Staatstrojaner, *Zitiergebot* e a decisão do *Bundesverfassungsgericht* de 2025: atualização do quadro constitucional da busca remota on-line do § 100b *StPO* (policeware)[1]

Sauvei Lai[2]

Resumo: Este artigo examina a decisão do Tribunal Constitucional Federal da Alemanha de 24 de junho de 2025, na reclamação constitucional *1 BvR 180/23, Trojaner II*, que redefiniu o quadro constitucional da busca remota on-line (*Online-Durchsuchung*) e da interceptação de telecomunicações na fonte (*Quellen-TKÜ)* em sistema informático do investigado, no âmbito do processo penal germânico. A Corte consolidou um duplo controle das normas habilitadoras da investigação oculta digital: um controle material, que reserva a medida à criminalidade especialmente grave, e um controle formal, fundado no *Zitiergebot*, a exigência da nomeação expressa de cada direito fundamental comprimido pela lei restritiva. Examinam-se, ainda, o regime bifásico de proteção do núcleo essencial da vida privada e a advertência quanto à gestão estatal de vulnerabilidades tecnológicas. Ao final, projeta-se o precedente sobre o ordenamento brasileiro, à luz do PL 402/2024 e da ADPF 1143/DF.

Palavras-chave: Policeware. Busca remota on-line. Quellen-TKÜ. Zitiergebot. Prova digital. Bundesverfassungsgericht.

Abstract: *This article analyses the judgment of the German Federal Constitutional Court (Bundesverfassungsgericht) of 24 June 2025 in Constitutional Complaint No. 1 BvR 180/23 (Trojaner II), which substantially reshaped the constitutional framework applicable to remote digital searches (Online-Durchsuchung) and source telecommunications surveillance (Quellen-TKÜ) carried out through the infiltration of an investigated person's information system within the German criminal process. The Court articulated a dual constitutional review of statutory authorisations for covert digital investigations: a substantive review, limiting such powers to the investigation of particularly serious offences, and a formal review, based on the constitutional principle known as the Zitiergebot, which requires the legislature expressly to identify every fundamental right affected by a restrictive statute. The decision also elucidates a two-tier mechanism for safeguarding the*

[1] **Declaração de transparência sobre o uso de Inteligência Artificial.** O autor utilizou sistema de inteligência artificial generativa como ferramenta de apoio em etapas específicas da pesquisa e da redação científica, incluindo organização preliminar de conteúdos, sugestões de estrutura textual, revisão gramatical, tradução e aperfeiçoamento estilístico. Todo o material produzido com auxílio dessa ferramenta foi objeto de supervisão humana contínua, com conferência independente das informações, reescrita parcial ou integral quando necessário, verificação das fontes empregadas e validação crítica dos argumentos desenvolvidos. A responsabilidade pela seleção das referências, pela exatidão das citações, pela análise jurídica empreendida, pelas posições doutrinárias defendidas e pelas conclusões alcançadas é integralmente do autor. A inteligência artificial foi empregada exclusivamente como ferramenta de suporte, não tendo atuado como autora, coautora ou responsável pelo conteúdo científico do trabalho.

[2] Promotor de Justiça do Ministério Público do Estado do Rio de Janeiro (desde 1999). Mestre em Direito Digital. Especialista em Teoria Geral do Processo. Professor. (Co)autor de obras e artigos jurídicos. Coordenador acadêmico da pós-graduação do IERBB/MPRJ (2024/2026). Presidente da Comissão Permanente de Estudos em Direito Digital do IERBB/MPRJ (2024/2026). Integrante do Grupo de Combate a Crimes Cibernéticos do MPRJ (2024/2025). Membro-auxiliar da Procuradoria-Geral da República no Supremo Tribunal Federal e Superior Tribunal de Justiça (2021/2023). Examinador do concurso público para Delegado da Polícia Civil do Rio de Janeiro (2021/2022). Membro do grupo de trabalho da sub-relatoria da revisão do novo Código de Processo Penal (NCPP) na Câmara dos Deputados (2019). Representante da Associação Nacional dos Membros do Ministério Público (CONAMP) perante a Câmara dos Deputados na discussão do NCPP (2021) e Supremo Tribunal Federal na audiência pública da ADPF 1143/DF (2024). Autor do anteprojeto de lei nº 4.939/2020 sobre provas digitais e outras diretrizes. Ex-Defensor Público do Rio de Janeiro (1998/1999). Aprovado no concurso público para Delegado da Polícia Federal (1997).

inviolable core sphere of private life and highlights the constitutional risks arising from the State's retention and management of technological vulnerabilities. Finally, the article explores the possible repercussions of the ruling for Brazilian law, with particular reference to Bill No. 402/2024 and ADPF 1143/DF.

Keywords: *Policeware. Online remote search. Source telecommunications surveillance. Zitiergebot. Digital evidence. German Federal Constitutional Court.*

A permissão para o uso do *policeware* (software de vigilância eletrônica instalado ocultamente no dispositivo do investigado para a captação remota de dados e de comunicações, seja em tempo real, seja por acesso ao conteúdo armazenado)[3], como medida investigativa na apuração de crimes praticados, introduzida no § 100b na *Strafprozessordnung* (*StPO*)[4], o Código de Processo Penal alemão, em julho de 2017, não encerrou o ciclo de exame constitucional sobre a matéria.

Em 24 de junho de 2025, o *Bundesverfassungsgericht* (*BVerfG*), Tribunal Constitucional Federal alemão, guardião da *Grundgesetz* (*GG*, a Lei Fundamental de Bonn, isto é, a Constituição alemã[5]) e cujo controle de constitucionalidade corresponde, no Brasil, ao exercido pelo Supremo Tribunal Federal, ao julgar o processo *1 BvR 180/23*[6] (*Trojaner II*, por constituir o segundo pronunciamento do tribunal sobre o *Staatstrojaner*, após o precedente de 2008), submeteu o uso da ferramenta investigativa a novo controle de constitucionalidade, exigindo observância a requisitos materiais e formais que condicionam a ferramenta tecnológica.

A decisão não proibiu o emprego do *Staatstrojaner*, mas delimitou com maior rigor as fronteiras da intervenção estatal no espaço digital do investigado, impondo ao legislador exigências de densidade normativa que o marco regulatório então vigente não satisfazia.

---

[3] Sobre o conceito, os requisitos, as condições e as salvaguardas do policeware em perspectiva do Direito comparada: LAI, Sauvei. Policeware: infecção de software em sistema informático do investigado para fins de vigilância eletrônica. Salvador: JusPodivm, 2024. Disponível em: https://www.editorajuspodivm.com.br/policeware-infeccao-de-software-em-sistema-informatico-do-investigado-para-fins-de-vigilancia-eletronica-2024-1ed. Acesso em: 13/07/2026.

[4] ALEMANHA. Strafprozessordnung (StPO), § 100b, Abs. 1. Disponível em: https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0659. Acesso em: 26/06/2026. Na tradução oficial inglesa do § 100b, Abs. 1, StPO (Section 100b (1)): "Technical means may be used even without the knowledge of the person concerned to gain covert access to an information technology system used by the person concerned and to extract data from that system ('covert remote search of information technology systems') if [...] certain facts give rise to the suspicion that a person has, either as an offender or participant, committed an especially serious crime as referred to in subsection (2) [...]." Em tradução livre: "Mesmo sem o conhecimento do investigado, é permitido intervir, por meios técnicos, em um sistema informático por ele utilizado, e dele coletar dados (busca remota on-line), quando [...] determinados fatos fundamentem a suspeita de que alguém, como autor ou partícipe, cometeu um crime especialmente grave dentre os designados no Absatz 2 [...]."

[5] ALEMANHA. Grundgesetz (GG), art. 10, Abs. 1, na tradução oficial inglesa (Article 10 (1)): "The privacy of correspondence, posts and telecommunications shall be inviolable." Em tradução livre: "O sigilo da correspondência, bem como o sigilo postal e o das telecomunicações, são invioláveis." Disponível em: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html. Acesso em: 13/07/2026.

[6] BUNDESVERFASSUNGSGERICHT. Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II). Disponível em: Bundesverfassungsgericht - Decisions search - Order of 24 June 2025 Acesso em: 13/07/2026.

O ponto de partida do tribunal foi o diagnóstico de que a *Online-Durchsuchung* e a *Quellen-Telekommunikationsüberwachung* (*Quellen-TKÜ*), respectivamente, a busca remota que acessa a totalidade dos dados armazenados no sistema informático (§ 100b *StPO*) e a interceptação, na própria fonte, das telecomunicações em curso antes de sua criptografia (§ 100a, Abs. 1, S. 2 e 3, *StPO*)[7], não afetam um único direito fundamental, mas podem atingir dois simultaneamente.

A vigilância de telecomunicações na fonte, operada pela instalação de software oculto diretamente no dispositivo do investigado, para fins de monitoramento eletrônico, afeta tanto o *IT-Grundrecht*, direito à confidencialidade e à integridade dos sistemas informáticos[8], construído pela própria corte desde 2008[9], quanto o sigilo das telecomunicações previsto no art. 10, Abs. 1, *GG*, considerando que o acesso direto ao dispositivo possibilita a captação de comunicações em curso.

A *Online-Durchsuchung* do § 100b, por alcançar todos os dados armazenados no sistema informático do investigado, sujeita-se igualmente a essa dupla incidência quando o conteúdo interceptado inclui comunicações em curso.[10] O tribunal reafirmou que os sistemas informáticos contemporâneos, sobretudo os *smartphones*, funcionam como verdadeiros "centrais da personalidade", acumulando dados de comunicação, registros pessoais, informações de localização, dados de saúde e elementos biométricos em densidade suficiente para reconstituir um retrato detalhado da personalidade do indivíduo, o que, por si só, revela a intensidade da intervenção estatal, impondo a elevação das exigências de justificação constitucional.

No plano material, o *BVerfG* declarou a nulidade parcial do § 100a, Abs. 1, Sätze 2 e 3, *StPO*, por violação ao princípio da proporcionalidade em sentido estrito[11]. A *Quellen-TKÜ lato sensu* (§ 100a, Abs. 1, S. 2, *StPO*), que autoriza a vigilância das telecomunicações em curso mediante acesso direto ao dispositivo, foi reputada incompatível com o art. 2º, Abs. 1,

---

[7] Para o exame no direito comparado dessas modalidades: LAI, Sauvei. Policeware: infecção de software em sistema informático do investigado para fins de vigilância eletrônica. Salvador: JusPodivm, 2024. Disponível em: https://www.editorajuspodivm.com.br/policeware-infeccao-de-software-em-sistema-informatico-do-investigado-para-fins-de-vigilancia-eletronica-2024-1ed. Acesso em: 13/07/2026.

[8] No direito brasileiro, a confidencialidade, a integridade e a disponibilidade dos dados e sistemas informáticos encontram tutela, no plano infraconstitucional, na Convenção sobre o Crime Cibernético (Convenção de Budapeste, de 23/11/2001), aprovada pelo Decreto Legislativo nº 37, de 16/12/2021, e promulgada pelo Decreto nº 11.491, de 12/04/2023, cujo Título 1 (arts. 2º a 6º) reúne os "crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador". Nos termos do art. 2º (Acesso ilegal): "Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. [...]". Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 13/07/2026.

[9] BUNDESVERFASSUNGSGERICHT. Urteil vom 27. Februar 2008 – 1 BvR 370/07 (BVerfGE 120, 274). Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html. Acesso em: 26/06/2026.

[10] BUNDESVERFASSUNGSGERICHT. Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II), Rn. 195. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2025/06/rs20250624_1bvr018023en.html Acesso em: 26/06/2026.

[11] O princípio da proporcionalidade desdobra-se em três derivações sucessivas: adequação (a medida é apta a promover o fim perseguido), necessidade (inexiste meio igualmente eficaz e menos gravoso) e proporcionalidade em sentido estrito (os benefícios superam os ônus impostos aos direitos fundamentais). No caso, a busca remota pode ser adequada e necessária à elucidação do delito, porém, tratando-se de infração de pequena gravidade, a intensidade da intervenção nos direitos fundamentais supera o ganho investigativo. A referência clássica sobre a estrutura tripartite do princípio é a teoria dos direitos fundamentais em: ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução de Virgílio. Afonso da SILVA. São Paulo: Malheiros, 2011, p. 167.

c/c art. 1º, Abs. 1, e com o art. 10, Abs. 1, *GG* (respectivamente, o direito geral de personalidade, do qual deriva o direito à confidencialidade e à integridade dos sistemas informáticos, além do sigilo das telecomunicações), na medida em que o catálogo de crimes autorizadores não abrangia crimes especialmente graves, mas sim infrações cuja pena máxima não excedesse três anos de privação de liberdade. Levando em conta a dupla e intensa afetação de direitos fundamentais decorrente do acesso direto ao dispositivo, que permite capturar, além do conteúdo da comunicação, sincronizações de nuvem, dados de localização, padrões de uso e registros de alta pessoalidade, o tribunal reputou que a medida somente se justifica na persecução de criminalidade de especial gravidade[12], com pena máxima superior a cinco anos ou de peso equivalente ao dessa faixa sancionatória (isto é, ainda que a pena máxima cominada não supere cinco anos, admite-se a medida quando o desvalor concreto do crime se equipare ao das infrações dessa faixa, afastando-se um critério puramente aritmético), em linha com o parâmetro já estabelecido para outras medidas de alta invasividade, como a escuta ambiental.[13] A *Quellen-TKÜ* ampliada (§ 100a, Abs. 1, S. 3[14], *StPO*), que autoriza o acesso a conteúdos de comunicação já armazenados no dispositivo, não foi declarada inconstitucional, mas o tribunal delimitou-lhe o alcance. É lícita apenas em relação a dados que, durante o período de vigilância, também seriam alcançáveis por uma interceptação telefônica convencional (§ 100a, Abs. 1, S. 1, *StPO*), de modo que o acesso retroativo a conteúdos armazenados, fora daquele intervalo temporal, ou seja, anteriores ao início da medida, seria vedado. Assim, uma conversa de aplicativo trocada e gravada no aparelho dias antes da autorização judicial, embora ainda armazenada no dispositivo, não poderia ser acessada.

No plano formal, a decisão introduziu exigência autônoma de validade que não havia sido objeto de escrutínio constitucional anterior nas matérias de investigação digital, isto é, o cumprimento do *Zitiergebot*[15], previsto no art. 19, Abs. 1, S. 2, *GG*. Por força desse princípio constitucional, toda lei que restringe direito fundamental deve indicar expressamente, em seu texto, qual direito está sendo limitado, com a menção do respectivo artigo da Lei Fundamental.

---

[12] A expressão empregada pelo tribunal é "besonders schwere Straftaten" (crimes especialmente graves), reservando-se a medida, em regra, às infrações com pena máxima superior a cinco anos de privação de liberdade. BUNDESVERFASSUNGSGERICHT. Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II), Rn. 205. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2025/06/rs20250624_1bvr018023en.html Acesso em: 13/07/2026.

[13]BUNDESVERFASSUNGSGERICHT. Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II). O julgamento foi publicado em agosto de 2025 e decidido simultaneamente com o processo 1 BvR 2466/19 (Trojaner I), relativo às habilitações preventivas do § 20c PolG NRW, mantidas como constitucionais em sua integralidade. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2025/bvg25-069.html Acesso em: 13/07/2026.

[14] ALEMANHA. Strafprozessordnung (StPO), § 100a, Abs. 1, S. 3, na tradução oficial inglesa (Section 100a (1), third sentence): "The content and the circumstances of the communication stored in the person concerned's information technology systems may be intercepted and recorded if they could also have been intercepted and recorded in encrypted form during ongoing transmission processes in the public telecommunications network." Em tradução livre: "Os conteúdos e as circunstâncias da comunicação armazenados no sistema informático do investigado podem ser monitorados e registrados quando também pudessem, durante o processo de transmissão em curso na rede pública de telecomunicações, ter sido monitorados e registrados em forma cifrada." Disponível em: https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0575. Acesso em: 13/07/2026.

[15] Zitiergebot, em tradução livre, corresponde ao "dever de citação", a exigência constitucional de que a lei restritiva nomeie expressamente o direito fundamental limitado, com indicação do respectivo artigo da Lei Fundamental (art. 19, Abs. 1, S. 2, GG). Disponível em: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html. Acesso em: 14/07/2026.

Assim, o § 100b *StPO*, ao autorizar a *Online-Durchsuchung*, permite ingerência tanto no *IT-Grundrecht* quanto no art. 10, Abs. 1, *GG*, mas o texto legal omitiu a referência expressa a este último direito. Consequentemente, o *BVerfG* tratou essa omissão como vício de inconstitucionalidade formal, sem emitir qualquer juízo sobre o mérito ou sobre a proporcionalidade da medida[16], pois o erro do legislador não foi autorizar uma intervenção de conteúdo abusivo, mas ter regulamentado de forma imprecisa e sem especificar expressamente quais liberdades constitucionais estariam sendo comprimidas, impedindo que os cidadãos soubessem com exatidão de que modo o Estado poderia interferir em sua esfera privada. Tal requisito (de transparência normativa) adquire relevo no ambiente digital, no qual uma única medida investigativa pode incidir sobre múltiplos direitos fundamentais de forma simultânea e difusa. Como solução pragmática, o *BVerfG* declarou o § 100b *StPO* incompatível com a Constituição, todavia, manteve sua vigência provisória[17] até a edição de nova disciplina legislativa, gerando período de transição em que as investigações em curso não foram automaticamente interrompidas.[18]

No plano metodológico, a decisão de 2025 consolida, na jurisprudência do *BVerfG*, o chamado duplo controle constitucional das normas permissivas de investigação oculta digital. De um lado, o controle material, centrado na proporcionalidade em sentido lato (adequação, necessidade e proporcionalidade em sentido estrito), que examina se a intensidade da medida e o catálogo de crimes autorizadores guardam relação de equilíbrio com a magnitude da intervenção em direitos fundamentais. De outro, o controle formal, fundado no *Zitiergebot*, que escrutina se o texto legal nomeia explicitamente cada direito fundamental afetado, impondo ao legislador um dever de clareza e transparência como condição autônoma de validade.

Esses dois níveis de controle são independentes entre si e a ausência de qualquer um deles invalida a norma, mesmo que o outro esteja plenamente satisfeito. Trata-se de evolução significativa em relação ao marco anterior de 2008, que havia criado o *IT-Grundrecht* como direito à confidencialidade e integridade dos sistemas informáticos, mas que não havia articulado de forma tão nítida essa camada formal de exigência democrática de transparência legislativa.

---

[16]BUNDESVERFASSUNGSGERICHT. Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II). O dispositivo da decisão declarou nulos os §§ 100a Abs. 1 Sätze 2 e 3 c/c § 100a Abs. 1 S. 1 Nr. 1, Abs. 2 Nr. 1 (Buchst. a, c, d e t), Nr. 6 e Nr. 7 Buchst. b StPO, na redação da Lei de 17 de agosto de 2017 (BGBl. I, S. 3202), por violação ao art. 2º, Abs. 1, c/c art. 1º, Abs. 1, GG e, apenas quanto ao § 100a Abs. 1 S. 2, também ao art. 10, Abs. 1, GG. Em transcrição do trecho pertinente (BUNDESVERFASSUNGSGERICHT, Press Release nº 69/2025, itens B.III.3 e C, na versão oficial inglesa): "For formal reasons, the legislative authorisation of remote searches is incompatible with the Constitution. Insofar as the provision (also) grants powers to interfere with Art. 10(1) of the Basic Law, it does not satisfy the requirement that the affected fundamental right be expressly specified laid down in Art. 19(1) second sentence of the Basic Law." Em tradução livre: "A busca remota on-line é, por razões formais, incompatível com a Constituição. O dispositivo, na medida em que autoriza (também) intervenções no art. 10, Abs. 1, GG, não satisfaz o Zitiergebot do art. 19, Abs. 1, S. 2, GG." Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2025/bvg25-069.html. Acesso em: 14/07/2026.

[17] Em transcrição do trecho pertinente (BUNDESVERFASSUNGSGERICHT, Press Release nº 69/2025, item C, na versão oficial inglesa): "In contrast, § 100b(1) of the Code of Criminal Procedure must merely be declared incompatible with the Constitution. [...] The provision will continue to apply until the legislator adopts a new provision." Em tradução livre: "Em contrapartida, o § 100b, Abs. 1, StPO é apenas declarado incompatível com a Constituição. [...] O dispositivo permanece em vigor até uma nova disciplina legislativa." BUNDESVERFASSUNGSGERICHT. Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II). Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2025/bvg25-069.html. Acesso em: 14/07/2026.

[18]TSAMBIKAKIS & PARTNER RECHTSANWÄLTE. Trojaner II: Quellen-TKÜ teilweise verfassungswidrig. Outubro de 2025. Disponível em: https://www.tsambikakis.com/aktuelles/trojaner-beschluss. Acesso em: 26/06/2026.

A decisão também reforçou as obrigações decorrentes da proteção do núcleo essencial da vida privada, regulada no § 100d *StPO*, estabelecendo que ela deve ser observada em dois momentos sequenciais. No primeiro, durante a coleta de dados, os órgãos responsáveis pela implementação do *Staatstrojaner* devem adotar filtros tecnológicos[19] destinados a impedir, na medida do possível, a extração de informações pertencentes à esfera central da vida privada do investigado. No segundo, durante a análise e o processamento dos dados obtidos, os elementos eventualmente capturados que pertençam àquela esfera devem ser destruídos imediatamente ou submetidos ao tribunal competente para deliberação sobre sua usabilidade, nos termos já previstos no § 100d, Abs. 3, *StPO*. O *BVerfG* ressalvou, contudo, que em vigilâncias automatizadas em tempo real a interrupção imediata da operação ao se detectar conteúdo de núcleo pode ser tecnicamente inviável, de forma que o dever de destruição imediata *a posteriori* substitui, nessas hipóteses, o dever de interrupção da medida.[20]

Um aspecto que o *BVerfG* deixou em aberto, mas sobre o qual emitiu advertência ao legislador, é a dependência estrutural do *Staatstrojaner* em relação a vulnerabilidades de software não corrigidas, as denominadas *zero-day exploits* (falhas de segurança ainda desconhecidas do próprio fabricante e, por isso, sem correção disponível)[21]. Para que o programa malicioso de monitoramento eletrônico seja instalado secretamente no dispositivo do investigado, é necessário explorar falhas existentes em sistemas operacionais ou aplicativos, falhas essas que, por definição, não ficam disponíveis apenas para os órgãos investigativos, mas também para atacantes hackers de qualquer natureza. O tribunal não reconheceu nessa dependência uma violação do dever de proteção do Estado em relação à segurança digital da população em geral, mas impôs expressamente ao legislador a obrigação de desenvolver um regime de gestão dessas vulnerabilidades, a fim de que o instrumento de investigação não se converta em vetor de risco para a infraestrutura digital de toda a sociedade, através de comunicação da falha ao fabricante para sua correção, depois de alcançada a finalidade investigativa, evitando que a mesma brecha permaneça explorável por criminosos contra, por exemplo, hospitais, instituições financeiras ou serviços públicos essenciais.[22]

O *Trojaner II* não reverte o modelo alemão de persecução penal digital construído entre 2008 e 2017, e sim o refina em três dimensões. Restringe o catálogo material de crimes autorizadores da *Quellen-TKÜ* a infrações de especial gravidade; estabelece o *Zitiergebot* como requisito formal autônomo de validade das normas de investigação digital, cobrando do legislador dever de transparência constitucional explícita quanto a cada direito

---

[19] Trata-se de mecanismos automatizados de triagem que buscam bloquear, já na coleta, a captura de dados pertencentes ao núcleo essencial da vida privada, por exemplo, rotinas que interrompam a gravação ao identificarem comunicações de conteúdo manifestamente íntimo (diários pessoais, conversas com médicos, sacerdotes ou familiares próximos) ou que descartem automaticamente os trechos assim classificados.

[20] BUNDESVERFASSUNGSGERICHT. Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II). O tribunal reconheceu que, especialmente em vigilâncias automatizadas em tempo real, a interrupção imediata da operação ao se detectar conteúdo de núcleo pode ser tecnicamente inviável, de forma que o dever de destruição imediata *a posteriori* substitui, nessas hipóteses, o dever de interrupção da medida. A versão oficial da decisão em inglês está disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2025/06/rs20250624_1bvr018023en.html. Acesso em: 14/07/2026.

[21] Sobre a dependência estrutural do policeware em relação a vulnerabilidades não corrigidas: LAI, Sauvei. Policeware: infecção de software em sistema informático do investigado para fins de vigilância eletrônica. Salvador: JusPodivm, 2024. Disponível em: https://www.editorajuspodivm.com.br/policeware-infeccao-de-software-em-sistema-informatico-do-investigado-para-fins-de-vigilancia-eletronica-2024-1ed. Acesso em: 13/07/2026; e BUNDESVERFASSUNGSGERICHT. Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II).

[22] TSAMBIKAKIS & PARTNER RECHTSANWÄLTE. Trojaner II: Quellen-TKÜ teilweise verfassungswidrig, 2025. Disponível em: https://www.tsambikakis.com/aktuelles/trojaner-beschluss. Acesso em: 13/07/2026.

fundamental afetado; e especifica o regime bifásico de proteção do núcleo essencial da vida privada, ajustando-o às características próprias das técnicas da vigilância automatizada.

O precedente tem significado para além do sistema alemão, na medida em que evidencia uma tensão estrutural presente em qualquer ordenamento que pretenda incorporar o *policeware* como meio de obtenção de prova. A multifuncionalidade das tecnologias investigativas digitais reclama normas de maior densidade do que as habitualmente suficientes para medidas tradicionais de investigação, porque uma única intervenção pode atravessar, simultaneamente, múltiplos âmbitos de proteção constitucional de direitos fundamentais, e o legislador que não os nomeia com precisão produz, mesmo sem intenção, um poder opaco incompatível com o Estado Democrático de Direito.

No Brasil, esse desafio está posto. Tramita no Senado Federal o Projeto de Lei nº 402/2024, que disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares, enquanto o Supremo Tribunal Federal examina a Arguição de Descumprimento de Preceito Fundamental (ADPF) 1143/DF, proposta pela Procuradoria-Geral da República, na qual se discute a ausência de regulamentação do uso desses programas, requerendo à corte a fixação de balizas para uso imediato pelos órgãos de investigação, ação em cuja audiência pública o autor deste artigo expôs, como representante da Associação Nacional dos Membros do Ministério Público (CONAMP), alguns dos parâmetros aqui examinados.[23]

Rio de Janeiro 14 de julho de 2026.

*

[23] BRASIL. Senado Federal. Projeto de Lei nº 402, de 2024. Ementa: disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 13/07/2026. Sobre a ADPF 1143/DF (rel. Min. Cristiano Zanin) e a audiência pública realizada em 10 e 11 de junho de 2024: STF, processo nº 6900814. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814. Acesso em: 13/07/2026. A participação do autor, representando a CONAMP (*amicus curiae*), está registrada em: https://www.conamp.org.br/imprensa/noticias/9304-stf-audiencia-publica-sobre-o-uso-de-ferramentas-de-monitoramento-secreto-conta-com-participacao-da-conamp.html. Acesso em: 13/07/2026.