O ACESSO AUTORIZADO A APARELHOS *SMART*: BURLA AO AGENTE INFILTRADO DIGITAL?

THE AUTHORIZED ACCESS TO SMART DEVICES: CHEAT TO THE DIGITAL UNDERCOVER AGENT?

Nereu Giacomolli

Doutor em Processo Penal pela Universidad Complutense de Madrid com estágio pós-doutoral na Università degli studi di Torino. Professor do programa de pós-graduação em Ciências Criminais pela PUCRS e em Direito da Universidade Autónoma de Lisboa. Advogado.
Link Lattes: http://lattes.cnpq.br/5969235847033808
ORCID: 0000-0003-1753-0334
nereu@giacomolli.com

Luiz Eduardo Cani

Doutorando em Ciências Criminais na PUCRS. Bolsista da CAPES. Professor. Advogado.
Link Lattes: http://lattes.cnpq.br/8283452898258709
ORCID: 0000-0003-4016-5945
luiz@cani.adv.br

Resumo: No embalo das técnicas especiais de investigação, introduziu-se no Brasil a figura emblemática do agente infiltrado digital, sem, contudo, um regramento mínimo: sequer foi definido o meio para tal infiltração. Daí decorre o recurso a *malwares* e outras práticas extremamente invasivas. Paralelamente, vê-se o crescente uso do acesso a aparelhos eletrônicos para obtenção de informações – não raro, provas produzidas antecipadamente desde o início das investigações. Analisou-se algumas peculiaridades desses dois meios de obtenção de prova.

Palavras-chave: Crime organizado - Interceptação telefônica - Busca e apreensão.

Abstract: In the trail of special investigation techniques, the emblematic figure of the digital undercover agent was introduced in Brazil, without, however, a minimum regulation: the manner for such infiltration was not even defined. On account of this, the resort to malware and other extremely invasive practices. At the same time, there is the growing use of access to electronic devices to obtain information – frequently, evidences produced anticipatedly in the beginning of the investigations. Some peculiarities of these two means of obtaining evidence were analyzed.

Keywords: Organized crime - Telephone interception - Search and seizure.

O acesso autorizado a aparelhos *smart*: burla ao agente infiltrado digital?

1. A introdução de técnicas especiais de investigação se deve à Convenção de Palermo, por meio da qual os Estados signatários se comprometem a introduzir nos respectivos ordenamentos jurídicos, desde que compatível aos princípios fundamentais, técnicas de entrega vigiada, vigilância eletrônica, operações de infiltração e outras técnicas de vigilância destinadas a "combater eficazmente a criminalidade organizada" (art. 20, item 1, do Decreto 5.015/04).

Dentre essas técnicas, elencamos: (a) interceptação telefônica (Lei 9.296/96); (b) captação ambiental de sinais eletromagnéticos, óticos e/ou acústicos (art. 8º-A da Lei 9.296/96); (c) ação controlada (art. 1º, § 6º, da Lei 9.613/98; art. 53, II, da Lei 11.343/06; e arts. 8º e 9º da Lei 12.850/13); (d) infiltração de agentes (art. 1º, § 6º, da Lei 9.613/98; art. 53, I, da Lei 11.343/06; e arts. 10 a 14 da Lei 12.850/13); (e) afastamento de sigilos bancário, fiscal, financeiro e eleitoral (art. 1º, §§ 3º e 4º, da Lei complementar 105/01; art. 198, § 1º, do CTN; arts. 28 e 29 da Lei 7.492/86; art. 94-A, I, da Lei 9.504/97; e art. 30-A, § 1º, da Lei 9.504/97 c/c art. 22, VIII, da Lei complementar 64/90); (f) acesso a registros de ligações telefônicas e telemáticas, a dados constantes em bancos de dados públicos e privados, e a informações eleitorais ou comerciais (arts. 15 a 17 da Lei 12.850/13); (g) delação premiada (art. 159, § 4º, do Código Penal; art. 25, § 2º, da Lei da 7.492/86; art. 16, parágrafo único, da Lei 8.137/90; art. 8º, parágrafo único, da Lei 8.072/90; art. 1º, § 5º, da Lei 9.613/98; arts. 13 a 15 da Lei 9.807/99; art. 41 da Lei 11.343/06; e arts. 3º-A a 7º da Lei 12.850/13); (g) acordo de leniência (arts. 86 e 87 da Lei 12.529/11, com efeitos na esfera penal por força dos arts. 13 a 15 da Lei 9.807/99); (h) compra direta de informações (Lei 13.608/18); e (i) cooperação jurídica internacional (art. 3º, VIII, da Lei 12.850/13 c/c Decretos 6.747/09 e 9.662/19).

As diretrizes da Convenção de Palermo foram elaboradas em face do *maxi* processo da *Cosa Nostra*, na Sicília, o maior processo italiano contra uma organização criminosa existente até então, seguido pelo atual *maxi* processo em razão da *'Ndrangheta*, na Lombardia. Devido ao conjunto de dificuldades na persecução na busca de provas acerca dos crimes, a vigilância constante pretendida na Convenção mira os aparelhos eletrônicos como excelentes fontes e meios.

Dito de outro modo, para perseguir crimes circunscritos aos pactos de silêncio (*omertà*), criaram-se mecanismos para incentivar os investigados a falar (delação premiada e acordo de leniência, *v.g.*) e estabeleceram-se técnicas de investigação reprodutoras das ações investigadas (dentre as disposições que regulamentam a infiltração de agentes, tem-se a autorização para a prática de alguns crimes, *v.g.*).

2. O compromisso com a introdução de técnicas especiais de investigação à vigilância da criminalidade organizada, por conta da adesão à Convenção de Palermo, ensejou a necessidade de apreciar as medidas compatíveis com o ordenamento jurídico brasileiro. Desde a promulgação, a Constituição Federal contempla, expressamente, medidas de interceptação das comunicações telefônicas (art. 5º, XII).

Indubitavelmente, o sigilo abrange toda a dimensão do preceito: correspondência, comunicação telegráfica, dados e comunicação telefônica – nessa ordem. Assim, tudo isso compõe a esfera da

inviolabilidade constitucional.

A exceção consiste em autorização constitucional ao afastamento do sigilo, por ordem judicial, conforme lei a ser editada (norma constitucional de eficácia contida por princípio institutivo) durante a *persecutio criminis*, isto é, tanto na fase de investigação quanto na processual.

Primeiro entrave: qual o "último caso"?

Três podem ser as respostas: (a) as comunicações, na medida em que vêm após as correspondências e os dados; (b) os dados e as comunicações telefônicas, pois separados das correspondências e das comunicações telemáticas; ou (c) as comunicações telefônicas, por estarem após a correspondência, a comunicação telemática e os dados. Qualquer outra resposta excede os limites dos sentidos.

Considerada a primeira resposta (a), implícito está que a inviolabilidade constitucional é atribuída aos dados e não à comunicação dos dados.[1] Para se considerar os dados e as comunicações telefônicas, é preciso ignorar que não se trata apenas do "último caso", mas também do "penúltimo caso". Restam, então, duas opções: a Constituição admite o afastamento do sigilo apenas das comunicações telefônicas ou também das comunicações telemáticas.

Entende-se que se trata de hipótese de afastamento apenas do sigilo das comunicações telefônicas. A consequência imediata dessa constatação é a de que as técnicas especiais de investigação não poderiam ser utilizadas para a obtenção de dados, pois afastariam, de maneira inconstitucional, a inviolabilidade do sigilo.

3. Mas não é esse o entendimento majoritário na doutrina e na jurisprudência. Muito diferente disso, as práticas jurídicas produziram uma cisão entre dado e registro, como se o registro não fosse um dado, para que se pudesse deixar de aplicar a inviolabilidade constitucional do sigilo de dados aos aparelhos eletrônicos. A consequência dessa operação foi uma situação paradoxal, na qual o sigilo existe e vale, mas não se aplica. Subsidiariamente, remanesceu a proteção constitucional à privacidade e à intimidade (art. 5º, X, CF).

Primeira burla: a jurisprudência afastou o sigilo constitucional dos dados a pretexto de estar tutelada apenas a comunicação. Assim, todos os dados decorrentes das comunicações passaram a receber tratamento constitucional muito menos protetivo. De invioláveis, os dados se tornaram apreensíveis. Apreensões que sequer pressupõem um rol taxativo de crimes por força dos quais poderiam ocorrer e culminar no periciamento de aparelhos eletrônicos. Esse movimento possibilitou um alargamento das técnicas especiais de investigação, cujas práticas e utilização vêm se tornando cada vez mais amplas e profundas.[2]

Segunda burla: na falta de lei específica, passou-se a adotar a Lei 9.296/96 como parâmetro ao acesso autorizado aos aparelhos eletrônicos, como se todo acesso a dados fosse interceptação de comunicação telefônica ou equiparado. Faz-se de conta que não há diferença, ou talvez até oposição, entre a interceptação (durante a comunicação e desde um local distante do aparelho) e o acesso (após toda a atividade e em posse do aparelho).

4. A consequência da preponderância desses entendimentos é a admissibilidade da captura de dados por vários métodos de obtenção de prova. O mais comum passou a ser a apreensão dos aparelhos eletrônicos e o acesso aos dados nele contidos. A preponderância desse método se deve, certamente, aos requisitos menos rigorosos (admitido para a persecução de qualquer crime, sem prazo fixado para início e fim da medida e sem necessidade de apresentar muitos indícios para requerer autorização judicial – quando essa não é dispensada por se tratar de crime permanente), mas também por possibilitar uma devassa espaço-temporal limitada tão somente pelos dados armazenados no aparelho e nas contas a ele vinculadas.

Em outras palavras: basta apreender um aparelho eletrônico e obter autorização judicial para acessar todo o conteúdo armazenado e/ou vinculado[3] (contas em quaisquer servidores: *e-mails*, nuvens, sistemas, redes sociais, sites de relacionamento, instituições financeiras, instituições de ensino, etc.). Implícito a essa autorização, por conta da total ausência de regramento específico da medida, há entendimento de que todos os aplicativos e contas vinculados ao aparelho podem ser acessados (devassados), sem limitação temporal (burla do próprio limite temporal de duração da interceptação, prevista no art. 5º da Lei 9.296/96, utilizada como fundamento legal ao acesso ao aparelho eletrônico) e sem qualquer necessidade de apresentação de indícios e de apontamento de relação causal entre a persecução em andamento e a medida pretendida (burla ao princípio da especialidade da prova).

Portanto, trata-se de um método atípico de obtenção de prova, de proximidade entre investigador e aparelho, de acesso ilimitado ao conteúdo armazenado/vinculado, com poucos requisitos e muitos benefícios, com potencial muito mais invasivo do que a maioria das técnicas especiais de investigação, tratado como se fosse interceptação telefônica.

5. Outro método que pode se tornar cada vez mais comum é o do agente infiltrado digital, recentemente introduzido nos arts. 10-A a 11 da Lei 12.850/13 por meio da Lei 13.964/19. Trata-se de um método que, de certa forma, é fruto de uma tripla especialização. Primeira, do acesso autorizado a aparelho eletrônico, pois pressupõe autorização judicial, mas se dá sem a apreensão do aparelho. Segunda, da interceptação telefônica, na medida em que permite obter dados sobre as atividades realizadas durante o período da infiltração. Terceira, da infiltração de agentes, porquanto não são mais necessárias investidas presenciais.

Quiçá se possa dizer que, ao fim e ao cabo, tem-se uma especialização das técnicas especializadas de investigação, destinada à persecução de infração penal praticada por organização criminosa ou organização terrorista, ou de infrações penais previstas em tratados ou convenções, cuja execução tenha iniciado ou cujo resultado tenha se produzido no país (art. 10-A, § 3º c/c art. 1º da Lei 12.850/13).

Como se pode notar, mesmo em uma rápida leitura das disposições legais, não há regramento específico do meio à execução da infiltração de agentes. Daí porque no Brasil, assim como vem ocorrendo na Europa, para realizar a infiltração de agente digital, as polícias recorrem frequentemente ao uso de *malware*: programa de computador que se instala no aparelho após a quebra dos protocolos de segurança e permite a devassa do aparelho, inclusive a adulteração dos dados armazenados.[4]

6. Há inúmeras anomias e antinomias decorrentes do uso do *malware* para a infiltração de agentes: desde a já mencionada ausência de limitação dos meios à consecução da infiltração, passando pelo quase eterno prazo (em termos digitais) de até 720 dias (art. 10-A, § 4º, da Lei 12.850/13), até chegar à autorização de prática de crimes a fim de perseguir crimes (art. 10-C da Lei 12.850/13). Sem contar o já mencionado afastamento inconstitucional do sigilo de dados.

Interessa neste articulado, contudo, apenas a constatação de que se trata de medida excepcionalíssima e requer a apresentação de elementos de investigação que indiquem a prática de infração penal prevista no catálogo: relacionada à organização criminosa, organização terrorista, ou prevista em tratado ou convenção internacional.

Para executar a medida, o agente há de se aproximar do suspeito no espaço digital. Essa aproximação pode ocorrer por meio de solicitação de amizade em redes sociais, envio de mensagem por *e-mail* ou aplicativo de troca de mensagens ou, a medida mais invasiva, acessando aparelho eletrônico com quebra dos protocolos de segurança: seja utilizando técnicas de *hacking* manual ou lançando mão de ferramentas automatizadas (*softwares* como *malwares*, *keyloggers*, *trojans* etc.).

7. Portanto, as medidas de acesso com autorização judicial não são necessariamente distintas. A depender do meio utilizado na infiltração do agente digital, pode-se ter mera especialização do acesso autorizado a aparelhos eletrônicos. O *malware* é a "certa forma" que implica em uma tripla especialização ou em uma especialização das técnicas especiais de investigação: executado à distância, com acesso a todo o conteúdo armazenado e/ou vinculado, sem restrição

temporal para trás (embora delimitado temporalmente no futuro para até 720 dias).

Comparando-se uma medida a outra tem-se, por um lado (acesso autorizado a aparelho eletrônico), uma medida atípica, sem regramento específico, ilimitada temporalmente pela decisão judicial (o limite temporal do conteúdo decorre do momento da apreensão), executada de posse do aparelho, que precisa ser obtida após a apreensão lícita, admitida à persecução de qualquer infração penal (ou, quando aplicada a Lei 9.296/96 como parâmetro, para os crimes apenados com reclusão), e, por outro (infiltração de agente digital por meio de *malware*), uma medida típica, com regramento poroso, limitada temporalmente pela decisão judicial apenas em relação ao futuro (prazo máximo de 720 dias), executada à distância do aparelho sem necessidade de proximidade física, admitida apenas à persecução de infrações penais determinadas. Ambas comungam da devassa inconstitucional aos dados dos usuários, da vinculação à reserva jurisdicional e da ausência de restrição legal ao conteúdo armazenado/vinculado que pode ser obtido.

8. **Última burla**: o acesso autorizado a aparelho eletrônico para a persecução de crimes previstos na Lei 12.850/13. Lançar mão da apreensão de aparelhos eletrônicos na persecução dos crimes para os quais é cabível o agente infiltrado digital consiste tanto em violação ao princípio da especialidade da prova quanto em burla indevida à reserva legal (catálogo de infrações penais). Sendo tal medida, altamente invasiva, prevista exclusivamente para tais infrações penais, como *extrema ratio*, não é possível lançar mão de medida ainda mais invasiva e menos regrada (acesso autorizado a aparelhos eletrônicos) a fim de contornar os requisitos legais e realizar uma persecução com menos limites, restrições e definições.

Ademais, admitida a infiltração de agente digital, não pode sê-lo por *malware*, pois o uso dessa técnica de investigação não possui proporcionalidade em sentido estrito: é a medida mais restritiva de direito fundamental, sem qualquer justificativa para tanto, sobretudo porque cabíveis outras metodologias muito menos invasivas.

9. Pode-se dizer que tanto o acesso autorizado a aparelhos eletrônicos quanto o uso de *malware* à infiltração digital de agentes são burlas. O *malware*, especificamente, é a burla no seio da burla: burla-se a tutela constitucional dos dados para que se possa obtê-los, depois burla-se a infiltração para utilizar uma técnica dissimulada, consistente na violação da privacidade e da intimidade dos suspeitos para investigá-los. E, ainda assim, pode-se burlar o *malware* com o acesso autorizado, impondo uma burla de terceiro grau: contorno do catálogo.

Por isso, propõe-se três medidas restritivas das técnicas especiais de investigação, indispensáveis a evitar o alargamento indefinido e ilimitado das investigações.

Primeiro: se se quer reconhecer a constitucionalidade do afastamento do sigilo de dados, há que se admitir tais técnicas apenas à investigação de um número assaz reduzido de crimes. Trata-se da proposta, bastante debatida na Europa, da formação de um catálogo de crimes nos quais as técnicas são admitidas: "O catálogo de crimes deve ser, desde logo, aferido do tecido constitucional e deve assumir-se como um critério limitativo em razão dos tipos legais de crime [e em razão da pena]."[5]

Segundo: aparelhos eletrônicos de uso pessoal contêm dados que excedem qualquer conteúdo apreensível em uma busca domiciliar (domicílio físico). Há dados de todas as ordens, desde públicos até dados relacionados aos mais profundos segredos da vida pessoal do usuário – os quais não podem ser acessados por ninguém. Sigilos fiscal e bancário podem ser afastados requisitando-se informações. Comunicações telefônicas podem ser interceptadas durante a realização. O trajeto de suspeitos pode ser acompanhado em campanas. Conversas com outras pessoas podem ter o conteúdo descoberto por inquirição ou captação por um dos interlocutores. Enfim, há diversas medidas menos invasivas do que o acesso a aparelhos eletrônicos, seja por autorização judicial após apreensão, seja por infiltração de *malware*. Não se pode admitir medidas mais invasivas quando outras, muito menos invasivas, estão à disposição do Estado. Os custos operacionais jamais justificam a supressão dos direitos e das garantias fundamentais.[6]

Terceiro: é necessário distinguir conteúdo armazenado de conteúdo vinculado. Todo conteúdo vinculado excede o mandado judicial de acesso ao aparelho. Todas as vinculações excedem o conteúdo do armazenamento e podem ser obtidas por outros meios de investigação. Notadamente, as quebras de sigilos fiscal e bancário, e as requisições de dados para servidores de *internet*.

Notas

[1] *A latere* de tal fato: "A resposta adequada à Constituição, nesse caso, é no sentido de que *qualquer que seja o meio utilizado para a comunicação* – telegráfica, de dados e telefônica – e passível de interceptação para prova em investigação criminal e instrução processual penal, desde que autorizada por ordem judicial, nos termos da Lei n. 9.296/96." (STRECK, 2018, p. 314).

[2] Nesse sentido: "Primeiramente, sobreleva destacar que não se confundem *comunicação telefônica* e os *registros telefônicos*, as quais, inclusive, recebem proteção jurídica distinta. E, como já enfatizamos em outras oportunidades, entendemos que não se pode interpretar a cláusula do art. 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional *é da comunicação 'de dados' e não os 'dados'*." (BRASIL, 2012).

[3] O que aqui se chama de dado vinculado, geralmente disponível em todos os aparelhos *smart*, vem sendo equivocadamente tratado como se fosse dado armazenado, de modo a permitir devassas irrestritas, conforme Ricardo Jacobsen Gloeckner e Daniela Dora Eilberg já destacaram: "A situação se torna ainda mais complexa quando se constata que o uso de telefones celulares também é feito para acessar dados digitais que não se encontram armazenados no próprio aparelho (*cloud computing*). O acesso de conteúdo armazenado na nuvem trata da capacidade do dispositivo em acessar dados que estão armazenados em servidores remotos. Alguns usuários não conseguem distinguir entre os dados armazenados no celular e aqueles armazenados na nuvem, como bem identificado pelo *Brief for Amicus Curiae Electronic Privacy Information Center* (Epic). E tais dados estariam fora da margem de proteção da doutrina SITA. Acentuou o juiz Roberts que esse tipo de busca seria como encontrar a chave da casa no bolso do suspeito e argumentar que tal fato autorizaria a busca feita pela polícia." (GLOECKNER; EILBERG, 2019, p. 365).

[4] "*Malware*, em definição simples, refere-se a um programa malicioso instalado clandestinamente por terceiro em um sistema de processamento, uma ameaça destinada à quebra da confidencialidade e integralidade dos dados nele contidos. Trata-se de um *software* previamente programado cuja função é infectar dispositivos eletrônicos (*smartphone, tablet* ou *PC*) para tornar possível o acesso remoto às informações, comunicações ou arquivos neles armazenados ou acessar suas funcionalidades (áudio, vídeo, *e-mail*, câmera, *web* e etc) independentemente de estarem ativas ou não." (MENDES, 2020, p. 162-163).

[5] VALENTE, 2018, p. 19-20.

[6] Ademais, o *malware* lançado contra um suspeito pode lesar terceiros: "Não é demais lembrar que o usuário do *e-mail* ou do dispositivo (ainda que sendo um 'não suspeito'), ao se infectar com o *malware* corresponderá às máximas expectativas dos investigadores e desta forma, pela expectativa gerada a partir da evidência esquizofrênica, também se projeta na pessoa do 'não suspeito' o resultado: o culpado." (MENDES, 2020, p. 199).

Referências

BRASIL. Supremo Tribunal Federal (2. Turma). *HC 91.867/PA*, Relator: Min. Gilmar Mendes, 24 de abril de 2012. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acesso em: 23 nov. 2021.

GLOECKNER, Ricardo J.; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios frente aos avanços tecnológicos. *Revista Brasileira de Ciências Criminais*, v. 156, pp. 353-392, 2019.

MENDES, Carlos Hélder C. F.. *Tecnoinvestigação criminal.* Entre a proteção de dados e a infiltração por *software*. Salvador: JusPodivm, 2020.

STRECK, Lenio Luiz. Art. 5º, XII. *In*: CANOTILHO, J. J. Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. (Coord.). *Comentários à Constituição do Brasil.* São Paulo: Saraiva, 2018, p. 314.

VALENTE, Manuel. O reforço dos princípios constitucionais na obtenção de prova no mundo digital. *Revista de Direito de Polícia Judiciária*, ano 2, n. 3, pp. 11-25, 2018.

Autores convidados