Software espião e monitoramento secreto de dispositivos de dados e comunicação

29/06/2024

Introdução

A discussão a respeito dos limites do poder investigativo estatal e a proteção da privacidade vive um novo capítulo no julgamento da ação direta de inconstitucionalidade por omissão (ADO nº 84/DF [1]) ajuizada pela Procuradoria-Geral da República (PGR), sob a relatoria do ministro Cristiano Zanin.

Arguindo o vácuo normativo do Congresso, a PGR postulou que o STF estabeleça — enquanto não suprida a omissão legislativa — "balizas provisórias à salvaguarda dos direitos fundamentais à intimidade e à privacidade, e à inviolabilidade do sigilo das comunicações pessoais e de dados, até que seja sanada a lacuna normativa inconstitucional".

A sociedade contemporânea, impulsionada e beneficiada pelos avanços tecnológicos que objetivam a inclusão digital, enfrenta desafios significativos no que concerne à proteção dos direitos fundamentais, em especial, da privacidade e autonomia dos indivíduos. Dentre esses desafios, destaca-se a utilização de ferramentas de intrusão virtual remota e de monitoramento secreto, as quais colocam em risco a inviolabilidade das comunicações pessoais e a intimidade.

É neste contexto que se destaca a necessidade de uma releitura (mutação constitucional [2]) de dispositivos constitucionais (CRFB, art. 5º, incisos X e XII) para alcançar-se uma normatividade que faça frente ao uso (ainda indiscriminado) dessas novas tecnologias e, ao mesmo tempo, que assegure a efetividade de direitos fundamentais consagrados na Constituição.

Proteção constitucional da privacidade e da intimidade

A Constituição de 1988, em seu artigo 5º, incisos X e XII, consagra a inviolabilidade da intimidade, da vida privada e do sigilo das comunicações pessoais e de dados. Esses dispositivos estabelecem um escudo protetor contra interferências indevidas, assegurando a dignidade e a liberdade individual. Buscando dar concretude a essas garantias, a legislação infraconstitucional (Lei nº 9.296/1996, Lei nº 12.965/2014 e a Lei nº 13.709/2018) teceu um manto normativo no intuito proteger os dados e a privacidade no ambiente digital. Contudo, essas leis não abordam de forma abrangente as novas tecnologias de intrusão, como os *spywares/malwares* [3], que operam sem o conhecimento ou consentimento do usuário, evidenciando a necessidade de uma regulamentação mais específica, robusta e uniforme.

Impactos das ferramentas de intrusão na privacidade

Ferramentas avançadas de tecnologia — como, p. ex., o Pegasus, da NSO Group — têm sido utilizadas para exercer a vigilância cibernética, interceptando dados ao infectar dispositivos de dados e comunicação. A NSO Group sustenta que o produto é comercializado para que Estados

investiguem crimes de alta gravidade (terrorismo, tráfico, etc).

Porém, na obra "Pegasus" [4], os autores Laurent Richard e Sandrini Rigaud denunciaram que o *spyware* teria sido utilizado para hackear ativistas dos direitos humanos, advogados e jornalistas [5]. Em um processo movido pelo WhatsApp contra a NSO Group, estima-se que aproximadamente 1400 usuários tiveram seus equipamentos infectados apenas em um período de duas semanas [6]. E, em uma decisão proferida em 23/02/2024, a justiça do Northern District of California ordenou [7] que a empresa israelense apresente documentos e o código-fonte do Pegasus, possibilitando identificar o número de pessoas que realmente foram hackeadas.

O envio de *links* maliciosos; o *download* de *softwares* supostamente oficiais e a interceptação de tráfego de rede não criptografado com a introdução direta de códigos maliciosos (*zero-click*), são apenas algumas das maneiras — quase imperceptíveis — de vigiar e extrair informações constantes de dispositivos de comunicação.

Uma vez instalada, a ferramenta explora vulnerabilidades do sistema (*zero-day vulnerabilities*), permitindo que o *spyware* atue como administrador e execute comandos no dispositivo infectado sem a necessidade de interação do usuário.

O *software* consegue, passando a comandar o sistema informático, realizar uma série de funcionalidades invasivas que alcançam todo o tipo de informação sensível existente no dispositivo, trazendo sérias implicações para a segurança e a privacidade digital, tais como: copiar e transmitir mensagens de aplicativos como WhatsApp, iMessage, Telegram, e-mails; identificar a localização do dispositivo em tempo real; ativar remotamente e secretamente gravar o áudio e o vídeo a partir do próprio aparelho; monitorar a registrar teclas apertadas (keylogging) "como se o investigador *espreitasse* por cima do ombro do visado" [8]; extrair as listas de contatos, registros de chamadas e agendas; informar o histórico de navegação, senhas, dados de aplicativos, etc [9]. Além disso, o *spyware* também pode se camuflar, evitando a sua identificação por *softwares* de segurança e consegue alterar arquivos para se manter operante e resistir a tentativas de remoção.

O diuturno aprimoramento das tecnologias tem a força de promover sobremaneira os direitos humanos e, ao mesmo tempo, são instrumentos importantes para a investigação e repressão de crimes graves e de execução sofisticada, que fomentam na sociedade "uma maior tolerância para a imposição de medidas progressivamente mais restritivas de direitos fundamentais" [10].

A interceptação das comunicações e a "*vigilância discreta, inclusive por meios eletrônicos*", inclusive fazem parte das recomendações do Parlamento Europeu e do Conselho para a investigação dos casos de abuso sexual e exploração sexual de crianças [11]. Ou seja, não há dúvida que a utilização de *spywares* garante uma maior qualidade probatória, ao possibilitar um monitoramento diuturno do alvo sem a necessidade de colaboração de terceiros [12]. Porém, faz-se necessário voltar os olhos para o necessário equilíbrio entre a inovação tecnológica e a proteção de direitos, de maneira a garantir que os avanços não solapem a privacidade e a autonomia individual [13].

Teoria da 'mente estendida'

A maneira como as leis disciplinam (ou deveriam disciplinar) a flexibilização da nossa privacidade, deve levar em consideração a garantia de outros bens e valores resguardados pela Constituição. Se não é possível falar-se em direitos de caráter absolutos, devemos ter claro que o exercício legítimo e eficiente de uma ação investigativa (e de inteligência) não pode desprezar a ressignificação do círculo mais restrito de nossa intimidade sob a roupagem dos novos dispositivos de comunicação. Segundo Matthew Noah Smith (Associate Professor da Northeastern University), os nossos dispositivos eletrônicos "*são literalmente partes de nossas mentes*", ou seja, uma forma de "*mente estendida*":

> *"Não há distinção fundamental entre os processos que ocorrem na massa encefálica em seu crânio e os processos que ocorrem no pequeno bloco de silício, metal e vidro que é seu iPhone. O disco rígido de estado sólido que armazena fotos no telefone são suas memórias da mesma forma que certos grupos de neurônios que armazenam imagens em seu cérebro são memórias. Nossas mentes se estendem além de nossas cabeças e dentro de nossos telefones."* [14]

A ideia da "mente estendida" já havia sido tratada por Andy Clark e David J. Chalmers na década de 1990 ("*The Extended Mind*" [15]) sob a perspectiva — agora, ainda mais atual — de que quase ninguém mais depende de sua memória para se recordar de dados periféricos (p. ex., o número de telefones, endereços, senhas de aplicativos, aniversário, etc). "De acordo com a tese da mente estendida, nossos smartphones — pelo menos nesses aspectos — já se tornaram parte de nossas mentes" [16] e, assim, "fornecem mais informações sobre a sua pessoa que eventual violação do seu domicílio físico" [17].

Spacca

Daniel Avelar
juiz de Direito

Agindo como uma forma de "*cerebroscópio*" — "um dispositivo mitológico capaz de mostrar os pensamentos de uma pessoa na tela [18]" —, os *spywares* alcançam a informação que apenas se extrai sob o "*soro digital da verdade*" [19], na privacidade do teclado, nas sombras dos sites não indexados e nos abismos da *dark web*.

A forma mais usual de acesso dos brasileiros à internet é por meio de dispositivos móveis, especificamente smartphones. De acordo com a pesquisa TIC Domicílios 2023, realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), 99% dos usuários de internet no Brasil se conectam à rede pelo telefone celular [20].

Em 2022, a pesquisa noticiou que cerca de 149 milhões de indivíduos com 10 anos ou mais (81%) eram usuários de Internet. E, segundo com o mesmo instituto, em setembro de 2022, o país alcançou a marca de 5 milhões de nomes registrados sob o domínio

.br1. “Se considerarmos os países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e do Grupo dos 20 (G20), o .br ocupa a quinta posição entre os domínios de topo para código de país (country-code Top Level Domain [ccTLD]) mais populares” [21].

Os números dilatados evidenciam a pujança da utilização de smartphones para o acesso à rede. Mas a modernização da tecnologia embarcada nos aparelhos é igualmente um dado que não deve ser desprezado. Para além da mera função de comunicação, identificamos que os aparelhos carregam um espelhamento no nosso “eu” do passado, do presente e projetam o nosso futuro. Com isso, relativizando o princípio da vedação à autoincriminação, o acesso indiscriminado via *spywares* ainda se torna um instrumento de obtenção de prova contra terceiros suspeitos (ou não) da prática de todo e qualquer ato desviante, seja ele (i)legal ou meramente (i)moral.

Daí segue a necessidade, pelo avanço tecnológico que compacta a nossa intimidade ao mundo digital [22], de uma ressignificação do alcance das normas esculpidas no art. 5º., X e XII, da CRFB e de uma regulamentação do uso dessas novas tecnologias. Somente assim será possível garantir a convivência harmoniosa das liberdades e a efetiva proteção dos direitos de todos os cidadãos.

Necessidade de regulamentação específica e adequada

Considerando o grau de invasividade à garantia da intimidade, da autodeterminação e de outras garantias constitucionais inerentes ao Estado democrático de Direito (p. ex., a liberdade de imprensa), não há dúvida que o emprego desse tipo de tecnologia deve: estar condicionado à reserva de lei qualificada; estar amparado em requisitos rígidos, porém, compatíveis com os avanços tecnológicos; ser medida de exceção, ou seja, ser utilizado apenas quando outros meios de prova menos invasivos não sejam suficientes para alcançar o fim buscado; identificar o tipo de software utilizado, a sua versão e a forma de instalação; estar atrelado a objetivos e crimes específicos de extrema gravidade ou praticados por técnicas sofisticadas e meios digitais, vedando-se pesquisas meramente exploratórias; fixar prazo razoável de duração (prorrogável ou não); e ser dirigida exclusivamente para fins de investigação criminal ou instrução processual penal.

Além disso, para qualquer tipo de regulamentação futura, a cadeia de custódia da prova deverá ser obrigatoriamente observada, identificando-se: o *software* utilizado, data e período da sua utilização, o agente responsável, a forma de extração e cópia dos dados e o seu armazenamento.

Outrossim, de maneira a evitar-se o compartilhamento desarrazoado de dados sensíveis e desconectados do objeto da investigação, mostra-se necessária a imposição de regras para a destruição de dados irrelevantes e a fixação de um procedimento de fiscalização para a prevenção de abusos focado na confidencialidade dos dados.

Conclusão

O avanço tecnológico, ao mesmo tempo que proporciona inúmeros benefícios, também impõe desafios significativos à proteção dos direitos fundamentais de privacidade e intimidade. A

ausência de uma regulamentação específica sobre o uso de ferramentas de intrusão e monitoramento secreto constitui uma omissão inconstitucional que compromete a efetividade dos mandamentos constitucionais. É imperativo que o Congresso adote medidas normativas urgentes para estabelecer diretrizes claras e adequadas, garantindo o respeito aos direitos fundamentais consagrados na Constituição Federal e protegendo os cidadãos contra invasões arbitrárias de sua privacidade.

_____

[1] ADPF n. 1143/DF

[2] STF, 2a. Turma, HC n. 168052, Rel. Min. Gilmar Mendes, j. 20/10/2020. Conforme alertam Gloeckner e Eliberg: "A evolução dos aparelhos celulares e a revolução provocada pelo surgimento dos smartphones garantem certamente que antigos julgados e decisões resultem, com o passar dos anos, insuscetíveis de bem apreender os novos fenômenos tecnológicos, requerendo-se, sempre, a reflexão em torno do novo. (GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. **Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos**. In. Revista Brasileira de Ciências Criminais, vol. 156/2019, p. 353-393, Jun/2019).

[3] De acordo com Ramalho: o "termo malware, (...), resulta da contracção do adjectivo malicious (malicioso) e do substantivo software (programa informático) e pode ser definido resumidamente como 'um conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça' ou, mais desenvolvidamente, como 'um programa simples ou auto-replicativo que discretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático'" (RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital**. Coimbra: Almedina, 2017 (E-book)). Fabrício Weiblen, prefere a terminologia "software (ou programa) de controle remoto" ou "software (ou programa) espião", eis que "malware", "spyware" ou "vírus de Estado" são termos vinculados "à noção de ilicitude em seu uso, o que não é adequado para uma ferramenta que, guardadas as necessárias limitações jurídicas (...), releva-se essencial para a apuração de crimes na atualidade". (WEIBLEN, Fabrício Pinto. **O uso de software espião na investigação criminal. Interpretação aberta à tecnologia, (in)admissibilidade e tratamento jurídico adequado**. Londrina: Thoth Editora, 2024, p. 22 (E-book)).

[4] RICHARD, Laurent; RIGAUD, Sandrine. **Pegasus. The Secret Technology that Threatens the End of Privacy and Democracy.** Londres: Ed. Macmillan/Pan Books, 2023 (E-book).

[5] Denúncias similares foram feitas pela mídia internacional: https://www.nytimes.com/2023/09/14/world/europe/galina-timchenko-meduza-pegagus-spyware-russia.html?searchResultPosition=2 De acordo com o site "Forbidden Stories", pelo menos 180 jornalistas ao redor do mundo teriam sido selecionados como alvo por clientes da empresa NSO

Group (https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/).

[6] O número de aparelhos infectados pode alcançar cifras inimagináveis. É o que denuncia o "Forbidden Stories" e a Anistia Internacional: "Forbidden Stories e a Anistia Internacional tiveram acesso a um vazamento de mais de 50.000 registros de números de telefone que os clientes da NSO selecionaram para vigilância. Segundo uma análise desses registros realizada pelo Forbidden Stories e seus parceiros, os telefones de pelo menos 180 jornalistas foram selecionados em 20 países por pelo menos 10 clientes da NSO. Esses clientes governamentais variam de autocráticos (Bahrein, Marrocos e Arábia Saudita) a democráticos (Índia e México) e abrangem todo o mundo, desde a Hungria e o Azerbaijão na Europa até o Togo e Ruanda na África. Como o Projeto Pegasus irá mostrar, muitos deles não hesitaram em selecionar jornalistas, defensores dos direitos humanos, opositores políticos, empresários e até chefes de estado como alvos dessa tecnologia invasiva". Disponível em: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

[7] Case n. 19-cv-07123-PJH, WhatsApp Inc., et al., v. NSO Group Technologies Limited, et al.,: https://cdn-conjur.s3.amazonaws.com/uploads/2024/06/gov.uscourts.cand_.350613.292.0.pdf

[8] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital**. Coimbra: Almedina, 2017 (E-book).

[9] "Pegasus essentially owns a mobile phone; it can break down defenses built into a cell phone, including encrypton, and gain something close to free rein on the device, without ever tipping off the owner to its presence. That includes all text and voice communications to and from the phone, location data, photos and videos, notes, browsing history, even turning on the camera and the microphone of the device while the user has no idea it's happening. Complete remote personal surveillance, at the push of a button". (RICHARD, Laurent; RIGAUD, Sandrine. **Pegasus. The Secret Technology that Threatens the End of Privacy and Democracy.** Londres: Ed. Macmillan/Pan Books, 2023 (E-book).

[10] RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital**. Coimbra: Almedina, 2017 (E-book).

[11] Directiva 2011/92 do Parlamento Europeu e do Conselho. Extrai-se da Recomendação n. 27: "Os responsáveis pela investigação e pela acção penal relativas aos crimes referidos na presente directiva deverão dispor de instrumentos de investigação eficazes. Estes instrumentos podem incluir a intercepção de comunicações, a vigilância discreta, inclusive por meios electrónicos, a monitorização de contas bancárias ou outras investigações financeiras, tendo em conta, nomeadamente, o princípio da proporcionalidade e a natureza e gravidade dos crimes investigados. Se for caso disso, e de acordo com a legislação nacional, tais instrumentos deverão também incluir a possibilidade de as autoridades policiais utilizarem uma identidade falsa na Internet". Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32011L0093

[12] Enquanto uma busca e apreensão – ressalta Weiblen – "mostra apenas uma 'fotografia' do atual estado do material apreendido", o software permite um "monitoramento contínuo do comportamento do sistema alvo" e, "possibilita também a obtenção de 'conteúdos voláteis',

como diálogos em *chats* ou postagens anônimas em fóruns online". WEIBLEN, Fabrício Pinto. **O uso de software espião na investigação criminal...** Ob. cit., p. 27.

[13] "Tanto a noção de eficácia, como a de tutela de direitos e garantias dos cidadãos, pressupõem a adequação dos meios processualmente existentes ao objecto e características do processo. No primeiro caso, requer-se, em abstrato, que os meios sejam aptos a identificar o autor do ilícito e a recolher prova processualmente válida para a sua condenação. No segundo caso, requer-se que, em concreto, o sacrifício dos direitos do arguido e a redução das suas garantias sejam os estritamente necessários e constitucionalmente admissíveis para a investigação e obtenção de prova, à luz do critério da proporcionalidade". (id).

[14] „There is simply no principled distinction between the processes occurring in the meaty glob in your cranium and the processes occurring in the little silicon, metal, and glass block that is your iPhone. The solid-state drive storing photos in the phone are your memories in the same way that certain groups of neurons storing images in your brain are memories. Our minds extend beyond our heads and into our phones". SMITH, Matthew Noah. An iPhone is an Extension of the Mind. In. Slate. 29/02/2016, disponível em https://slate.com/technology/2016/02/apple-and-the-fbi-think-iphones-are-safes-a-philosopher-explains-what-they-really-are.html, com acesso em 25/06/2024.

[15] CLARK, Andy; CHALMERS, David. J. **The Extended Mind**. In. Analysis 58:10-23. Reprinted in (P. Grimm, ed) The Philosopher's Annual, vol. XXI, 1998.

[16] CLARK, Andy. The Experience Machine: **How Our Minds Predict and Shape Reality**, New York: Phanteon Books, 2023, p. 172 (E-book).

[17] CARVALHO RAMOS, André de. **Curso de direitos humanos**, 10ª ed., São Paulo: Saraiva, 2023, p. 861.

[18] PINKER, Steven. Prefácio da obra: DAVIDOWITZ-STEPHENS, Seth. Todo mundo mente. O que a internet e os dados dizem sobre quem realmente somos. São Paulo: Alta Books, 2018 (E-book).

[19] DAVIDOWITZ-STEPHENS, Seth. Todo mundo mente. O que a internet e os dados dizem sobre quem realmente somos. São Paulo: Alta Books, 2018 (E-book), p. 129.

[20] Fonte: CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros – TIC Domicílios 2023. Disponível em: https://cetic.br/pt/tics/domicilios/2023/individuos/C16/

[21] Fonte: CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros – TIC Domicílios 2023. Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2024/06/tic_domicilios_2022_livro_eletronico.pdf

[22] A esfera do privado, esclarecem Gloeckner e Eiberg, "corresponde inequivocamente o conjunto de dados pessoais, o que gera um direito à "autodeterminação informativa", sendo, em

consequência disso, uma condição da cidadania. Tomando-se o telefone celular como um conector entre diversos utilitários e aplicativos, chega-se facilmente à conclusão de que o dispositivo carrega tantas informações que, no limite, acabam se confundindo como uma extensão informacional da própria pessoa". (GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. **Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos**. In. Revista Brasileira de Ciências Criminais, vol. 156/2019, p. 353-393, Jun/2019).

Fonte: https://conjur.jumps.com.br/2024-jun-29/software-espiao-e-monitoramento-secreto-de-dispositivos-de-dados-e-comunicacao/