autoridade sem que a matéria avance (Brasil, 2020; Brasil, 2022b). A ausência dessa instância produz efeito que raramente se explicita. Como não há quem audite a arquitetura das bases dos provedores, não há como verificar se a separação entre registros de conexão e cadastro é real ou meramente lógica, isto é, se as duas tabelas estão em sistemas distintos com controles de acesso próprios ou se convivem no mesmo ambiente, acessíveis pela mesma consulta.

A diferença é técnica e produz consequências jurídicas diretas sobre a plausibilidade de qualquer regime alternativo ao controle judicial.

Propõe-se, em consequência, a inclusão de novo parágrafo no art. 10 da Lei nº 12.965/2014, com a seguinte redação: a operação pela qual o provedor vincula registros de conexão ou de acesso a aplicações a dados cadastrais, com a finalidade de identificar

usuário determinado, depende de autorização judicial específica e fundamentada, ainda que os dados cadastrais isoladamente considerados possam ser requisitados na forma do § 3º.

O destinatário da proposta é o Congresso Nacional, e a via natural é a inclusão do dispositivo em projeto de lei já em tramitação sobre proteção de dados na persecução penal. Duas observações acompanham a redação sugerida.

A primeira é que a expressão usuária determinada exclui do dispositivo os pedidos de identificação em massa, que permanecem vedados pelo art. 11, § 3º, do Decreto nº 8.771/2016 e exigiriam disciplina própria, provavelmente incompatível com o desenho atual.

A segunda é que a referência ao § 3º evita a leitura de que o novo parágrafo revogaria por incompatibilidade a requisição administrativa de dados cadastrais. Ainda que a técnica legislativa admita soluções mais elegantes, a redundância parece preferível ao risco de interpretação restritiva do dispositivo remanescente.

Ao parágrafo proposto deve corresponder disciplina da exceção, com quatro requisitos cumulativos: perigo atual a bem jurídico de alto valor, imprescindibilidade do acesso imediato demonstrada no momento da requisição, documentação contemporânea dos elementos justificadores e submissão ao juízo competente em vinte e quatro horas. A inobservância de qualquer deles acarreta inutilizabilidade.

Enquanto a lei não vier, e a experiência legislativa recente recomenda não contar com prazo curto, o critério pode ser aplicado por via interpretativa. Órgãos de persecução penal dispõem de margem para autorregulação, e a fixação de orientação institucional que oriente a formulação de pedidos de correlação por via judicial reduziria a variação entre unidades e diminuiria o risco de nulidade. Uma diretriz nesse sentido, dirigida aos órgãos de controle das carreiras policiais e ministeriais, produziria efeito prático antes de qualquer alteração legislativa.

Uma objeção previsível merece resposta antes do fecho. Exigir autorização judicial para cada correlação poderia produzir decisões padronizadas, proferidas em série

e sem exame efetivo, hipótese em que o controle se converteria em formalidade e o custo se somaria à ineficácia.

O risco existe e não deve ser minimizado. Ele se reduz pela mesma via que reduz o risco em outras medidas de urgência: fundamentação específica sobre a necessidade da correlação, indicação do período consultado e vedação a pedidos genéricos, requisitos que o Decreto nº 8.771/2016 já impõe à requisição administrativa de dados cadastrais e que seriam transpostos, com adaptação, ao pedido judicial.

Registre-se que a proposta não amplia o rol de hipóteses de reserva de jurisdição, e sim explicita hipótese já contida no art. 10, § 1º, hoje contornada por via oblíqua. O ganho é de segurança jurídica: o provedor deixa de decidir sozinho, o investigado passa a contar com parâmetro verificável e o órgão de persecução obtém prova que resiste ao controle de admissibilidade.

Quanto ao alcance da proposta, duas delimitações são necessárias. A primeira é que o parágrafo sugerido não alcança a hipótese em que a autoridade já dispõe da identidade do investigado e busca apenas confirmar dado cadastral, situação que permanece regida pelo § 3º.

A segunda é que o regime proposto não incide sobre informações fornecidas de modo voluntário pelo próprio titular ou por terceiro legitimado, porque aí inexistiria operação estatal de correlação. Delimitar o alcance da tese é condição de sua utilidade prática, já que proposta destinada a alcançar tudo termina por não vincular nada.

CONCLUSÃO

O presente estudo dedicou-se à análise da reserva de jurisdição na identificação de usuários de internet a partir de endereço IP, especialmente no contexto da ADC 91 e da controvérsia sobre o alcance do art. 10 da Lei nº 12.965/2014.

A pesquisa demonstrou que a discussão não se limita à oposição formal entre dados cadastrais e registros de conexão. O ponto central reside na operação de correlação que vincula um identificador técnico, um marco temporal e uma pessoa determinada.

Essa operação, embora possa produzir como resultado informações cadastrais, possui impacto constitucional próprio, pois reconstrói um vínculo entre indivíduo e uso da rede. Buscando responder se a identificação civil de usuário por IP, data e horário pode ser realizada mediante simples requisição administrativa, estabeleceu-se como objetivo geral determinar o verdadeiro objeto do controle judicial nessa hipótese.

Por meio de abordagem hipotético-dedutiva, com análise normativa, jurisprudencial e comparada, examinou-se o regime jurídico brasileiro da requisição de dados, a experiência europeia sobre separação entre bases informacionais e as consequências processuais da obtenção de prova digital sem controle jurisdicional adequado.

Esse percurso permitiu confirmar a hipótese inicial de que o objeto relevante não é apenas o dado entregue, mas o tratamento informacional necessário para produzi-lo. No primeiro eixo de análise, constatou-se que o Marco Civil da Internet estrutura a proteção de dados em camadas distintas, diferenciando o acesso direto a dados cadastrais da disponibilização de registros de conexão e de acesso a aplicações.

Essa distinção, embora relevante, mostra-se insuficiente quando a autoridade pública formula requisição que, sob aparência cadastral, exige consulta a registros técnicos protegidos. A identificação por endereço IP não corresponde a uma busca simples em cadastro estático.

Ela pressupõe a localização de uma sessão de conexão, a verificação do marco temporal e a associação desse evento técnico a um usuário determinado. Por isso, a operação ultrapassa o campo da requisição cadastral ordinária.

No segundo eixo, verificou-se que a correlação entre bases deve ser compreendida como objeto normativo autônomo. O cruzamento entre registro de conexão e cadastro civil produz uma informação nova, inexistente em cada uma das bases consideradas isoladamente. O cadastro revela quem é o usuário; o registro técnico indica um evento de conexão; a correlação entre ambos afirma que determinada pessoa esteve associada a determinado IP em determinado momento.

Essa conclusão desloca o debate do rótulo atribuído ao dado para a função desempenhada pelo tratamento. Assim, o regime jurídico aplicável deve considerar a intensidade da ingerência e o risco de afetação à privacidade, à proteção de dados e ao contraditório.

No terceiro eixo, a comparação com o direito europeu evidenciou que o acesso a dados de identidade civil associados a endereços IP somente pode prescindir de controle prévio quando houver salvaguardas institucionais e técnicas robustas.

A separação estanque entre bases, a auditoria independente, o registro das consultas e a existência de autoridade de controle efetiva são pressupostos centrais desse modelo. No Brasil, entretanto, ainda não há disciplina legal específica para o tratamento de dados pessoais em matéria penal nem autoridade independente com competência adequada para fiscalizar esse campo. Essa lacuna impede a transposição automática da solução europeia e reforça a necessidade de preservação da autorização judicial como regra.

Diante do percurso desenvolvido, conclui-se que a identificação de usuário de internet por meio de IP, data e horário deve submeter-se à reserva de jurisdição. A resposta ao problema de pesquisa é, portanto, negativa: não é juridicamente adequado tratar essa diligência como simples fornecimento de dado cadastral.

Embora o resultado possa consistir em nome, filiação ou endereço, a sua obtenção depende de acesso e tratamento de registros técnicos protegidos. A exceção de urgência pode ser admitida apenas em hipóteses concretas, justificadas e posteriormente controladas pelo Judiciário.

Fora desses limites, a requisição direta fragiliza a proporcionalidade da medida e compromete a confiabilidade da prova produzida.

Reconhece-se que o debate comporta posições divergentes. De um lado, sustenta-se que a requisição direta favorece a eficiência da persecução penal, reduz atrasos investigativos e evita a perda de registros em crimes digitais, especialmente diante dos prazos legais de guarda.

De outro, argumenta-se que a dispensa generalizada de autorização judicial amplia o poder estatal de vigilância, transfere ao provedor a responsabilidade de decidir sobre direitos fundamentais e aumenta o risco de identificações equivocadas ou desproporcionais.

Ambas as preocupações são legítimas. Contudo, a eficiência investigativa não pode eliminar controles mínimos de necessidade, adequação, rastreabilidade e responsabilização. Ao término da investigação, entende-se que a solução constitucionalmente mais adequada consiste em reconhecer o ato de correlação como categoria jurídica própria.

O provedor que vincula IP, tempo e identidade civil não apenas informa um dado já existente; ele participa da produção de um elemento probatório relevante para a persecução penal. Por essa razão, a autorização judicial deve funcionar como garantia ordinária de controle, sem impedir respostas excepcionais em situações de urgência real.

O desenvolvimento futuro da matéria exige disciplina legislativa específica, critérios técnicos de documentação das consultas e mecanismos independentes de fiscalização. Enquanto tais instrumentos não forem plenamente instituídos, a reserva de jurisdição permanece como a salvaguarda mais consistente para equilibrar investigação penal e proteção de direitos fundamentais.

REFERÊNCIAS

ABREU, Jacqueline de Souza. **Privacidade, segurança e tecnologia**. 2022. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2022. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2139/tde-03102022-093648/publico/6853927DIO.pdf>. Acesso em: 28 ago. 2026.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza (org.). **Direitos fundamentais e processo penal na era digital**: doutrina e prática em debate. São Paulo: InternetLab, 2018. v. 1.

AZEVEDO, Cynthia Picolo Gonzaga de et al. **Nota técnica**: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Belo Horizonte: IRIS; Brasília: LAPIN, 2022. Disponível em: <https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf>. Acesso em: 28 ago. 2026.

CORDEIRO, G.H.A.; LUCA, G.D.; BARROS, R.M.; OLIVEIRA, P.C.; RENZETTI FILHO, R.N.; VITORIANO, R.M.; SANTOS, J.L.; FERREIRA, C.C.P. Reserva de jurisdição e arquitetura de dados: a ADC 91 e o teste de separação estanque no direito europeu. **Revista Eletrônica Amplamente**, Natal/RN, v. 5, n. 3, p. 1164-1195, jul./set., 2026.



BADARÓ, Gustavo Henrique. **A cadeia de custódia da prova digital**. In: OSNA, Gustavo; SARLET, Ingo Wolfgang; MATIDA, Janaína Roland; REICHEL, Luis Alberto; JOBIM, Marco Félix; RAMOS, Vitor de Paula (org.). *Direito probatório*. Londrina: Thoth, 2023.

BRASIL. Câmara dos Deputados. **Comissão de Juristas**. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf>. Acesso em: 28 ago. 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022b. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2326300>. Acesso em: 28 ago. 2026.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República, 2016.

BRASIL. **Lei nº 12.830, de 20 de junho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Brasília, DF: Presidência da República, 2013.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores. Brasília, DF: Presidência da República, 1998.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 626.983/PR**. Relator: Ministro Olindo Menezes (Desembargador convocado do TRF da 1ª Região). Sexta Turma. Julgado em 8 fev. 2022a. Informativo de Jurisprudência nº 724. Disponível em: <https://www.stj.jus.br/sites/portaltj/Paginas/Comunicacao/Noticias/18022022-E-valido-pedido-de-congelamento-de-dados-telematicos-antes-de-autorizacao-judicial--decide-Sexta-Turma.aspx>. Acesso em: 28 ago. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Declaratória de Constitucionalidade nº 91**. Relator: Ministro Cristiano Zanin. Andamento processual. Brasília, DF: STF, 2026a. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=7036064>. Acesso em: 28 ago. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4.906/DF**. Relator: Ministro Nunes Marques. Plenário. Julgamento finalizado em 11 set. 2024. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4357880>. Acesso em: 28 ago. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 5.059 e Ação Direta de Inconstitucionalidade nº 5.073**. Relator: Ministro Dias Toffoli.

CORDEIRO, G.H.A.; LUCA, G.D.; BARROS, R.M.; OLIVEIRA, P.C.; RENZETTI FILHO, R.N.; VITORIANO, R.M.; SANTOS, J.L.; FERREIRA, C.C.P. Reserva de jurisdição e arquitetura de dados: a ADC 91 e o teste de separação estanque no direito europeu. *Revista Eletrônica Amplemente*, Natal/RN, v. 5, n. 3, p. 1164-1195, jul./set., 2026.



Andamento processual. Brasília, DF: STF, 2026b. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4483504>. Acesso em: 28 ago. 2026.

CONSELHO DA EUROPA. Tribunal Europeu de Direitos Humanos. Case of Benedik v. Slovenia. **Petição nº 62357/14**. Quarta Seção. Julgado em 24 abr. 2018. Disponível em: <https://www.bailii.org/eu/cases/ECHR/2018/363.html>. Acesso em: 28 ago. 2026.

DEKHUIJZEN, Anja Elisabeth. **La Quadrature du Net II and data retention under Article 15(1) e Privacy Directive**: CJEU walks a tightrope on IP addresses retention and access for public authorities in non-serious crime. *European Data Protection Law Review*, v. 11, n. 2, 2025. Disponível em: <https://edpl.lexxion.eu/article/EDPL/2025/2/17>. Acesso em: 28 ago. 2026.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2020.

ESTADOS UNIDOS. Supreme Court. **Carpenter v. United States, 585 U.S. 296 (2018)**. Julgado em 22 jun. 2018. Disponível em: <https://caselaw.findlaw.com/court/us-supreme-court/16-402.html>. Acesso em: 28 ago. 2026.

LYNSKEY, Orla. **The foundations of EU data protection law**. Oxford: Oxford University Press, 2015.

MENDES, Laura Schertel Ferreira; BIONI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

SAAD, Marta; COSTA ROSSI, Helena; HENRIQUE PARTATA, Pedro. **A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria?** Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, e1071, 2024. DOI: <https://doi.org/10.22197/rbdpp.v10i3.1071>.

SARKIS, Jamilla Monteiro. **Direito da pessoa imputada ao anonimato digital**. *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, e1044, 2024. DOI: <https://doi.org/2197/rbdpp.v10i3.1044>.

SOLOVE, Daniel J. **A taxonomy of privacy**. *University of Pennsylvania Law Review*, v. 154, n. 3, p. 477-564, 2006. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622. Acesso em: 28 ago. 2026.

UNIÃO EUROPEIA. **Parlamento Europeu e Conselho**. Diretiva 2002/58/CE, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. *Jornal Oficial das Comunidades Europeias*, 2002.

UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-207/16**, Ministério Fiscal. Grande Secção. Julgado em 2 out. 2018. ECLI:EU:C:2018:788. Disponível em: <https://dpcuria.eu/case?reference=C-207/16>. Acesso em: 28 ago. 2026.

UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-470/21**, La Quadrature du Net e outros. Pleno. Julgado em 30 abr. 2024. Disponível em: <https://curia.europa.eu/site/upload/docs/application/pdf/2024-04/cp240075en.pdf>. Acesso em: 28 ago. 2026.

Submissão: junho de 2026. Aceite: julho de 2026. Publicação: setembro de 2026.

CORDEIRO, G.H.A.; LUCA, G.D.; BARROS, R.M.; OLIVEIRA, P.C.; RENZETTI FILHO, R.N.; VITORIANO, R.M.; SANTOS, J.L.; FERREIRA, C.C.P. Reserva de jurisdição e arquitetura de dados: a ADC 91 e o teste de separação estanque no direito europeu. **Revista Eletrônica Amplamente**, Natal/RN, v. 5, n. 3, p. 1164-1195, jul./set., 2026.

