A infiltração online no processo penal – Notícia sobre a experiência alemã

The Online Search in the Criminal Procedure Law – About the German Experience

Luís Greco[1]

Universidade Humboldt - Berlim, Alemanha

luis.greco@rewi.hu-berlin.de

https://orcid.org/0000-0003-3087-4561

Orlandino Gleizer[2]

Universidade Humboldt - Berlim, Alemanha

gleizero@student.hu-berlin.de

http://lattes.cnpq.br/5773080132816841

https://orcid.org/0000-0002-4877-748X

Resumo: O artigo descreve a discussão alemã sobre a técnica de investigação da infiltração online no processo penal e tenta extrair lições para o sistema brasileiro.

Palavras-chave: infiltração online; processo penal; direitos fundamentais; direito alemão.

[1] Professor Catedrático de Direito Penal, Direito Processual Penal e Direito Penal Estrangeiro e Teoria do Direito Penal da Universidade Humboldt, de Berlim, Alemanha. Habilitação em direito penal na Universidade Ludwig Maximilian, de Munique, Alemanha; doutor em direito e LL.M. na mesma instituição.

[2] Doutorando em Ciência do Direito pela Universidade Humboldt de Berlim; LL.M pela Universidade de Augsburg (Alemanha); mestre em Direito Penal pela Universidade do Estado do Rio de Janeiro. Advogado criminal; assistente científico junto à cátedra do Prof. Dr. Dr. Eric Hilgendorf, na Universidade Julius Maximiliam de Würzburg (Alemanha).

Abstract: *The article describes the German discussion about the online-infiltration as a fact-finding measure in Criminal Procedure and tries to learn some lessons for the Brazilian system.*

Keywords: *online search; criminal procedure; fundamental rights; German law.*

I. Introdução

Pode o Estado acessar nossos computadores remotamente, sem nosso conhecimento, com a finalidade de, vasculhando o conteúdo ali disponível, obter prova de crimes? Se sim, diante de que pressupostos? É dessas duas perguntas, sobre a legitimidade abstrata e concreta daquilo que no presente trabalho chamaremos de *infiltração online*, e que na Alemanha é conhecido como Online-Durchsuchung – o que seria mais literalmente de traduzir-se como "busca online" – que cuidaremos no presente artigo. A primeira delas, veremos, receberá uma resposta clara e definitiva: no Direito brasileiro, inexiste legitimação para essa medida. A experiência alemã será descrita em detalhe, sobretudo no que diz respeito à segunda pergunta, isto é, aos pressupostos da infiltração, a fim de oferecer elementos para um debate sobre uma eventual introdução da medida no Brasil.

Nossas reflexões terão, por primeiro passo, uma recapitulação da dogmática dos direitos fundamentais, que demarca âmbitos da vida em que o Estado só pode adentrar observando pressupostos relativamente severos (II.). Passaremos a uma análise mais detida da infiltração online, em que descreveremos as dimensões em que ela configura uma intervenção em direito fundamental, levando em conta especialmente o novo direito fundamental, cunhado pelo Tribunal Constitucional Federal alemão (Bundesverfassungsgericht – BVerfG), à integridade e confiabilidade de sistemas informáticos (III.). Depois de um breve retorno ao direito brasileiro (IV.), em que verificaremos a impossibilidade da medida segundo a *lex lata*, daremos notícia do regime da infiltração online no direito alemão, porque cremos que ele pode servir como linha de orientação para uma eventual legislação brasileira sobre o tema (V.). Por fim, mencionaremos três pontos controvertidos na Alemanha, conferindo especial atenção às dúvidas sobre a constitucionalidade da nova lei (VI.).

II. Considerações prévias sobre justificação de intervenções em direitos fundamentais

1. Antes de nos voltarmos à medida da infiltração online, é preciso assentar algumas premissas sobre os limites à atuação do Estado em um regime que conhece direitos fundamentais, tal qual o brasileiro. A Constituição Federal brasileira assegura aos indivíduos direitos fundamentais oponíveis contra todos os poderes do Estado – Executivo, Legislativo e Judiciário (cf., especialmente, o art. 5º CF). Isso significa, inquestionavelmente, que o Estado não pode tudo contra o indivíduo; há espaços em que, em princípio, o Estado não pode adentrar, e esses espaços chamam-se *direitos fundamentais*. Diante do imperativo jurídico de proteger os indivíduos e a sociedade e de promover os fins que lhe incumbem (por ex., art. 3º CF), o Estado pode ver-se forçado a adentrar nesses espaços individuais protegidos. Para tanto, ele necessitará de uma *justificação especial*.

Dessas ideias um tanto simples derivam os conceitos básicos da teoria dos direitos fundamentais que manejaremos no curso do presente artigo.[3] Esses conceitos, elaborados pelo constitucionalismo alemão, vêm aos poucos encontrando eco na doutrina brasileira.[4] O espaço demarcado por cada direito fundamental, aquele setor da vida objeto da proteção especial, chama-se *âmbito de proteção* do direito fundamental; aqui terá início a nossa análise. O comportamento estatal que impossibilita ou dificulta a prática de algo que se insere no âmbito de proteção é uma *intervenção* – a segunda etapa da análise. Toda intervenção estatal deve estar *justificada* – o que se examinará em terceiro lugar. Caso essa justificação

---

[3] Para um panorama desse "processo penal constitucional" alemão *Greco*, Introdução in: *Wolter*, O inviolável e o intocável no direito processual penal: reflexões sobre a dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal, São Paulo, 2018, p. 30 e ss.

[4] *Ferreira Mendes*, Limitações dos direitos fundamentais, in: Ferreira Mendes/Gonet Branco, Curso de Direito Constitucional, 12ª. ed., 2017, p. 190 e ss.; *Sarlet*, Teoria geral dos direitos fundamentais, in: Sarlet/Marinoni/Mitidiero, Curso de direito constitucional, 7ª. ed., 2018, p. 305 e ss. (385 e ss.); *Dimoulis/Martins,* Teoria Geral dos Direitos Fundamentais, 5ª. ed., 2014, p. 129 e ss.

não possa ser afirmada, qualifica-se a intervenção de *violação* ao direito fundamental. Violações são intervenções não justificadas, portanto ilícitas.

2. Detenhamo-nos a essa terceira etapa, a da *justificação*. Há, pelo menos, três pressupostos de relevância geral – ou seja, pertinentes a todos os direitos fundamentais – a serem respeitados: um, de natureza formal, é a existência de um fundamento legal; os outros dois, materiais, consistem em que a intervenção não afete o conteúdo essencial/de dignidade desses direitos e seja proporcional.

a) O limite formal, de que direitos fundamentais estão submetidos a uma *reserva de lei*, encontra-se constitucionalmente positivado (art. 5º II CF): "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei".[5] O Executivo e também o Judiciário precisam de um fundamento legal, que é o que os autoriza a agir contra os cidadãos. Porque, numa democracia, em que "todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente" (art. 1º parágrafo único CF), é apenas o povo quem pode autorizar, por meio de seu consentimento expressado através das leis votadas e aprovadas por seus representantes, o exercício do poder de intervir.

Aqui, parecem-nos relevantes cinco rápidas observações. Os direitos fundamentais protegem o cidadão não apenas do Executivo, das instâncias de persecução, mas também dos juízes; isso significa que, onde inexistir lei prevendo uma intervenção, é descabida a discussão se ela é possível mediante autorização judicial. A lei não regula intervenção, mas a *fundamenta, autoriza, torna juridicamente possível*.[6] Por isso também é descabido justificar intervenções no slogan de que não há direitos absolutos ou na proporcionalidade, dispensando uma lei; ainda que isso fosse correto,[7] não cabe intervenção sem lei que a autoriza. Além disso,

---

[5] Em detalhe sobre a reserva de lei e o que daí decorre para o processo penal, *Greco* (nota 3), p. 36 e ss.

[6] *Greco* (nota 3), p. 40.

[7] Pensamos que o direito de não ser torturado é absoluto (cf. *Greco*, As regras por trás da exceção: reflexões sobre a tortura nos chamados "casos de bomba-relógio", in: RBCC 78 [2009], p. 7 e ss.); assim também o é o direito de não ser escravizado. O slogan de que inexistem direitos absolutos implica em um questionamento da própria ideia de dignidade humana, fundamento também da ordem constitucional brasileira (art. 1º III CF). Sobre a dignidade humana no direito brasileiro, especialmente sobre a discussão em torno da

a lei deve ser precisa (*mandato de determinação*) – cláusulas gerais de autorização só permitem intervenções bagatelares –, com o que se torna inadmissível estender seu alcance a hipóteses não expressamente previstas (*proibição de analogia*). Por fim, observe-se que da mera competência para a realização de uma tarefa (como investigar, acusar ou julgar) não se pode derivar qualquer autorização para intervir em esferas protegidas (*distinção entre normas de competência entre e normas autorizitativas*).[8]

b) Um primeiro limite material é o de que a intervenção estatal não pode atingir o núcleo dos direitos fundamentais, o que tradicionalmente se chama de *conteúdo essencial* [Wesensgehalt] ou *de dignidade*.[9] Esse núcleo do direito fundamental é *intocável*; qualquer intervenção já implica em uma violação.[10] Essa ideia poderia ser exemplificada da seguinte forma: enquanto trancar alguém em uma cela de prisão representa uma intervenção justificável no direito fundamental à liberdade de locomoção (art. 5º XV CF), colocar essa pessoa em uma prisão perpétua impassível de ser revista afetaria a liberdade em seu âmago e, com isso, a dignidade humana.[11]

c) Por fim, o terceiro requisito geral de justificação de uma intervenção em direito fundamental é a *proporcionalidade*, uma barreira que os direitos fundamentais de defesa levantam também contra o próprio legislador, submetendo-o a *limites* na imposição de *limites* ao gozo dos direitos fundamentais ("limites dos limites").[12] A ideia da proporcionalidade é verificar, por meio de diferentes critérios, a harmonia entre o propósito (constitucionalmente legítimo) do legislador e o grau de afetação da esfera individual, em uma relação meio-fim. A intervenção tem de ser idônea, necessária e adequada para a promoção desse fim. É esse

---

possibilidade de relativizá-la, *Sarlet*, Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988, 10ª. ed. Porto Alegre, 2015, item 6.2 e ss.

8 *Greco* (nota 3), p. 37 e ss.

9 A rigor, estamos procedendo a uma simplificação: nem sempre se identifica conteúdo essencial e conteúdo de dignidade, cf. com referências *Greco* (nota 3), p. 35.

10 *Greco* (nota 3), p. 32.

11 *Greco* (nota 3), p. 35.

12 Cf., por todos, *Sarlet* (nota 4), p. 394 ss.

o nível mais complexo da operacionalização dogmática da justificação de intervenções em direitos fundamentais, já que aqui assumem relevância considerações das mais diversas ordens.

III. A infiltração online enquanto intervenção em direitos fundamentais da perspectiva do direito alemão

1. Desenvolvimento da infiltração online no direito alemão

A possibilidade da infiltração estatal, oculta e remota, em dispositivos informáticos para a investigação de crimes começou a ser discutida pelos tribunais alemães por volta de 2006. Em um primeiro momento, houve tentativas de utilização desse método oculto de investigação com base em aplicações extensivas ou mesmo analógicas de três normas do ordenamento jurídico alemão: aquelas que autorizavam a apreensão de objetos com finalidade investigativa (§ 94 Código de Processo Penal alemão – Strafprozessordnung, StPO), a de busca domiciliar (§ 102 StPO) e do monitoramento de telecomunicações (§ 100a StPO).

a) A decisão do Bundesgerichtshof de 2007 (BGHSt 51, 211)

Após os primeiros casos chegarem ao *Bundesgerichtshof* (tribunal alemão equivalente a nosso STJ, doravante BGH), a Corte, em 2007, entendeu não haver fundamento legal para a invasão de computadores, e que uma analogia tampouco seria possível.[13] Em síntese, estabeleceu-se, pela primeira vez, que o acesso aos dados armazenados no computador dos investigados seria uma severa intervenção ao direito fundamental à autodeterminação informacional – direito fundamental que o BVerfG já reconhecia desde 1983[14] – deduzido do direito ao livre desenvolvimento da personalidade e da dignidade humana (Art. 2 Abs. 1 c/c Art. 1 Abs. 1 Lei Fundamental, Grundgesetz – GG). A norma de autorização para

[13] BGHSt 51, 211.

[14] Cf. a decisão do censo, BVerfGE 65, 1; a respeito, em detalhe, *Greco* (nota 3), p. 41 e ss.

buscas domiciliares (§ 102 StPO) – um método de investigação físico, e não virtual – não autorizaria a medida, já que a busca em objetos físicos se baseia no princípio da publicidade: o investigado deve ser notificado e tem o direito de acompanhar a medida de busca em seu domicílio (§ 106 Abs. 1 Satz 2 StPO).[15] Tampouco as normas que autorizam intervenções ocultas alcançariam a medida.[16] A norma que autoriza o monitoramento de telecomunicações (§ 100a StPO) também não poderia ser aplicada ao caso: ainda que, durante a devassa nos dispositivos informáticos, possivelmente dados e procedimentos de telecomunicação sejam tangenciados, o objetivo central da medida seria a coleta abrangente de todas as informações armazenadas nos dispositivos, não necessariamente derivadas de telecomunicações.[17] De vigilância acústica domiciliar (§ 100c StPO) tampouco se trataria.[18] Por fim, a cláusula geral para investigações do Ministério Público e da Polícia (§ 161 StPO)[19] não abrangeria uma intervenção tão severa em direito fundamental.[20] O BGH também rechaça qualquer tentativa no sentido de fundamentar a medida combinando os elementos das várias normas, por violação da ideia de reserva de lei e do mandato de determinação.[21] E a publicação do julgado no repertório oficial conclui com uma frase a que a recepção brasileira da ideia de proporcionalidade deveria atentar: "O princípio da proporcionalidade limita, no caso concreto, as faculdades legalmente previstas, e não pode, portanto, substituir-se a um fundamento autorizativo que inexista."[22] *Não é a proporcionalidade, e sim a lei proporcional, que fundamenta intervenção em direito fundamental*.

Por isso, o tribunal afirmou que uma intervenção tão severa em direitos fundamentais de liberdade precisaria estar amparada por uma *norma autorizativa específica*, que, para ser constitucionalmente compatível, precisaria também se atentar aos severos pressupostos de intervenção

---

15 BGHSt 51, 211 (212 e ss., nm. 4 e ss.).

16 BGHSt 51, 211 (217 e ss., nm. 17 e ss.).

17 BGHSt 51, 211 (217 e ss., nm. 18).

18 BGHSt 51, 211 (218, nm. 19).

19 A respeito, *Greco* (nota 3), p. 39.

20 BGHSt 51, 211 (218, nm. 21).

21 BGHSt 51, 211 (219, nm. 22).

22 BGHSt 51, 211 (219, nm. 22).

exigidos pelo direito fundamental em questão. Ou seja, a medida carecia, até então, de *fundamento legal*.

b) A evolução posterior

Paralelamente à decisão do BGH, o estado alemão de Renânia do Norte-Vestfália inseriu, em sua Lei de Proteção à Constituição de 2006 [*Verfassungsschutzgesetz*] dispositivo que autorizaria a medida. A rigor, não se tratava aqui de processo penal, e sim de *direito dos serviços de inteligência*. No direito alemão, o Serviço de Proteção à Constituição realiza a atividade de inteligência estatal contra o extremismo político.[23] O direito de inteligência, cuja finalidade é a *coleta de informações* em momento prévio à existência de perigos, é um ramo autônomo, que não se confunde com o processo penal. Fala-se em um imperativo de separação [*Trennungsgebot*]: persecução e inteligência, direito processual penal (repressivo, fundado na suspeita) e o direito de inteligência (que se orienta pela precaução) não podem misturar-se, doutro modo, cair-se-ia na Gestapo.[24] A norma em questão não autorizava a infiltração online, portanto, com finalidade de busca de provas para o processo penal, mas para antecipar-se a crimes ainda não ocorridos.

Essa norma foi objeto, em 2008, da primeira decisão do BVerfG sobre a infiltração online.[25] Dentre outras coisas, a Corte declarou inconstitucional o dispositivo, criou um novo *direito fundamental à garantia da confiabilidade e integridade de sistemas informáticos*, derivando-o do direito geral de personalidade (Art. 2 Abs. 1 c/c Art. 1 Abs. 1 GG) e formulando os pressupostos materiais e procedimentais mínimos para a legitimidade da medida. Retornaremos a essa decisão fundamental logo em seguida (abaixo, 2.).

As exigências da corte serviram de base para a criação, em 2008, de norma autorizativa de infiltração online na Lei do Ofício Criminal

---

[23] Sobre o que segue *Greco* (nota 3), p. 51 e ss.

[24] O imperativo de separação separa também polícia preventiva e inteligência; o direito alemão conhece, assim, três níveis separados, o da polícia repressiva, o da polícia preventiva e o da inteligência.

[25] BVerfGE 120, 274.

Federal (Gesetz über das Bundeskriminalamt, BKA-Gesetz), uma lei de polícia preventiva, que não se aplica ao processo penal, de orientação repressiva.[26] Essa norma, então submetida a novo escrutínio da corte em 2016,[27] foi declarada parcialmente constitucional. Em 2017, o legislador criou norma autorizativa para a infiltração online como medida de investigação no processo penal (§ 100b StPO). A constitucionalidade dessa norma, por sua vez, encontra-se atualmente submetida a nova avaliação do BVerfG. Enquanto essa decisão é aguardada, as únicas considerações da corte sobre a infiltração online são aquelas relativas ao âmbito do direito de inteligência e do direito de polícia.

2. A infiltração online da perspectiva do BVerfG: o novo direito fundamental e suas exigências

a) A primeira conclusão alcançada pelo BVerfG na decisão sobre a Lei da Renânia do Norte-Vestfália foi a de que os direitos fundamentais dos Arts. 10 e 13 GG – que garantem proteção ao sigilo das telecomunicações e ao domicílio, respectivamente – não seriam aptos a proteger o indivíduo suficientemente contra o acesso a seus sistemas informáticos. O primeiro ponto de discussão localiza-se, portanto, no *âmbito de proteção* desses direitos fundamentais (sobre esse conceito, acima, II.). A pergunta é: o que protegem eles?

aa) O *Art. 10 GG*, na visão do BVerfG, protege a *telecomunicação* privada, garantindo a confiabilidade da comunicação entre indivíduos distantes entre si, em razão da maior vulnerabilidade a interceptações indevidas (especialmente, estatais).[28] O direito ao sigilo das telecomunicações, essencial para a proteção da privacidade, defende o indivíduo contra o levantamento não autorizado de informações e garante a privacidade à distância, de modo que comunicantes gozem do mesmo nível de privacidade que teriam em uma comunicação presencial. Por isso, ele protege, em última instância, o livre desenvolvimento da personalidade.[29]

---

[26] Cf. a nota 24.

[27] BVerfGE 141, 220.

[28] BVerfGE 120, 274 (306 e ss.).

[29] Cf. já BVerfGE 115, 166 (182).

A Corte entendeu, no entanto, que nem o acesso às informações nas mídias de armazenamento, nem o monitoramento da utilização de um sistema informático seriam intervenções à garantia de confiabilidade da telecomunicação do Art. 10 GG. E isso mesmo que a transferência dos dados obtidos nos dispositivos infiltrados até a central do investigador ocorresse por meio de sistemas de telecomunicação, como acontece com o acesso online em mídias de armazenamento de um computador alheio.[30]

bb) O *Art. 13 GG*, protetor da *inviolabilidade do domicílio*, garante ao indivíduo, com vistas à dignidade humana e ao interesse no desenvolvimento da personalidade, um espaço físico elementar de vida. O bem protegido desse direito fundamental é a esfera espacial na qual a vida privada se desenvolve.[31] Na visão do BVerfG, esse direito fundamental não seria pertinente, pois seu objeto de proteção seria uma componente espacial do âmbito privado, que não seria tangenciada, caso uma intervenção ocorresse fora do domicílio ou o local do dispositivo em questão (um laptop ou um smartphone) não fosse reconhecível durante a investigação. A utilização de uma conexão do dispositivo com a internet ou com um outro computador também não interferiria na esfera espacial da vida privada.[32]

cc) Por isso, o BVerfG entendeu que, para fazer frente aos especiais perigos ao livre desenvolvimento da personalidade na era digital, vinculados à utilização de computadores como dispositivos individuais ou como sistemas interconectados, seria necessário construir um *outro direito fundamental*, a ser derivado do direito geral de personalidade, por sua vez derivado de uma leitura conjunta do Art. 2 Abs. 1, que prevê o direito ao livre desenvolvimento da personalidade, e do Art. 1 Abs. 1 GG, que protege a dignidade humana.[33]

(1) Na ordem jurídica alemã, o *direito geral de personalidade* (Art. 2 Abs. 1 GG)[34] é um direito fundamental de alcance geral. Ele protege, na

---

30 BVerfGE 120, 274 (308).

31 Cf. já BVerfGE 89, 1 (12); 103, 142 (150 s.).

32 BVerfGE 120, 274 (309 e ss.).

33 BVerfGE 120, 274 (302 e ss.).

34 Art. 2 Abs. 1 GG: "... direito ao livre desenvolvimento da personalidade, desde que não se violem os direitos alheios, a ordem constitucional ou a lei moral".

visão do BVerfG, elementos da vida humana que não gozem de proteção expressa por outras liberdades constitucionais mas também sejam importantes para a garantia do livre desenvolvimento da personalidade.[35] Ou seja, trata-se de um direito de caráter subsidiário.

Segundo o BVerfG, as expressões do direito geral da personalidade até então desenvolvidas não seriam suficientes para proteger os usuários de sistemas informáticos. Em especial, o direito afetado não é *autodeterminação informacional*, porque não se trata apenas de proteger os dados privados dos usuários.[36] A classificação de dados como privados depende ainda, muitas vezes, do contexto nos quais os dados são descobertos e da relação que tenham com outros dados. Frequentemente, a infiltração do sistema, que nem sempre possibilita a coleta apenas de dados privados e atinge indiscriminadamente todos aqueles armazenados no dispositivo, não permite, de antemão, verificar o significado dos dados para o afetado e quais outras informações podem ser construídas ao relacionar esses dados entre si. Por isso, haveria o risco de formação de perfis da personalidade do indivíduo usuário do sistema. O acesso a esses sistemas pode alcançar dados potencialmente enormes e expressivos, mesmo antes da execução de medidas dirigidas ao levantamento de dados. Portanto, em relação à gravidade que representa para o direito à personalidade do afetado em relação ao levantamento de seus dados individuais, a proteção conferida pelo direito à autodeterminação não seria suficiente para proteger contra todos os riscos da infiltração online.

(2) Diante dessas conclusões, o BVerfG entendeu que o caráter subsidiário do direito geral à personalidade – com sua função de suprir lacunas na proteção ao livre desenvolvimento da personalidade do indivíduo – e a proteção da dignidade humana (Art. 2 Abs. 1 c/c Art. 1 Abs 1 GG) demandariam a direta *garantia da confiabilidade e integridade dos sistemas informáticos*, que as expressões até então derivadas desses direitos ainda não seriam capazes de prover. O Tribunal constrói, assim, um novo direito fundamental, com um âmbito de proteção próprio, para dar

[35] Cf. *Greco* (nota 3), p. 33 e s.

[36] BVerfGE 120, 274 (311 e ss.).

conta de novos setores em que a personalidade tem de poder livremente desenvolver-se e dos novos perigos que ali se põem.

b) O BVerfG também dedica algumas considerações sobre as *intervenções* nesse direito. Haverá uma intervenção caso os órgãos públicos acessem sistemas que, solitariamente ou em razão de conexões técnicas, possam conter dados pessoais do afetado em uma certa dimensão e variedade que revelem partes essenciais da forma de vida de uma pessoa ou uma imagem expressiva de sua personalidade.[37] Não apenas em relação ao uso privado do sistema informático, mas também ao uso comercial, é possível, em regra, a partir do comportamento do usuário, obter informações sobre características pessoais ou preferências. Ainda segundo a Corte, essa proteção do direito fundamental se estenderia também, por exemplo, a telefones móveis ou agendas eletrônicas, que dispõem de uma grande variedade de funções e podem abranger e armazenar dados pessoais de variada natureza. Esse direito protege o interesse do usuário de que os dados criados, processados e armazenados no dispositivo continuem privados. Além disso, o sistema estaria protegido contra a intervenção na sua integridade, afetada caso ele seja acessado de tal modo que seu desempenho, suas funções e seus conteúdos armazenados pudessem ser facilitados à utilização por terceiros. Esse direito protegeria, especialmente, contra intervenções ocultas.

c) Como o direito geral de personalidade não é garantido de forma absoluta, mas permite restrições de forma expressa,[38] o BVerfG se manifesta, por fim, sobre a *justificação* de restrições a esse direito.[39] A garantia de confiabilidade e integridade dos sistemas informáticos pode sofrer intervenções tanto com propósitos preventivos (direito de polícia) quanto repressivos, ou seja, para a persecução de crimes (direito processual penal). Intervenções, como vimos (acima, II.), precisam estar justificadas formal e materialmente. O mais interessante, no entanto, são as exigências constitucionais de proporcionalidade estabelecidas pela Corte para uma eventual norma autorizativa.

---

[37] BVerfGE 120, 274 (313 e ss.).

[38] Cf. a nota 34.

[39] BVerfGE 120, 274 (315 e ss.).

aa) Em primeiro lugar, exigiu-se que, tendo em vista a gravidade da intervenção no direito fundamental, ela só seria justificável em razão de perigos concretos para bens jurídicos *extremamente importantes* [*überragend wichtig*], que seriam o corpo, a vida, a liberdade e bens da coletividade que digam respeito aos fundamentos ou à subsistência do estado ou aos fundamentos da existência de seres humanos.[40]

bb) A corte também exigiu que esses perigos concretos estivessem *baseados em elementos fáticos*, que houvesse, ao menos, *uma probabilidade suficiente* de que os perigos concretos se realizassem, e que a medida só pudesse ser *autorizada por um juiz* (reserva de jurisdição).[41] No entanto, essas exigências – que visam impedir que a infiltração online se baseie em suspeitas difusas – já são comuns a muitas outras medidas de intervenção, inclusive muito menos graves que a infiltração online.[42]

cc) A conclusão mais importante do BVerfG, pertinente também a outras medidas de intervenção na personalidade, era a de que o *núcleo da esfera privada* [*Kernbereich privater Lebensgestaltung*] fosse protegido por precauções legais suficientes.[43] A Corte não viu aqui a necessidade de impor proibições gerais de levantamento de dados em determinados âmbitos. No entanto, impôs um mecanismo de proteção de dois níveis:[44] ao mesmo tempo que seria necessário, tecnicamente (por meio de softwares ou dispositivos de busca), tentar garantir que dados do núcleo da esfera privada não fossem levantados, caso tais mecanismos não fossem suficientes para impedir o levantamento destes dados, eles deveriam ser excluídos em uma segunda etapa. A ideia central do BVerfG é a de que, para o desenvolvimento livre da personalidade, é importante assegurar aos indivíduos que expressem sentimentos, reflexões, visões de mundo e experiências pessoais sem medo de estar sendo observados por órgãos estatais. Mesmo que o indivíduo tenha praticado crimes e possa ser investigado por eles, há condições mínimas que não lhe podem ser negadas.

---

40 BVerfGE 120, 274 (328).

41 BVerfGE 120, 274 (326, 328 e ss., 331 e ss.).

42 *Bär*, Comentário à decisão BVErfGE 120, 274, in: MMR 2008, p. 325 e ss. (326).

43 BVerfGE 120, 274 (335 e ss.).

44 *Bär*, MMR 2008, p. 326.

O *núcleo da esfera privada* é um conceito que surge da *teoria das esferas* de Hubmann para o direito civil.[45] Essa ideia pode ser melhor concretizada se imaginarmos três círculos concêntricos. O externo seria o da *esfera social* ou pública, que está sujeita a intervenções sem altos pressupostos de justificação, e é afetado por perguntas sobre a vida social ou pública, como a profissão, ou pequenas pesquisas online sobre o que é público a respeito do investigado. O intermediário seria o da *esfera privada* ou do sigilo, que exige maiores pressupostos de justificação e é afetado por coleta de informações, p.ex., sobre a rotina de uma pessoa, sobre suas compras e seu círculo de amigos. E, por fim, o círculo interno seria o *núcleo da esfera privada*, que não comportaria qualquer intervenção. Trata-se, portanto, do conteúdo essencial do direito à privacidade, sobre o qual falamos anteriormente (acima, II.), e é uma expressão da dignidade humana.[46] O que está contido nesse núcleo é controverso. A princípio, o BVerfG nega que uma informação pertença ao núcleo da vida privada, caso ela tenha alguma relação imediata com crimes. Essa parece ser a única conclusão atualmente alcançável, com certa segurança, a partir dos julgados da Corte. A proteção absoluta de diários já foi objeto de empate no BVerfG em 1989,[47] e o voto "vencedor" (em questão de empate não se declara a inconstitucionalidade) se baseava, principalmente, no fato de que os registros tratavam de crimes e no argumento de que quem faz uso da forma escrita, renuncia a um total controle sobre os conteúdos correspondentes.[48]

Embora essa decisão do BVerfG se refira a norma do direito de polícia, as balizas de legitimaçãoe para uma eventual norma autorizativa também parecem aplicar-se, naquilo que cabível, ao processo penal. O legislador alemão, tentando se orientar por essas diretrizes, autorizou, no Código de Processo Penal alemão (§ 100b StPO), o uso da infiltração online para a persecução de crimes.

---

45 *Greco* (nota 3), p. 34.

46 Cf. *Greco* (nota 3), p. 34.

47 BVerfGE 80, 367.

48 *Greco* (nota 3), p. 72.

IV. Observação intermediária da perspectiva brasileira

O exposto já nos coloca em posição de responder à primeira pergunta formulada no artigo, quanto à legitimidade abstrata da infiltração online, da perspectiva do direito processual penal brasileiro. Se levarmos a sério a ideia de reserva de lei insculpida no art. 5 II CF, basta verificar que inexiste dispositivo expresso que autorize a medida, para concluir que ela é *inadmissível entre nós*.

Seria necessário apenas esclarecer a razão específica pela qual ela precisa ser expressamente prevista, concretamente: *em qual dos direitos previstos no art. 5º CF ela intervém*? Trata-se de intervenção no âmbito de proteção do art. 5º X, que declara "invioláveis a intimidade, a vida privada ... das pessoas", ou do art. 5º XII, que também qualifica de "inviolável o sigilo ... de dados"? Ou há necessidade de recorrer a um novo direito fundamental não-escrito relativo à confiabilidade e integridade dos sistemas informáticos? Tendemos para essa última posição. Ainda que o conteúdo armazenado no computador se refira a aspectos da vida alheios à intimidade ou à vida privada, ou seja, se encontre fora do âmbito do art. 5º X CF, ele nos parece digno de proteção. Além disso, o "sigilo de dados" mencionado no art. 5º XII CF se refere a dados, não à própria máquina, que pode encontrar-se ainda vazia, por assim dizer, em estado virgem. Temos, assim, a impressão de que haja uma necessidade dogmática de recepcionar a figura do direito fundamental à *confiabilidade e integridade dos sistemas informáticos*, extensão a que a própria CF expressamente se abre (art. 5º § 2º CF: "Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados...").

Se quisermos dotar as nossas instâncias persecutórias de uma faculdade de intervir nesse direito, precisaremos, assim, de *lei específica que a fundamente* (e não apenas a regule). Enquanto inexistir essa lei, o acesso ao conteúdo de sistemas informáticos terá de ocorrer através das medidas da busca e da apreensão do dispositivo físico em que esse conteúdo se encontra armazenado. O legislador não estará livre para dotar essa lei do conteúdo que queira, mas terá de atender a exigências constitucionais que, se não necessariamente coincidem com as que acabamos de expor, que o BVerfG formulou para a Alemanha (acima, III.

2.), deveriam ao menos delas tomar conhecimento. Também por isso, parece-nos interessante observar como o legislador processual penal alemão atendeu a essas exigências por meio do novo dispositivo sobre a medida, introduzido em 2017. É a isso que agora nos voltamos.

V. A infiltração online no processo penal da perspectiva do legislador alemão: o novo § 100b StPO

Em julho de 2017, com a intenção de melhorar a efetividade e praticabilidade do processo penal na Alemanha,[49] o legislador inseriu no Código de Processo Penal alemão, dentre outras normas, a do § 100b, que autoriza a infiltração online com base nas exigências estabelecidas, até então, pelo BVerfG. Passemos em rápida revista seus principais pressupostos de aplicação (1.) e os mecanismos legais de proteção do indivíduo durante a execução da medida (2.).

1. Os principais pressupostos autorizadores da infiltração online nos termos do § 100b StPO

a) A suspeita do fato

Em primeiro lugar, a medida só pode ser autorizada diante da suspeita do fato. As normas processuais penais alemãs fazem referência a três tipos de suspeitas, para distintas fases processuais: a suspeita inicial [*Anfangsverdacht*], a suspeita forte [*dringender Verdacht*] e a suspeita suficiente [*hinreichender Verdacht*]. [50] Enquanto a *suspeita forte* é afirmada nos casos em que, segundo o estado atual da investigação, haja grande

[49] Críticos a esse mote da reforma *Schünemann*, Legitimation durch Verfahren?, StraFo 2015, p. 177 e ss. (186 e ss.); *Greco*, Fortgeleiteter Schmerz – Überlegungen zum Verhältnis von Prozessabsprache, Wahrheitsermittlung und Prozessstruktur, in: GA 2016, p. 1 e ss. (14). Para críticas sobre o procedimento legislativo para a introdução da norma no Código de Processo Penal alemão, *Beukelmann*, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017, 440.

[50] Ver *Greco* (nota 3), p. 59; e *Gleizer*, in: Hilgendorf/Valerius, Direito Penal: Parte Geral, São Paulo, 2018, p. 153, nota de tradutor.

probabilidade de que o imputado tenha praticado o crime, a *suspeita suficiente* é afirmada quando o imputado tem mais chance de, em vista das provas colhidas, ser condenado do que absolvido. Mas isso não significa que esta esteja abrangida por aquela, já que a suspeita suficiente é verificada sempre ao término dos procedimentos investigatórios, enquanto a suspeita forte se baseia no estado atual da investigação, que pode vir a ser alterado. A suspeita inicial corresponde à nossa *notitia criminis*, uma vez que impõe a instauração de uma investigação preliminar; a suspeita suficiente, à nossa justa causa, impondo a propositura da denúncia. A suspeita forte autoriza, principalmente, a prisão preventiva (ao lado de outros pressupostos, como a fuga ou o perigo de fuga).

Em que pese o legislador não ter estabelecido expressamente o nível da suspeita apta a fundamentar a autorização de infiltração online (§ 100b Abs. 1 Nr. 1 StPO: "fatos determinados fundamentem a suspeita"), o BVerfG entende, em relação à escuta ambiental (§ 100c StPO), que a suspeita precisa ser maior do que uma mera suspeita inicial.[51] O BGH[52] parece ser menos exigente: ele afirma a desnecessidade de uma suspeita forte ou suficiente, e contenta-se com o que ele chama de suspeita *simples* [*einfacher Verdacht*], categoria desenvolvida pela jurisprudência, cuja relação com a tripartição tradicional ainda não foi de todo esclarecida.

O que está claro é que não bastam meros boatos, desconfianças e suposições não verificadas; tampouco bastam suposições especulativas, relativas ao pertencimento a um grupo ou mesmo à experiência criminalística dos investigadores, mas sem base no caso concreto. É necessário que, em razão de circunstâncias relacionadas ao caso, a partir de depoimentos de testemunhas, observações ou outros indícios fáticos, haja indicação, em grau significante, do cometimento de um crime do catálogo de fatos, ou seja, é exigida uma *base fática sólida*, apoiada em circunstâncias concretas

---

[51] BVerfGE 109, 279 (350); *Wolter/Greco*, in: *Wolter* (coord.), Systematischer Kommentar zur Strafprozessordnung (= SK-StPO), vol. 2, 5a. ed., Köln, 2016, § 100a nm. 43.

[52] BGH NStZ 2010, 711; BeckRS 2016, 15673. Nessas decisões, o BGH analisa o grau de suspeita necessário para a medida de monitoramento de telecomunicações (§ 100a StPO).

e de certa extensão.[53] Está claro que a suspeita é sempre uma prognose, a realizar-se no momento da autorização da medida; não é possível, assim, fundamentação retrospectiva, por meio de informações eventualmente obtidas após a autorização da medida.[54]

b) O catálogo de fatos

A medida só pode ser autorizada para a investigação dos crimes previstos no catálogo de fatos da norma autorizativa. Esse pressuposto tem seu fundamento não apenas no princípio da proporcionalidade, que exige a imposição de um rol de crimes especialmente graves, como também na exigência de reserva de lei, no sentido de que a lei tem de fixar os precisos limites da medida.

Ao concretizar o novo direito fundamental à confiabilidade e integridade de sistemas informáticos, o BVerfG estabeleceu, como visto (acima, III. 2. c] aa]), que o emprego da infiltração online só seria justificável em razão de perigos concretos para bens jurídicos *extremamente importantes*, que seriam o corpo, a vida, a liberdade e outros bens importantes para a coletividade, cuja ameaça colocaria em risco as bases ou a existência do estado de direito ou as bases da existência dos seres humanos.[55] Por exigência do BVerfG,[56] o legislador estabeleceu um catálogo de crimes especialmente graves como pressuposto para a infiltração online. Consequentemente, o legislador criou um catálogo único de crimes para a infiltração online (§ 100b Abs. 2 StPO) e para a escuta ambiental (§ 100c Abs. 1 Nr. 1 StPO), medidas mais invasivas à privacidade do que o monitoramento de telecomunicações (§ 100a StPO), cujo catálogo prevê crimes (meramente) graves.

---

[53] BVerfGE 100, 313 (395); BVerfG NStZ 2003, 441 (443); BGH NStZ 2010, 711; *Wolter/Greco*, SK-StPO, § 100a nm. 43; *Graf*, in: Graf (coord.), Beck'scher Online-Kommentar Strafprozessordnung (= BeckOK StPO), 33ª. ed., 1.4.2019, § 100b nm. 12.

[54] *Graf*, BeckOK StPO, § 100b nm. 12, 13.

[55] BVerfGE 120, 274 (328).

[56] BVerfGE 10, 274 (334).

c) A gravidade no caso concreto

Ao criar a norma autorizativa, o legislador ainda se preocupou em positivar um firme posicionamento da jurisprudência constitucional,[57] estabelecendo a necessidade de que a medida esteja baseada não só na gravidade abstrata do crimes, ou seja, no fato dele constar do *catálogo de crimes* especialmente graves, mas também em sua *gravidade concreta* (§ 100b Abs. 1 Nr. 2 StPO: "... o fato é de especial gravidade também no caso concreto"), que deve estar refletida nas específicas circunstâncias em que ele tenha ocorrido.[58] Pode-se dizer que, enquanto a exigência de gravidade abstrata é a concretização da ideia de proporcionalidade que o direito fundamental impõe ao legislador, a exigência de demonstração da gravidade concreta é o seu efeito em relação ao juiz. Como exemplo de gravidade concreta, pode-se mencionar uma grande vantagem em um crime de corrupção ou os efeitos de um crime para a vítima,[59] ou o cometimento de simultâneo de vários fatos integrantes do catálogo,[60] ou o cometimento a partir de uma estrutura organizada.[61]

d) A subsidiariedade

A infiltração online também só pode ser autorizada caso a investigação dos fatos ou do local onde se encontre o afetado, seja, "de outro modo, impossibilitada ou fundamentalmente dificultada" (§ 100b Abs. 1 Nr. 3 StPO). A ideia é afastar a possibilidade de que se lance mão, diretamente, de medidas muitos invasivas quando outras menos invasivas são possíveis. Entre essas medidas encontram-se, principalmente, a busca e a apreensão.[62] A medida pressupõe, assim, um estado de necessidade probatório.[63]

---

[57] BVerfGE 109, 279 (345 e s.).

[58] *Soiné*, NStZ 2018, p. 498 s.

[59] *Graf*, BeckOK StPO, § 100b nm. 15.

[60] *Bruns*, in: Hannich (coord.), Karlsruher Kommentar zur Strafprozessordnung, 8a. ed., München, 2019 (= KK-StPO), § 100b nm. 8.

[61] *Bruns*, KK-StPO, § 100b nm. 8.

[62] Cf. a fundamentação oficial da lei, Bundestag-Drucksache 18/12785, p. 55; *Bruns*, KK-StPO, § 100b nm. 9.

[63] Sobre esse conceito *Greco* (nota 3), p. 61.

Em síntese, costuma-se afirmar que outras medidas *impossibilitam* a investigação [a tornam *aussichtlos*], caso não existam outros meios de encontrar a informação pretendida ou os meios existentes não apresentem perspectiva de mesmo resultado qualitativo. Já o critério de *dificuldade fundamentalmente maior* pode ser afirmado diante de um possível atraso temporal da investigação ou do fato de que medidas alternativas poderiam encontrar apenas informações piores ou não obter as informações adequadas e suficientes para uma investigação mais rápida e eficiente.[64] Altos custos de medidas alternativas também podem justificar a subsidiariedade, desde que eles se mostrem indefensáveis segundo um juízo de proporcionalidade, que leve em conta a gravidade da intervenção.[65] No entanto, deve-se lembrar que a infiltração online também é uma medida de alto custo financeiro.[66]

e) A proporcionalidade em sentido estrito

As considerações de proporcionalidade exigem que não apenas o legislador, mas também o aplicador da lei verifique, antes e durante a execução da medida, se a intervenção é proporcional em relação aos resultados esperados ou à culpabilidade do afetado.[67] Aqui, cabem considerações de muitas ordens, como, por exemplo, a possibilidade de obter muito mais informações não vinculadas ao caso do que o contrário, ou uma grande distância temporal entre a execução do fato e a aplicação da medida, que sugira que o afetado não possua mais as provas do fato em seu dispositivo informático.[68]

f) Os possíveis afetados pela medida

De regra, a medida só pode ser dirigida contra o investigado (§ 100b Abs. 3 S. 1 StPO). No entanto, a medida também pode ser autorizada

---

64 *Graf*, BeckOK StPO, § 100b nm. 16.

65 *Graf*, BeckOK StPO, § 100b nm. 16.

66 *Graf*, BeckOK StPO, § 100b nm. 6.

67 *Graf*, BeckOK StPO, § 100b nm. 20.

68 *Graf*, BeckOK StPO, § 100b nm. 20.

caso seja de se esperar que, inevitavelmente, também venham a ser obtidas informações relacionadas a terceiros não-implicados (§ 100b Abs. 3 S. 2 StPO).[69] Essa é, na realidade, a regra em relação a tais medidas, já que sistemas informáticos contemporâneos dificilmente contêm informações relacionadas apenas ao usuário principal.

Sistemas informáticos de terceiros também podem ser objeto da medida caso sejam utilizados pelo investigado (mesmo sem a anuência do terceiro),[70] mas isso somente se a execução da medida apenas contra o investigado não for suficiente para a elucidação dos fatos ou da localização de um co-investigado.[71] Exemplos de terceiros afetados são familiares, amigos, vizinhos, e mesmo a vítima do crime.[72] Um outro exemplo de sistema informático de terceiros são os espaços de armazenamento em nuvem [*cloud-computing*], que pertencem, em regra, a empresas privadas.[73] A infiltração online de nuvens também levanta questões de cooperação jurídica internacional, tendo em vista que estes sistemas privados estão, em sua maioria, alocados fisicamente em diferentes países.[74]

2. Mecanismos de proteção do indivíduo durante a execução da infiltração online

Além dos pressupostos estabelecidos para a execução da medida, o legislador alemão também estabeleceu regras para a proteção do indivíduo durante a execução da infiltração online no processo penal.

---

[69] Sobre as diversas categorias de terceiros no processo penal alemão *Greco* (nota 3), p 62.

[70] *Graf*, BeckOK StPO, § 100b nm. 23; *Blechschmitt*, Quellen-TKÜ und Online--Durchsuchung, StraFo 2017, p. 361 e ss. (364); *Soiné*, Die strafprozessuale Online-Durchsuchung, NStZ 2018, p. 497 e ss. (499).

[71] *Graf*, BeckOK StPO, § 100b nm. 23.

[72] *Soiné*, NStZ 2018, 499 (499).

[73] Especificamente sobre o acesso a dados armazenados em nuvens, cf. a monografia de *Grözinger*, Die Überwachung von Cloud-Storage, Baden-Baden, 2018. Cf. também *Soiné,* NStZ 2018, 499 (500).

[74] Cf., por todos, *Soiné* NStZ 2018, 499 (500), com outras referências.

a) As cautelas técnicas e os protocolos do procedimento

Em razão da intervenção na integridade do sistema informático, são exigidas cautelas técnicas, com a finalidade de reduzir a intervenção ao mínimo possível e impedir o acesso desautorizado de terceiros por meio dos mecanismos utilizados pelo investigador. Desde o início, as manipulações necessárias para a execução da infiltração online devem ser praticadas com mecanismos que desfaçam de forma automática os efeitos da medida tão logo ela deixe de vigorar (§ 100b Abs. 4 StPO c/c § 100a Abs. 5 S 1 Nr. 3 StPO).

Além disso, e mais importante, por razões de proteção de dados, é o dever de tomar todas as precauções técnicas possíveis para impedir alteração, eliminação e conhecimento desautorizado dos dados copiados por parte de terceiros (§ 100b Abs. 4 StPO c/c § 100a Abs. 5 S. 2, 3). Isso significa que o local de armazenamento dos dados copiados, por exemplo, deve ser protegido, por mecanismos de segurança, tanto físicos quanto virtuais, contra acesso, por exemplo, de funcionários da repartição não autorizados à investigação e de particulares.

Para a proteção efetiva do direito fundamental do afetado e da validade das provas obtidas, o legislador ainda exige (§ 100b Abs. 4 StPO c/c § 100a Abs. 6 StPO) o registro de informações como a qualificação do meio técnico utilizado e o momento de sua utilização, a identificação do sistema informático e as alterações realizadas que não sejam simplesmente transitórias, os dados levantados e o departamento que executa a medida. Essas informações têm o condão de possibilitar a posterior verificação da proporcionalidade da medida durante a execução, a forma e a abrangência da intervenção, a obediência aos limites temporais, a tomada de todas as cautelas técnicas, a atribuição de responsabilidade e a qualificação das testemunhas da execução da medida.

Há quem afirme que esse dever de atender a cautelas técnicas fundamente quase que uma posição de garante daqueles que executam a infiltração.[75] Essas considerações concretizam a ideia de que poderes vêm com responsabilidades. Para a proteção efetiva do direito fundamental do afetado e da validade das provas obtidas, o legislador ainda exige o

[75] *Graf*, BeckOK StPO, § 100b nm. 29.

registro de informações relativas à execução da medida, a fim de possibilitar o controle posterior da custódia da prova e da responsabilidade dos agentes envolvidos em sua produção. Esses registros são chamados de protocolos do procedimento.

b) Proteção do núcleo de privacidade

Em relação à proteção dos espaços absolutos da vida do indivíduo (o conteúdo essencial dos direitos fundamentais), o legislador estabeleceu a *inadmissibilidade* da infiltração online (§ 100d Abs. 1 StPO) em situações nas quais se possa supor, com base em elementos fáticos, que a execução da medida venha a obter *apenas* informações do núcleo da esfera privada. O critério *apenas* é merecedor de muitas críticas da ciência.[76] Afirmam alguns, entre os quais o primeiro autor do presente que artigo, que seria praticamente impossível concluir a priori que outras informações, não pertencentes ao núcleo da esfera privada, não possam ser também obtidas mesmo nos mais íntimos espaços do indivíduo, essa regra não teria qualquer aptidão para proteger aquilo que justamente deve ser objeto de máxima proteção. A lógica deveria ser inversa. A legislação deveria proibir a execução da medida, caso, segundo elementos fáticos, sua execução ameaçasse a obtenção *também* de informações do núcleo da esfera privada, ainda que outras pertinentes ao caso pudessem ser obtidas. Essa ideia já foi concretizada pelo BVerfG em relação ao monitoramento de e-mails, quando a Corte, por interpretação redutiva conforme à constituição, vedou o acesso a telecomunicações caso algum conteúdo do núcleo da esfera privadas pudesse ser alcançado.[77]

Especificamente em relação à infiltração online, criou-se também a exigência de que, desde que possível, se assegure, com meios técnicos, que não sejam obtidos dados do núcleo da esfera privada (§ 100d Abs. 3 StPO). E que, na ocasião em que tais dados, apesar das precauções técnicas tomadas, porventura venham a ser obtidos, eles devem ser imediatamente eliminados ou submetidos ao juízo para apreciação sobre a possibilidade

---

[76] Cf., com outras referências, *Wolter/Greco*, SK-StPO, § 100a nm. 57 e ss..

[77] BVerfGE 124, 43 (69 s.). Cf. também *Wolter/Greco*, SK-StPO, § 100a nm. 57, com outras referências.

de serem valorados ou a necessidade de serem eliminados. Diferente de outras precauções, estabelecidas conjuntamente para o monitoramento de telecomunicações, a escuta ambiental e a infiltração online, aqui o legislador cria uma precaução aplicável apenas a esta última. Isso pode indicar que, em sua visão, diferente das demais medidas, a infiltração online permite alguma distinção prévia da natureza das informações por não servir à vigilância concomitante das atividades do investigado em seus sistemas informáticos, senão apenas à busca por arquivos já armazenados (abaixo, IV.).

c) Proteção dos portadores de um direito de recusa a testemunhar

Em relação à proteção do direito a não testemunhar contra o investigado (§ 100d Abs. 5 S. 1 StPO), a infiltração online é inadmissível para a produção de provas relacionadas a pessoas autorizadas a negar testemunho contra o investigado em razão da *profissão* (§ 53 StPO). Se, durante ou após a execução das medidas, passar a existir uma situação que autoriza a recusa a testemunhar, as informações obtidas não apenas não poderão ser valoradas, como deverão ser eliminadas imediatamente; nesse caso, a obtenção das informações e sua eliminação deverão ser documentadas (§ 100d Abs. 5 S. 2 c/c § 100d Abs. 2, S. 2 e 3 StPO). Em relação a pessoas autorizadas a negar testemunho em razão de *parentesco* (§ 52 StPO), as informações obtidas por meio da infiltração online só podem ser valoradas, caso o significado da relação de confiança não seja desproporcional ao interesse na investigação dos fatos ou da localização de um investigado (§ 100d Abs. 5 S. 2 StPO).

O direito de negar testemunho enquanto direito fundamental processual é entendido como consequência da ideia de proteção dos direitos fundamentais. Portanto, o legislador também estabeleceu proteção aos portadores desse direito, não permitindo que a infiltração online o viole. O que se pretende com essas regras é evitar a circunvenção do direito de não testemunhar contra o investigado, ou seja, que, diante da impossibilidade de se obrigar alguém a testemunhar, se permita obter as informações, por via transversa, de maneira oculta. Os advogados de defesa do investigado, diferente de todas as outras pessoas autorizadas a negar

testemunho, gozam do que se chama de *dupla proteção*.[78] As informações que eles trocam com o investigado não podem ser obtidas, em primeiro lugar, por uma garantia individual de que este não seja degradado a objeto do processo, mas também pela proteção público-institucional da relação de confiança essencial para o processo.

d) A proteção dos dados coletados: os imperativos de identificação, de notificação e de eliminação

Por fim, em razão da necessidade de proteção dos dados pessoais obtidos por meio de intervenção na esfera de privacidade do investigado, o legislador também estabeleceu uma série de cautelas adicionais, que valem para todas as medidas secretas.

Em primeiro lugar, os dados pessoais obtidos com a execução da medida devem ser *identificados* como tais, e se forem transferidos a outra instituição do Estado, a estas caberá manter a identificação (§ 101 Abs. 3 StPO).

Além disso, a fim de permitir àquele que teve o próprio âmbito de proteção afetado que submeta a medida a um controle judicial posterior, a lei também cria o dever de que o Estado, em regra, o *notifique* sobre a afetação (§ 101 Abs. 4 StPO). Essa regra é excepcionada em razão de interesses preponderantes de um terceiro (Abs. 4 S. 3). O imperativo de notificação surge no momento em que não houver riscos aos propósitos da investigação, à vida, à integridade física e à liberdade pessoal de uma pessoa; e o atraso da notificação superior a seis meses a partir do encerramento da medida é carente de autorização judicial (Abs. 6 S. 5).

Por fim, quando dados pessoais obtidos não forem mais necessários para a persecução penal ou para um eventual controle judicial da medida, eles devem ser imediatamente *eliminados* (§ 100d Abs. 8 StPO). A eliminação deve ser certificada nos autos (Abs. 8 S. 2) e, caso os dados sejam mantidos apenas para uma eventual verificação judicial da medida, eles não podem ser utilizados para nenhum outro propósito sem o consentimento do afetado, devendo ser acautelados de forma apropriada (Abs. 8 S. 3). O imperativo de eliminação dos dados tem por finalidade

[78] *Wolter/Greco*, SK-StPO, § 100a nm. 56.

reduzir a possibilidade de acesso a informações pessoais não (ou não mais) necessárias para a prova processual, zelando pela manutenção da proporcionalidade da medida de infiltração online.

VI. Questões especiais da infiltração online

Além dos ordinários problemas interventivos da infiltração em sistemas informáticos e da busca por informações relevantes para um processo penal, ainda há três outras questões que, em nosso entender, também merecem atenção.

1. A vigilância online

Alguns dispositivos informáticos presentes em nosso dia a dia possibilitam, tecnicamente, mais do que uma simples descoberta de informações armazenadas em suas memórias. O acesso remoto a celulares (ou até a uma Smart-TV)[79] permite, por exemplo, a observação simultânea de fatos contemporâneos, por meio da ativação de seus sistemas sensoriais, como microfone e câmera, sem o conhecimento do usuário afetado (vigilância online).[80] Como os celulares são objetos que nos acompanham de perto, do banheiro à beirada da cama, o acesso a esses dispositivos permite não apenas o encontro de informações armazenadas, por exemplo, na caixa de e-mails ou em conversa privada em um aplicativo de mensagens instantâneas, como também acesso ao áudio e vídeo de uma relação sexual, de uma discussão íntima e do diálogo com o médico ou com o advogado de defesa. Por meio de uma vigilância online é possível comprometer não apenas a proteção eficiente do núcleo da esfera privada, como também a própria confiança no uso de dispositivos informáticos, que se transformam em objetos de escuta e gravação ambiental.

Parece-nos que a medida não encontra fundamento legal no direito alemão, de modo que ela é impossível de *lege lata*. Isso vale com

---

[79] *Záboji*, „Unheimliche Bilder“, in: Frankfurter Allgemeine Zeitung, publicado em 8.6.2016, acessível em: http://bit.ly/2LZUCKM.

[80] Cf. *Soiné* NStZ 2018, 499 (502).

ainda maior razão para o Brasil. *Não se trata de uma infiltração online*, nos termos do § 100b StPO. A medida legalmente prevista permite um acesso à memória do dispositivo infiltrado, de forma que dele se extraiam informações já ali contidas. A vigilância online transforma o aparelho em câmera ou escuta, que produz novas informações.

Esse caráter produtivo da medida a aproxima da *vigilância acústica domiciliar*, autorizada, na Alemanha, pelo § 100c StPO, e mencionada no Brasil pelo art. 3º II Lei 12.850/2013 para investigação de organizações criminosas.[81] Parece-nos, entretanto, que *tampouco* esses dispositivos dão conta da medida. A vigilância acústica domiciliar distingue-se da vigilância online pelo fato de esta, em virtude da maior confiança que conferimos a nossos dispositivos pessoais, ampliar nossa exposição e vulnerabilidade e, além disso, utilizar-se de meios técnicos que nos pertencem, manipulando-os e, com isso, afetando também a integridade dos dispositivos informáticos privados. Os sistemas informáticos utilizados para uma vigilância online não são meios técnicos à disposição e de propriedade dos órgãos de persecução penal, mas dos afetados pela medida. Se trouxermos para casa um mero utensílio doméstico, como uma televisão com acesso à internet, estaremos, em última instância, trazendo um espião ao lar. Por se tratar de uma intervenção de qualidade distinta, seria necessário que estivesse autorizada expressamente como forma de execução da escuta ambiental.[82]

2. Métodos técnicos de infiltração online e problemas

Além da infiltração ordinária – com superação técnica dos obstáculos de segurança do dispositivo informático, por exemplo, por meio da obtenção das senhas do sistema – há, a princípio, outras três possibilidades técnicas de infiltração a dispositivos informáticos: por meio de a) acesso físico ao dispositivo para a instalação de malwares, b) colaboração

---

[81] Ocorre que a medida é ali apenas mencionada; não há dispositivo que a preveja em seus pressupostos, de forma que, a nosso ver, falta uma base legal também para essa medida no direito brasileiro, cf. já *Greco* (nota 3), p. 40.

[82] Cf. *Rüscher*, Alexa, Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden?, NStZ 2018, p. 687 e ss.

do afetado para a instalação de malwares no seu próprio dispositivo e c) lacunas de segurança existentes em algum software do dispositivo. Cada um desses três métodos levanta diferentes questões jurídicas, havendo quem os considere de todo ilegítimos.[83]

3. Inconstitucionalidade do § 100b StPO?

Como já demos notícia (acima, III.1.), a constitucionalidade da norma autorizativa para a infiltração online como medida de investigação no processo penal (§ 100b StPO) está atualmente submetida, por reclamação constitucional, à avaliação do BVerfG. Por razões de espaço, nós não discutiremos cada uma das alegadas inconstitucionalidades, mas nos limitaremos apenas a noticiar, dentre todas, três que entendemos mais importantes.[84]

Em primeiro lugar, a constitucionalidade da infiltração online é questionada em razão da amplitude do catálogo de fatos. Em sua decisão de 2008,[85] o BVerfG estabeleceu que o emprego da infiltração online só seria justificável em razão de perigos concretos para bens jurídicos *extremamente importantes*, que seriam o corpo, a vida, a liberdade e outros bens importantes para a coletividade, cuja ameaça colocaria em risco as bases ou a subsistência do estado de direito ou as bases da existência dos seres humanos. Do extenso catálogo de fatos constam, no entanto, crimes que, na visão dos reclamantes, não protegem tais bens jurídicos: entre outros, a falsificação de moeda, a lavagem de dinheiro, a corrupção e a receptação.

---

[83] Nesse sentido *Derin/Golla*, Der Staat als Manipulant und Saboteur der IT-Sicherheit, in: NJW 2019, 1111 ss. (1112 ss.). Ver também, com outra posição, *Soiné* NStZ 2018, 499 (500 ss.); *Bruns*, KK-StPO, § 100b nm. 6.

[84] Para as demais, cf. a síntese da Reclamação Constitucional, no site do partido político *Freie Demokratische Partei* (FDP) ajuizador da ação, em: https://www.fdp.de/sites/default/files/uploads/2018/08/20/fdp-vfb-gazeas-zusammenfassung.pdf. Conferir, também, a entrevista com o advogado do Reclamante, Nikolaos Gazeas, em: https://www.lto.de/recht/hintergruende/h/verfassungsbeschwerde-staatstrojaner-fdp-anwalt-interview-online-durchsuchung/.

[85] BVerfGE 120, 274.

Outra alegação de inconstitucionalidade se refere a uma proteção ineficiente do núcleo da esfera privada. Além do fato de a norma não prever uma proibição absoluta de levantamento de determinados dados, limitando-se a simplesmente proibir uma ulterior valoração dos mesmos (§ 100d Abs. 2 StPO), o legislador também não teria estabelecido a necessidade de que o magistrado fizesse juízo sobre o pertencimento ou não de uma informação ao núcleo da esfera privada antes que os órgãos de persecução penal tivessem acesso a ela.

Por fim, também se aponta inconstitucionalidade na desproporcional ausência de norma que garanta a mesma proteção dos profissionais dispensados do testemunho aos seus auxiliares, de forma que não se possa, por via transversa – acessando, por exemplo, os dispositivos informáticos da secretária do advogado –, esvaziar as garantias do sigilo profissional.

VII. Conclusão

Em síntese, podemos dizer que a infiltração online, como meio processual-penal de obtenção oculta e remota de provas armazenadas em sistemas informáticos é uma medida cada vez mais atraente na era da digitalização, em que informações necessárias ao processo estão, muitas vezes, apenas registradas em formato de dígitos 0-1, e não mais em papéis apreensíveis por meio de medidas convencionais, como a busca e apreensão. Em ordenamentos jurídicos que conhecem direitos fundamentais, ela é, no entanto, certamente uma intervenção. Em qual(is) direito(s) fundamental(is) ela intervém é a primeira pergunta a ser respondida. A resposta a essa pergunta pode nos levar, como na experiência alemã, a reconhecer a necessidade um específico direito fundamental que proteja os indivíduos dos riscos que a vida cercada de dispositivos informáticos pode lhes criar. A concretização de um direito à integridade e confiabilidade no uso de dispositivos informáticos parece ser uma boa resposta, dada pelo BVerfG, ao problema: um direito que proteja não apenas contra invasões à privacidade, mas também contra manipulações em sistemas informáticos privados, de modo que os indivíduos possam confiar em seu uso e, assim, desenvolver livremente suas personalidades na era da digitalização.

Um direito fundamental à integridade e confiabilidade no uso de sistemas informáticos deve criar altos obstáculos interventivos, tendo em vista as sérias consequências que uma intervenção pode criar para a vida dos indivíduos que tenham seus sistemas informáticos acessados por terceiros, especialmente agentes estatais. Esses pressupostos estão sendo discutidos há algum tempo pela ciência e pelos tribunais alemães e podem servir de parâmetro para a elaboração de uma norma autorizativa ainda inexistente no direito brasileiro. Na ausência de norma autorizativa para a infiltração online no ordenamento jurídico brasileiro, a ilegitimidade da medida é evidente. O Estado só pode atuar nos limites das autorizações do povo, conferidas por seus representantes no parlamento.

Como essa autorização inexiste no Brasil, é vedado às instâncias de persecução infiltrar-se em computadores de forma oculta. No Brasil, o acesso ao conteúdo de sistemas informáticos tem de fazer uso da busca e da apreensão do dispositivo físico em que esse conteúdo se encontra armazenado.

Apêndice:

§ 100b Infiltração online:

(1) Sem o conhecimento do afetado [ocultamente], pode-se, com meios técnicos, intervir em seu sistema informático e levantar dados que ali se encontrem, caso

1. fatos concretos fundamentem a suspeita de que alguém consumou ou, caso a tentativa seja punida, tentou consumar como autor ou partícipe, um crime especialmente grave, listado no rol da Abs. 2.,

2. o crime seja especialmente grave também no caso concreto

3. a investigação dos fatos ou do local onde se encontra o acusado, fosse, de outro modo, consideravelmente mais difícil ou infrutífera.

(2) Crimes especialmente graves no sentido da Abs. 1 Nr. 1 são:

1. do Código Penal:

a) crimes de alta traição e de perigo para o estado de democrático de direito... b) constituição de organizações criminosas ... e terroristas ... c) falsificação de moedas ... d) crimes sexuais ... e) pornografia infantil... f) homicídio e homicídio qualificado... g) crimes contra a liberdade pessoal (tráfico de pessoas... prostituição compulsória... escravidão... h) furto em bando... i) roubo grave e roubo com resultado morte... j) extorsão... k) crimes de receptação... l) casos especialmente graves de lavagem de dinheiro, ocultação de valores patrimoniais auferidos ilicitamente... m) casos especialmente graves de corrupção com ou sem infração de dever...

2. da lei de asilo: (...) a...b...

3. da lei de domicílio: a...b...

4. da lei de drogas: a...b...

5. da lei de controle de armas de guerra: a...b...

6. do código penal internacional:

a) genocídio ... b) crimes contra a humanidade c) crimes de guerra d) crimes de agressão

7. da lei de armas: a...b...

(3) A medida só pode se dirigir contra o afetado. Uma intervenção em sistemas informáticos de outras pessoas só é permitida, caso, em razão de fatos concretos, se possa assumir que

1. o afetado mencionado na decisão utilize sistemas informáticos da outra pessoa, e
2. a realização da intervenção apenas nos sistemas informáticos do afetado não possibilite a investigação dos fatos ou do local onde se encontra um co-investigado.
A medida também pode ser executada caso outras pessoas sejam afetadas de forma mediata.

(4) § 100a Absatz 5 e 6 se aplicam, com a exceção da Abs. 5 Satz 1 Nr. 1, naquilo que couber.

§ 100a Abs. 5 e 6:

(5) Em relação à medida, deve-se assegurar tecnicamente que
(...)
2. só sejam realizadas alterações no sistema informático que sejam indispensáveis para o levantamento dos dados, e
3. as alterações realizadas, desde que tecnicamente possíveis, sejam automaticamente excluídas ao término da medida.
O meio empregado deve ser protegido contra utilização desautorizada segundo o estágio da tecnologia. Dados copiados devem, segundo o estágio da tecnologia, ser protegidos contra alteração, exclusão e tomada de conhecimento desautorizados.

(6) Em toda ocasião em que se empregue a medida, é imperativo o registro
1. da qualificação do meio técnico utilizado e do momento de sua utilização,
2. de informações para a identificação do sistema informático e das alterações realizadas que não sejam simplesmente transitórias,
3. de informações que possibilitem a determinação dos dados levantados, e
4. do departamento que executa a medida.

§ 100d StPO:
(1) As medidas dos §§ 100a a 100c são inadmissíveis caso seja possível assumir, com base em elementos fáticos, que suas execuções venham a obter apenas informações relativas ao núcleo da esfera privada.

(2) Informações do núcleo da esfera privada, obtidas por meio das medidas dos §§ 100a a 100c, não podem ser valoradas no processo. Registros de tais informações devem ser imediatamente eliminados. O fato de terem sido obtidas e eliminadas deve ser documentado.
(3) Em relação à medida do § 100b [Infiltração online], deve-se, desde que possível, garantir que dados relativos ao núcleo da esfera privada não sejam obtidos. Informações relativas ao núcleo da esfera privada, obtidas por meio da medida do § 100b, devem ser imediatamente eliminadas ou submetidas, pela promotoria, ao juízo, para decisão a respeito da possibilidade de valoração e da eliminação dos dados. A decisão do juízo a respeito da possibilidade de valoração é vinculante para o outro processo.
(4) ... em relação à medida do § 100c.
§ 101 – Regras procedimentais relativas a medidas ocultas
... (8) Os dados pessoais, obtidos por meio das medidas, que não sejam mais necessários para a persecução penal ou para uma eventual verificação judicial devem ser eliminados imediatamente. Desde que os dados sejam mantidos apenas para uma eventual verificação judicial, eles podem ser utilizados sem o consentimento do afetado apenas para esse propósito; eles devem ser bloqueados.

Referências bibliográficas

Bär, Comentário à decisao BVErfGE 120, 274, in: MMR 2008, p. 325 e ss.

Beukelmann, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017, p. 440.

Blechschmitt, Quellen-TKÜ und Online-Durchsuchung, StraFo 2017, p. 361

Bruns, in: Hannich (coord.), Karlsruher Kommentar zur Strafprozessordnung, 8a. ed., München, 2019 (= KK-StPO).

Derin/Golla, Der Staat als Manipulant und Saboteur der IT-Sicherheit, in: NJW 2019, p. 1111.

Dimoulis/Martins, Teoria Geral dos Direitos Fundamentais, 5ª. ed., 2014.

Ferreira Mendes/Gonet Branco, Curso de Direito Constitucional, 12ª. ed., 2017.

Graf (coord.), Beck'scher Online-Kommentar Strafprozessordnung (= BeckOK StPO), 33ª. ed., 1.4.2019.

Greco, Fortgeleiteter Schmerz – Überlegungen zum Verhältnis von Prozessabsprache, Wahrheitsermittlung und Prozessstruktur, in: GA 2016, p. 1.

Grözinger, Die Überwachung von Cloud-Storage, Baden-Baden, 2018.

Hilgendorf/Valerius, Direito Penal: Parte Geral, São Paulo, 2018.

Rüscher, Alexa, Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden?, NStZ 2018, p. 687.

Sarlet, Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988, 10ª. ed. Porto Alegre, 2015.

Sarlet, Teoria geral dos direitos fundamentais, in: Sarlet/Marinoni/Mitidiero, Curso de direito constitucional, 7ª. ed., 2018.

Schünemann, Legitimation durch Verfahren?, StraFo 2015, p. 177.

Soiné, Die strafprozessuale Online-Durchsuchung, NStZ 2018, p. 497 e ss.

Wolter (coord.), Systematischer Kommentar zur Strafprozessordnung (= SK-StPO), vol. 2, 5a. ed., Köln, 2016.

Wolter, O inviolável e o intocável no direito processual penal: reflexões sobre a dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal, São Paulo, 2018.

Záboji, „Unheimliche Bilder", in: Frankfurter Allgemeine Zeitung, publicado em 8.6.2016, acessível em: http://bit.ly/2LZUCKM.

Informações adicionais e declarações dos autores
(integridade científica)

Declaração de conflito de interesses (conflict of interest declaration): os autores confirmam que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

- *Luís Greco*: projeto e esboço inicial, coleta e análise de dados, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.
- *Orlandino Gleizer*: projeto e esboço inicial, coleta e análise de dados, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.

Declaração de ineditismo e originalidade (declaration of originality): os autores asseguram que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atestam que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 30/07/2019
- Retorno rodada de correções: 16/09/2019
- *Autores convidados*

http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies - custom-1

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (BC e CC)

COMO CITAR ESTE ARTIGO:

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.278