

# DOS PROGRAMAS ESPIÕES NO ORDENAMENTO BRASILEIRO

## SPY PROGRAMS IN THE BRAZILIAN ORDER

Artigo submetido em 24 de setembro de 2024

Artigo aprovado em 28 de setembro de 2024

Artigo publicado em 30 de setembro de 2024

### Cognitio Juris

Volume 14 - Número 56 - Setembro de 2024

ISSN 2236-3009

### Autor(es):

Glauce Teodoro Martins Dias[1]

**RESUMO:** Este artigo disserta acerca da utilização de programas maliciosos pelos órgãos e agentes públicos na persecução penal impulsionado pelo ajuizamento da Arguição de Descumprimento de Preceito Fundamental 1143 (ADPF 1143) pela Procuradoria-Geral da República e a pesquisa do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) sobre *hacking* governamental. Dessa forma, analisamos os direitos fundamentais e humanos que envolvem a matéria, a atuação e a disseminação dos também chamados *malwares* nos equipamentos tecnológicos pessoais, a lacuna da legislação no país, a ADPF 1143, a partir de material bibliográfico, com o intuito de alcançar entendimento acerca da necessidade ou desnecessidade da regulamentação desses programas no país. O artigo conclui que, diante

do cenário observado, não só de crimes domésticos, mas de crimes que extrapolam o território nacional ou mesmo que ameaçam a soberania do país, faz-se necessária e urgente a regulamentação pelo Estado dos programas de espionagem, contudo, com critérios bastante definidos que observem direitos fundamentais e humanos já consagrados, além da possibilidade de se estabelecerem novos direitos.

**Palavras-chave:** Malwares; espionagem; Direitos Humanos; processo penal, ADPF 1143, órgãos públicos.

**RESUMEN:** Este artículo analiza el uso de programas maliciosos por parte de organismos y agentes públicos en la persecución penal impulsado por la presentación de la Denuncia de Incumplimiento del Precepto Fundamental 1143 – ADPF 1143 – por parte del Ministerio Público y la investigación del Instituto de Investigaciones en Derecho y Tecnología de Recife (IP.rec) sobre piratería gubernamental. De esta manera, analizamos los derechos fundamentales y humanos que involucran la materia, la acción y difusión del llamado malware en equipos tecnológicos personales, el vacío de legislación en el país, la ADPF 1143, con base en material bibliográfico, para llegar a una comprensión sobre la necesidad o innecesaria regulación de estos programas en el país.

**Palabras clave:** Malware; espionaje; derechos humanos; procedimiento penal; ADPF 1143; organismos públicos.

## **1 INTRODUÇÃO**

A legislação brasileira atual não dá espaço para a utilização de programas espões na persecução penal ou qualquer outra forma de uso deles pelo Estado, em que pese os argumentos daqueles que sustentam a necessidade de sua prática em razão do avanço tecnológico. Contudo, o ajuizamento de Ação Direta de Inconstitucionalidade por Omissão com Pedido de Medida Cautelar pela Procuradoria Geral da República e, posteriormente, sua conversão para Arguição de Descumprimento de Preceito Fundamental 1143,<sup>[1]</sup> a fim de

provocar o Legislativo a atuar no assunto, tem gerado intensa discussão.

Com efeito, não é de hoje que a mídia tem veiculado notícias[2] do uso de programas espões no território brasileiro por órgãos e agentes públicos, ainda que estes não tenham qualquer autorização legal para fazê-lo, e causado espanto aos cidadãos brasileiros que tomam conhecimento da informação, gerando, com isso, celeuma entre os operadores de direito. Tal cenário também já se verificou em outros países,[3] sendo fonte de discussão em outras cortes constitucionais.

Em novembro de 2022, o Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) divulgou importantes dados da pesquisa feita no Brasil acerca de contratos de fabricantes e representantes comerciais de *malwares* com a Administração Pública, revelando, assim, a prática do *hacking*, no país, por agentes e órgãos públicos.[4]

Os também chamados *malwares* possibilitam o acesso irrestrito a dispositivos móveis e fixos de instituições e de pessoas humanas, podendo alcançar informações em processamento ou armazenadas. Tal ação fere os direitos fundamentais consagrados na Constituição Federal de 1988 e que são irradiação no ordenamento jurídico brasileiro de Direitos Humanos.

A evolução tecnológica alcançada pela civilização atual revolucionou o modo de vida da pessoa humana, impactando em todas as suas dimensões. Atividades profissionais e estudantis se desenvolvem em ambiente virtual, assim como os relacionamentos — sejam amigáveis, amorosos ou familiares — são iniciados e/ou mantidos por aplicativos de relacionamento — WhatsApp, Instagram, Facebook, TikTok etc. — em espaços virtuais.

Da mesma forma, o avanço tecnológico impactou profundamente as atividades estatais e a forma como o Estado efetiva os serviços públicos — agendamento e atendimento de consultas médicas *online*; atendimentos *online* da Defensoria; audiências virtuais etc. Isso acabou gerando até mesmo a necessidade de proteção às pessoas vulneráveis

tecnologicamente,[5] ou seja, aquelas que, por não terem acesso a ferramentas tecnológicas, podem não se beneficiar de serviços ou até mesmo não os acessar, casos sejam impostos apenas de forma virtual.

De um lado, os defensores desse acesso remoto irrestrito aos dispositivos fixos e móveis sustentam que tal medida é necessária, já que os agentes do crime também evoluíram tecnologicamente. Desse modo, impedir a ação estatal, nesse sentido, seria manter os poderes públicos em condição desigual na persecução penal. De outro lado, os defensores do não acesso questionam o ataque a direitos fundamentais do cidadão no Estado brasileiro.

Em um passado recente, o uso de tal ferramenta tecnológica, também recente, estava vinculado à ação de criminosos,[6] dado o potencial de invasão e de possibilidade de causar danos aos invadidos. Contudo, no atual cenário, observa-se também a sua vinculação aos poderes estatais, tanto em nível nacional como internacional e global — motivo pelo qual este estudo se faz ainda mais necessário.

Este artigo, tomando por verdadeira a lacuna legislativa para tal prática estatal, objetiva, a partir de pesquisa de material bibliográfico, dissertar sobre os seguintes assuntos: os direitos humanos e fundamentais envolvidos na questão; os programas de espionagem e a sua aplicação; a lacuna quanto à matéria na legislação brasileira; e a Arguição de Descumprimento de Preceito Fundamental 1143.

A finalidade deste artigo é, então, o entendimento das variáveis — *malwares* — que compõem esse cenário, seus impactos sobre os direitos fundamentais dos cidadãos, especialmente os que tutelam o direito de privacidade/intimidade e a inviolabilidade do sigilo das comunicações pessoais, a fim de se concluir, ou não, pela necessidade de referida normatização pelo Estado e, caso essa primeira possibilidade se mostre afirmativa, indicar por meio de quais parâmetros isso deve se realizar.

## **2 DIREITOS FUNDAMENTAIS E HUMANOS**

Os direitos fundamentais, no Brasil, estão previstos no artigo 5º da Constituição Federal de 1988[7] (CF/88) e têm, como escopo, a proteção da pessoa humana frente ao Estado, que ora deve agir para protegê-la, ora deve deixar de atuar para protegê-la. Não se trata de direitos taxativos, mas que podem ser ampliados por força do regime e dos princípios adotados no país.

Tais direitos são irradiação dos Direitos Humanos no território brasileiro e resgatam períodos históricos da humanidade que culminaram na construção histórica dos direitos humanos. Norberto Bobbio[8] nos ensina este caráter histórico de referidos direitos:

os direitos do homem, por mais fundamentais que sejam, são direitos históricos, ou seja, nascidos em certas circunstâncias, caracterizadas por lutas em defesa de novas liberdades contra velhos poderes, e nascidos de modo gradual, não todos de uma vez e nem de uma vez por todas.

É importante rememorarmos aqui a Carta Magna de 1215 que também nos remete a um desses importantes momentos da história: o período em que o absolutismo monárquico estabelecia o rei como uma figura divina na terra, cabendo a ele acusar, julgar e condenar; ou absolver seus súditos, conforme seus próprios interesses e convicções. O rei era irresponsável por seus atos. Não existia, portanto, uma normativa prévia que determinasse quais os direitos ou deveres dos súditos e muito menos os do rei.

A sociedade medieval europeia compunha-se de clero, nobreza e povo. Na referida Carta, o Rei João Sem-Terra, pressionado pela instabilidade da época e pela nobreza, se comprometia a respeitar as leis.[9] Ainda que isso significasse dar direitos a pequeno e determinado grupo, trata-se de importante embrião para alcançar-se, ao longo da evolução das civilizações, a limitação da atuação do Estado, impondo-lhe deveres e responsabilidades, e a declaração de direitos aos governados.

Com isso, é possível observar o movimento político e jurídico que culminou, ao longo

da história, nas constituições escritas, nas quais se verifica a imposição de limitação do poder dos Estados.

Também as duas guerras mundiais e os holocaustos impostos — na Primeira, aos armênios; na Segunda, a judeus, negros, homossexuais, ciganos e pessoas com limitações físicas — têm profundo impacto na Declaração Universal de Direitos do Homem, em 1948.<sup>[10]</sup> Nela, tais direitos ganham a característica de universalidade, ecoando, até hoje, nos ordenamentos jurídicos dos Estados.

Dessa forma, são direitos dos cidadãos a privacidade, a intimidade e a inviolabilidade do sigilo das comunicações pessoais, todos eles sendo previstos na CF/88 e tendo sido irradiados pela construção histórica dos direitos humanos. Tais direitos são ofendidos quando há a intrusão de programas de monitoramento em equipamentos pessoais. Na experiência alemã de enfrentamento aos programas de espionagem, surge até mesmo um novo direito: o da integridade e confidencialidade que nos remete novamente à Bobbio:

[...] o fato mesmo de que a lista desses direitos esteja em contínua ampliação não só demonstra que o ponto de partida do hipotético estado de natureza perdeu toda a plausibilidade, mas nos deveria tornar conscientes de que o mundo das relações sociais de onde essas exigências deriva é muito mais complexo, e de que, para a vida e para a sobrevivência dos homens, nessa nova sociedade, não bastam os chamados direitos fundamentais, como os direitos à vida, à liberdade e à propriedade.

Dessa forma, em que pese a necessidade de o Estado se ajustar ao avanço tecnológico a fim de cumprir com efetividade as suas competências, isso não pode ser feito sem reserva legal e sem reserva jurisdicional. Se ocorrer dessa forma, haverá prejuízo aos referidos direitos e a ruptura com o Estado democrático de direito.

A Declaração Universal dos Direitos Humanos eleva a democracia como o regime mais adequado para o exercício dos Direitos Humanos. A sua ruptura, no entanto, refletiria na

fragilidade desses direitos.

### **3 PROGRAMAS-ESPIÕES**

No dia 25 de janeiro de 2024, uma reportagem veiculada pelo portal de notícia G1,<sup>[11]</sup> assim como outros importantes portais do país, afirmava que a Agência Brasileira de Inteligência (Abin) monitorou irregularmente políticos, policiais, jornalistas e juízes. Isso havia sido feito por meio do *software* israelense de espionagem First Mile.

O monitoramento efetuado pela referida agência de inteligência é possível de ser feito por meio de programas de espionagem popularizados nas últimas décadas. Embora, neste exemplo, seja observado o mau uso político da referida ferramenta em desfavor de autoridades e de pessoas públicas, seu uso não está restrito a atividades de perseguição política ou de inteligência, podendo, por exemplo, ser feito contra pessoas comuns na esfera penal.

Tais programas são passíveis de instalação física ou mesmo remota, sendo esta instalação a mais comum, tanto em dispositivos móveis quanto nos fixos. O objetivo de tal ação é permitir o acesso irrestrito a arquivos processados ou em processamento, fotos, vídeos e outros materiais, com a possibilidade de até mesmo captar imagens e sons em tempo real no raio permitido pelos equipamentos invadidos.

Os *malwares* infectam o dispositivo hospedeiro, utilizando-se de vulnerabilidades de segurança apresentadas pelos próprios dispositivos e de e-mails enviados à pessoa-alvo. Eles também podem ser disseminados pela rede de internet.

Nota-se que as empresas de tecnologia produzem os dispositivos que se revelam vulneráveis e devem/deveriam ser atualizados. Não obstante isso, pela lógica do mercado capitalista, também se observa a disseminação de ofertas — *deep web* ou *dark web* — desses *malwares* que, conforme alertado, valem-se dessas vulnerabilidades.

Outro ponto a ser observado é que os programas de espionagem, os quais são largamente adquiridos pelo Estado brasileiro,[12] são provenientes de empresas internacionais. Dessa forma, é possível questionar se o próprio país poderia estar sendo alvo de espionagem ao utilizar tais ferramentas, levando-se em conta, por exemplo, as denúncias já apresentadas por Edward Snowden.[13]

Os programas espiões são, portanto, parte da enorme evolução tecnológica alcançada pela humanidade nas últimas décadas. Tal avanço parece ser irreversível, devendo o Estado brasileiro ajustar-se a essa nova realidade. Como toda ferramenta, essa tecnologia pode ser usada não só para fins lícitos, como também para fins ilícitos — razão pela qual é imprescindível a regulamentação delas.

Do exposto, fica evidente que a realidade posta transcende a questão de Direitos Humanos e passa por uma discussão necessária acerca da ética na tecnologia. No entanto, para além da questão da ética, fica ainda mais evidente que o Brasil precisa de leis e políticas públicas sérias de fomento ao estudo, à pesquisa e à criação de tecnologia no país.

#### **4 DA LEGISLAÇÃO**

Conforme já afirmado, os direitos e as garantias fundamentais estão previstos no artigo 5º da Constituição da República Federativa do Brasil. As normas que se referem à privacidade, à intimidade e à inviolabilidade do sigilo das comunicações estão situadas nos incisos X e XII:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação;

[...]

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Mais uma vez, é preciso considerar que não há uma legislação própria no país para o uso de *malwares*. Houve, contudo, regulamentações, tais como a Lei de Interceptação Telefônica, a Lei de Investigação de Organizações Criminosas e o Estatuto da Criança e do Adolescente. Elas preveem hipóteses em que será dada a autorização judicial para a interceptação do fluxo de comunicações em sistemas de informática e telemática e, no caso das duas últimas leis, a figura do agente infiltrado virtual.

A Lei n.º 9296/96, também conhecida como Lei de Interceptação, regulamenta o artigo XII, parte final do artigo 5º da CF/88, reproduzido anteriormente. Na referida lei, anterior ao impacto do surgimento desses programas maliciosos, está abarcada a interceptação do fluxo de comunicações em sistemas de informática e telemática.[\[14\]](#)

Ocorre que a lei em comento tem um potencial invasivo e de lesividade muito menor do que aquele possibilitado pelos programas de espionagem. Ainda que haja a inclusão do artigo 10-A, com redação dada pela Lei n.º 13964, para incluir a possibilidade de captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, até mesmo sem determinação de ordem judicial, tais determinações não têm o condão de normatizar tais práticas de espionagem, uma vez que os *malwares* proporcionam intrusão muito maior.

Também a Lei n.º 12850/2013, a qual define a organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção de prova, as infrações penais correlatas e o procedimento criminal, é apontada como normatização suficiente para o agir estatal. No entanto, da mesma forma que a lei anterior, o potencial de intrusão é muito menor do que os referidos programas.

Faz-se importante também observar a Lei n.º 12.965/14 (Marco Civil da Internet), a qual estabelece os princípios, as garantias, os direitos e os deveres para o uso da internet no Brasil. É preciso destacar o artigo 2º da referida lei, o qual eleva, no inciso II, como um dos fundamentos do uso da internet no Brasil, os direitos humanos:[15]

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

[...]

II – os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

[...].

Também o artigo 7º da mesma lei[16] reforça os direitos fundamentais aos usuários da internet no país, restando claro que a lei em comento está em consonância com o Estado democrático de direito:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

[...]

Da mesma forma, o artigo 8º da referida Lei[17] corrobora as garantias do direito à privacidade e à liberdade de expressão nas comunicações:

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

Ainda pode-se citar a Lei n.º 13709,[18] a qual data de quatro anos após o Marco Civil da Internet e que dispõe sobre a proteção de dados pessoais, também conhecida como LGPD. Ela também tem como fundamentos, entre outros, o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; e os Direitos Humanos.

Aury Lopes Junior explica que:

(...) meio de obtenção de prova, ou *mezzi di ricerca dela prova*, como denominam os italianos, são instrumentos que permitem obter-se, chegar-se à prova. Não é propriamente “a prova”, senão meios de obtenção.[19]

Assim, observa-se que os *malwares* constituem meio atípico de prova no processo penal brasileiro e, por isso, não cabe sua utilização pelas polícias ou pelos ministérios públicos, seja em qualquer nível da federação. Além disso, seu uso por outros órgãos e agentes públicos não é democraticamente possível, ressaltando ainda que, nestes últimos, não se encontra

nem sequer a competência investigativa.

Maria Sylvia Zanella Di Pietro assevera:

Segundo o Princípio da Legalidade, a Administração Pública só pode fazer o que a lei permite. No âmbito das relações entre particulares, o princípio aplicável é o da autonomia da vontade.

O referido princípio está estritamente vinculado à observância dos direitos individuais pelo Estado democrático de direito.

Portanto, a pesquisa, no ordenamento jurídico brasileiro, resulta em uma negativa de lei para o uso de programas de espionagem. Desse modo, estando o Estado, pois, restrito a agir na presença da lei, sendo proibida a atuação sem lei, deve haver responsabilização de quem agiu ou age em desconformidade com ela.

## **5 DA ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 1143 - ADPF 1143**

O ajuizamento da Ação de Arguição de Descumprimento de Preceito Fundamental 1143, inicialmente uma Ação Direta de Inconstitucionalidade por Omissão com Pedido de Medida Cautelar pela Procuradoria-Geral, evidencia a ausência de legislação no país para a utilização dos programas de espionagem pelo Estado brasileiro.

Na referida ADPF, a Procuradoria-Geral da República vem pedir ao Supremo Tribunal Federal que fixe prazo para o Legislativo agir na regulamentação do uso de programas de espionagem no país, uma vez que este uso já é observado:

É que, a partir dos mais recentes avanços tecnológicos, houve uma proliferação global de ferramentas de intrusão virtual, utilizadas no âmbito de serviços de inteligência e de órgãos de repressão estatais, para a vigilância remota, secreta e invasiva de dispositivos móveis de comunicação digital, sob pretexto de combate ao terrorismo e ao crime organizado.[\[20\]](#)

Com efeito, a ADPF 1143 está em tramitação no Supremo Tribunal Federal sob relatoria do Ministro Cristiano Zanin. Ele chamou audiências públicas nos últimos dias 10 e 11 de junho de 2024, a fim de se aprofundar a discussão sobre a referida matéria, a qual contou com diversos *amicus curiae*.

A petição da Procuradoria Geral da República revela preocupação com a aquisição de programas de espionagem internacionais, tais como o Pegasus, um *malware* de criação israelense que detém grande potencial de intrusão em dispositivos informáticos.

Tal preocupação já foi revelada anteriormente pelo alto Comissariado da ONU.<sup>[21]</sup> Esse órgão classificou a situação de programas de espionagem em prática, especialmente o Pegasus, como algo alarmante, uma vez que deixa todos os cidadãos vulneráveis.

## 6 CONCLUSÃO

Inicialmente, nota-se que a questão do uso de *malwares* no Brasil e no mundo transcende a violação de direitos humanos e fundamentais, tratando-se do abandono da ética no avanço humano na área de tecnologia. No entanto, o que causa enorme espanto é que a ADPF 1143 é ajuizada ao Supremo Tribunal Federal em razão da atuação de órgãos e de agentes públicos em desconformidade com o ordenamento jurídico, ou seja, agindo quando não têm permissão para atuar.

Diante de todo cenário exposto, é forçoso considerar que a prática de *hacking* governamental estatal que se dá aqui é violadora de direitos fundamentais e humanos dos cidadãos brasileiros. O Estado não é irresponsável, logo, só pode agir quando vinculado à lei. Portanto, quando se afasta desta, deve haver a promoção de responsabilidades, pois, de outro modo, estaremos fatalmente diante de uma democracia muito frágil e, por isso mesmo, muito próxima da ruptura do Estado democrático de direito. O Estado não pode desrespeitar direitos fundamentais a pretexto de efetivar outros direitos.

O avanço tecnológico e seu profundo impacto no modo de vida social e no desenvolvimento das competências estatais parece irreversível. Ainda que o uso de *malwares* não pareça o mais adequado e democrático — diante do cenário observado, não só de crimes domésticos, mas de crimes que extrapolam o território nacional ou mesmo que ameaçam a soberania do país —, torna-se urgente e necessária a regulamentação pelo Estado dos programas de espionagem. No entanto, isso deve ser feito com base em critérios bastante definidos, os quais observem direitos fundamentais e humanos já consagrados, além da possibilidade de serem estabelecidos novos direitos.

Da mesma forma, a fim de se observar a segurança do Estado, a lei deve prever o desenvolvimento urgente de programas de monitoramento pelo próprio Estado brasileiro para uso tanto na persecução penal no país, como também para sua agência de inteligência. A experiência dos últimos anos tem demonstrado que não é cauteloso utilizar-se unicamente de *malwares* internacionais. Ainda que isso possa não ser uma tarefa fácil, não deixa de ser uma ação possível. É preciso ter em mente que o desconhecimento tecnológico faz o país refém de outras nações e, assim, passível de sofrer uma nova colonização.

Dessa forma, por meio da decisão de Arguição de Descumprimento de Preceito Fundamental 1143, o Brasil tem, pela sua Corte Constitucional, a oportunidade de se estabelecer, no mundo, como um verdadeiro Estado democrático de direito. Nosso país, portanto, pode estar profundamente comprometido com os mais nobres direitos e garantias do cidadão, ou, ao contrário disso, mostrar o quando ainda é uma democracia muito jovem e por demais frágil.

## REFERÊNCIAS

AMORIM, Daniela. Brasil tinha 7,3 milhões de lares sem internet e 28,2 milhões de excluídos digitais em 2021. **Estadão**, São Paulo, 16 set. 2022. Economia. Disponível em: <https://www.estadao.com.br/economia/brasil-exclusao-digital-2021/#:~:text=Exclu%C3%ADdos%20digitais%20representavam%2015%2C3,de%20idade%2C%20segundo%20o%20IBGE&t>

ext=RIO%20%2D%20A%20pandemia%20de%20covid,rede%20em%20casa%20em%202021.  
Acesso em: 16 jun. 2024.

BOBBIO, Norberto. **A era dos direitos**. Tradução de Carlos Nelson Coutinho. 30. reimp. Rio de Janeiro: Atlas, 2022. P. 5.

BRASIL. Conselho Nacional de Justiça. Recomendação n.º 101, de 12 de julho de 2021. **Diário da Justiça Eletrônico**, Brasília, DF, 12 jul. 2021. Disponível em:

<https://atos.cnj.jus.br/files/original1851022021071460ef3216bda0d.pdf>. Acesso em: 22 jun. 24.

BRASIL. Conselho Nacional de Justiça. Portaria n.º 12, de 23 de janeiro de 2006. **Diário da Justiça**, Brasília, DF, 23 jan. 2006. Disponível em:

[https://atos.cnj.jus.br/files//portaria/portaria\\_12\\_23012006\\_17102012182955.pdf](https://atos.cnj.jus.br/files//portaria/portaria_12_23012006_17102012182955.pdf). Acesso em: 22 jun. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em:

[https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88\\_Livro\\_EC91\\_2016.pdf](https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf). Acesso em: 16 jun. 2024.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Brasília, DF, 77, 24 abr. 2014. Disponível em:

[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 28 set. 2024.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). **Diário Oficial da União**. Brasília, DF, 157, 15 ago. 2018. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=529&pagina=1&data=15/08/2018&totalArquivos=64>. Acesso em: 28 set. 2024.

BRASIL. Supremo Tribunal Federal. ADPF 1143. Processo Eletrônico Público Medida Liminar, Número Único: 0013845-73.2024.1.00.0000. Distrito Federal, Relator: Min. Cristiano Zanin, Requerente: Procuradora-Geral da República, Interessado: Congresso Nacional, Procurador: Advogado-Geral da União, Amicus Curiae: Associação InternetLab de Pesquisa em Direito e Tecnologia. Disponível em:

<https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814>. Acesso em: 10 fev. 2025.  
Acesso em: 17 jun. 2024.

COMPARATO, Fabio Konder. **A afirmação histórica dos direitos humanos**. 12. ed. São Paulo: Saraiva Educação, 2019. p. 91.

COUTINHO, Mateus. Especialista alerta para riscos nos usos de programas de espionagem no Brasil. **Brasil de Fato**, DF, 6 jan. 2024. Política, Inteligência. Disponível em:  
<https://www.brasildefato.com.br/2024/01/06/especialista-alerta-para-riscos-nos-usos-de-programas-de-espionagem-no-brasil>. Acesso em: 10 jun.

FIRST Mile: o que se sabe sobre o software espião usado pela Abin. **G1**, Rio de Janeiro, 25 jan. 2024. Tecnologia. Disponível em:  
<https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml>. Acesso em: 10 jun. 2024.

GRINBERG, Felipe. Inteligência da PM monitorou atuação de políticos e advogado de Direitos Humanos na favela do Jacarezinho. **O Globo 100**, Rio de Janeiro, 16 maio 2024. Rio. Acesso em: 10 jun. 2024.

GRUPO hacker acusa governo alemão de criar software para espionar cidadãos do país. **Uol**, [S. /], 10 out. 2011. Notícias, tecnologia. Disponível em:

<https://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/10/10/grupo-hacker-acusa-governo-alemao-de-criar-software-espiao-para-vigiar-cidadaos-do-pais.jhtm>. Acesso em: 15 jun. 2024.

LOPES Jr., Aury. **Direito Processual Penal**. 15. ed. São Paulo: Saraiva Educação, 2018. p. 227.

LUCENA, André. Há 10 anos, Edward Snowden revelou um mundo sitiado pela espionagem americana. **Carta Capital**, São Paulo, 6 jun. 2023. Disponível em: <https://www.cartacapital.com.br/mundo/ha-10-anos-edward-snowden-revelou-um-mundo-sitiado-pela-espionagem-americana/>. Acesso em: 19 jun. 2024.

NACIONES UNIDAS. Derechos Humanos. **Suposta espionagem com software Pegasus preocupa ONU**. 19 jul. 2021. Disponível em: <https://acnudh.org/pt-br/los-gobiernos-deben-cesar-de-inmediato-el-uso-de-tecnologias-de-vigilancia-que-violen-los-derechos-humanos-bachelet/>. Acesso em: 28 set.

NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Disponível em: <https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humanos>. Acesso em: 28 set. 2024.

PAULO, Vicente; ALEXANDRINO, Marcelo. **Direito Constitucional descomplicado**. 3. ed., rev. e atual. Rio de Janeiro: Forense; São Paulo: Método: 2008. p. 124. RAMIRO, André (coord.); AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos Cesar M. **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil**. Recife: IP.rec, 2022.

---

[1] BRASIL. Supremo Tribunal Federal. ADPF 1143. Processo Eletrônico Público Medida Liminar, Número Único: 0013845-73.2024.1.00.0000. Distrito Federal, Relator: Min. Cristiano Zanin, Requerente: Procuradora-Geral da República, Interessado: Congresso Nacional,

Procurador: Advogado-Geral da União, Amicus Curiae: Associação InternetLab de Pesquisa em Direito e Tecnologia. Disponível em:

<https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814>. Acesso em: 10 fev. 2025.  
Acesso em: 17 jun. 2024.

[2] GRINBERG, Felipe. Inteligência da PM monitorou atuação de políticos e advogado de Direitos Humanos na favela do Jacarezinho. **O Globo 100**, Rio de Janeiro, 16 maio 2024. Rio. Acesso em: 10 jun. 2024.

COUTINHO, Mateus. Especialista alerta para riscos nos usos de programas de espionagem no Brasil. **Brasil de Fato**, DF, 6 jan. 2024. Política, Inteligência. Disponível em: <https://www.brasildefato.com.br/2024/01/06/especialista-alerta-para-riscos-nos-usos-de-programas-de-espionagem-no-brasil>. Acesso em: 10 jun.

FIRST Mile: o que se sabe sobre o software espião usado pela Abin. **G1**, Rio de Janeiro, 25 jan. 2024. Tecnologia. Disponível em: <https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml>. Acesso em: 10 jun. 2024.

[3] GRUPO hacker acusa governo alemão de criar software para espionar cidadãos do país. **Uol**, [S. l.], 10 out. 2011. Notícias, tecnologia. Disponível em: <https://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/10/10/grupo-hacker-acusa-governo-alemao-de-criar-software-espiao-para-vigiar-cidadaos-do-pais.jhtm>. Acesso em: 15 jun. 2024.

[4] RAMIRO, André (coord.); AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos Cesar M. **Mercadores da insegurança**: conjuntura e riscos do *hacking* governamental no Brasil. Recife: IP.rec, 2022.

[5] AMORIM, Daniela. Brasil tinha 7,3 milhões de lares sem internet e 28,2 milhões de

excluídos digitais em 2021. **Estadão**, São Paulo, 16 set. 2022. Economia. Disponível em: <https://www.estadao.com.br/economia/brasil-exclusao-digital-2021/#:~:text=Exclu%C3%ADdos%20digitais%20representavam%2015%2C3,de%20idade%2C%20segundo%20o%20IBGE&text=RIO%20%2D%20A%20pandemia%20de%20covid,rede%20em%20casa%20em%202021>. Acesso em: 16 jun. 2024.

[6] BRASIL. Conselho Nacional de Justiça. Recomendação n.º 101, de 12 de julho de 2021. **Diário da Justiça Eletrônico**, Brasília, DF, 12 jul. 2021. Disponível em: <https://atos.cnj.jus.br/files/original1851022021071460ef3216bda0d.pdf>. Acesso em: 22 jun. 24.

BRASIL. Conselho Nacional de Justiça. Portaria n.º 12, de 23 de janeiro de 2006. **Diário da Justiça**, Brasília, DF, 23 jan. 2006. Disponível em: [https://atos.cnj.jus.br/files//portaria/portaria\\_12\\_23012006\\_17102012182955.pdf](https://atos.cnj.jus.br/files//portaria/portaria_12_23012006_17102012182955.pdf). Acesso em: 22 jun. 2024.

[7] BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: [https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88\\_Livro\\_EC91\\_2016.pdf](https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf). Acesso em: 16 jun. 2024.

[8] BOBBIO, Norberto. **A era dos direitos**. 30. reimp. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Atlas, 2022. p. 5.

[9] “[...] a Magna Carta deixa implícito pela primeira vez, na histórica política medieval, que o rei acha-se naturalmente vinculado pelas próprias leis que edita. Quinhentos anos antes, Santo Isidoro (560-636), bispo de Sevilha, já havia defendido a ideia de que o príncipe devia submeter-se às leis que ele próprio promulgara, pois “só quando também ele respeita as leis, pode-se esperar que elas sejam obedecidas por todos” (Sententiae III, 51.4). COMPARATO,

Fabio Konder. **A afirmação histórica dos direitos humanos**. 12. ed. São Paulo: Saraiva Educação, 2019. p. 91.

[10] NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Disponível em: <https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humanos>. Acesso em: 28 set. 2024.

[11] Ver nota 3.

[12] RAMIRO, André (coord.). Ver nota 5.

[13] LUCENA, André. Há 10 anos, Edward Snowden revelou um mundo sitiado pela espionagem americana. **Carta Capital**, São Paulo, 6 jun. 2023. Disponível em: <https://www.cartacapital.com.br/mundo/ha-10-anos-edward-snowden-revelou-um-mundo-sitiado-pela-espionagem-americana/>. Acesso em: 19 jun. 2024.

[14] “A lei n.º 9.296/1996 veio legitimar a interceptação das comunicações telefônicas como meio de prova, estendendo também a sua regulação à interceptação do fluxo de comunicações em sistemas de informática e telemática (combinação dos meios de comunicação com informática) — e-mail (correio eletrônico), fax e outros — nos mesmos moldes em que autorizada constitucionalmente a interceptação telefônica propriamente dita, e para os mesmos fins.” PAULO, Vicente; ALEXANDRINO, Marcelo. **Direito Constitucional descomplicado**. 3. ed., rev. e atual. Rio de Janeiro: Forense; São Paulo: Método: 2008. p. 124.

[15] BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Brasília, DF, 77, 24 abr. 2014. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 28 set. 2024.

[16] BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Brasília, DF, 77, 24 abr. 2014. Disponível em:

[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 28 set. 2024.

[17] *Ibid.*

[18] BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). **Diário Oficial da União**. Brasília, DF, 157, 15 ago. 2018. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=529&pagina=1&data=15/08/2018&totalArquivos=64>. Acesso em: 28 set. 2024.

[19] LOPES Jr., Aury. **Direito Processual Penal**. 15. ed. São Paulo: Saraiva Educação, 2018. p. 227.

[20] BRASIL. Supremo Tribunal Federal. ADPF 1143. Processo Eletrônico Público Medida Liminar, Número Único: 0013845-73.2024.1.00.0000. Distrito Federal, Relator: Min. Cristiano Zanin, Requerente: Procuradora-Geral da República, Interessado: Congresso Nacional, Procurador: Advogado-Geral da União, Amicus Curiae: Associação InternetLab de Pesquisa em Direito e Tecnologia. Disponível em:

<https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814>. Acesso em: 10 fev. 2025. Acesso em: 28 set. 2024.

[21] NACIONES UNIDAS. Derechos Humanos. **Suposta espionagem com software Pegasus preocupa ONU**. 19 jul. 2021. Disponível em:

<https://acnudh.org/pt-br/los-gobiernos-deben-cesar-de-inmediato-el-uso-de-tecnologias-de-vigilancia-que-violen-los-derechos-humanos-bachelet/>. Acesso em: 28 set. 2024.