XII CONGRESSO RECAJ-UFMG

ESTADO, GOVERNANÇA, DEMOCRACIA E VIRTUALIDADES

VALTER MOURA DO CARMO

WILSON DE FREITAS MONTEIRO

MARCO ANTÔNIO SOUSA ALVES

E79
Estado, governança, democracia e virtualidades [Recurso eletrônico on-line] organização XII Congresso RECAJ-UFMG: UFMG – Belo Horizonte;

Coordenadores: Valter Moura do Carmo, Marco Antônio Sousa Alves e Wilson de Freitas Monteiro – Belo Horizonte: UFMG, 2021.

Inclui bibliografia
ISBN: 978-65-5648-369-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: As novas fronteiras tecnológicas do acesso à justiça e os direitos fundamentais digitais em perspectiva crítica.
1. Direito e Tecnologia. 2. Acesso à justiça. 3. Direitos fundamentais digitais. I. XII Congresso RECAJ-UFMG (1:2021: Belo Horizonte, MG).

CDU: 34

XII CONGRESSO RECAJ-UFMG

ESTADO, GOVERNANÇA, DEMOCRACIA E VIRTUALIDADES

Apresentação

É com muita alegria que o Programa RECAJ-UFMG – Acesso à Justiça pela Via dos Direitos e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais, a SKEMA Business School Brasil e o Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI tornam público à comunidade científica o conjunto dos oito livros produzidos a partir das discussões dos Grupos de Trabalho do XII Congresso RECAJ-UFMG, que teve por tema central "As novas fronteiras tecnológicas do acesso à justiça e os direitos fundamentais digitais em perspectiva crítica".

As discussões nos Grupos de Trabalho ocorreram em ambiente virtual ao longo dos dias 25 e 26 de novembro de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área, além de cento e quarenta e dois pesquisadoras e pesquisadores inscritos no total, provenientes de treze Estados da federação (Alagoas, Amazonas, Bahia, Distrito Federal, Espírito Santo, Minas Gerais, Piauí, Paraná, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe e São Paulo). Marcando um momento em que a terrível pandemia da COVID-19 finalmente dá sinais de apaziguamento, o que somente foi possível por conta da ciência, da vacinação em massa e do trabalho valoroso de todos os profissionais do Sistema Único de Saúde, o evento trouxe, após hiato de quase dois anos, painéis científicos presenciais na nova (e bela) sede da SKEMA Business School Brasil no bairro Savassi em Belo Horizonte-MG.

Os oito livros compõem o produto principal deste congresso, que há mais de uma década tem lugar cativo no calendário científico nacional. Trata-se de coletânea composta pelos cento e seis trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito grupos de trabalho geraram cerca de seiscentas páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre diversos temas jurídicos e sua relação com a tecnologia: Acesso à Justiça e Tecnologias do Processo Judicial; O Direito do Trabalho no século XXI; Estado, Governança, Democracia e Virtualidades; e Tecnologias do Direito Ambiental e da Sustentabilidade. No dia 26, serão abordados os seguintes temas: Formas de Solução de Conflitos e Tecnologia; Direitos Humanos, Gênero e Tecnologias do Conhecimento; Inteligência Artificial, Startups, Lawtechs e Legaltechs; e Criminologia e cybercrimes.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de vinte e quatro proeminentes pesquisadores ligados a renomadas instituições de ensino superior do país, dentre eles alguns mestrandos e doutorandos do próprio Programa de Pós-graduação em Direito da UFMG, que indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores e pós-graduandos que coordenaram os trabalhos.

Nesta esteira, a coletânea que ora se apresenta é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e com o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. Importante lembrar, ainda, da contribuição deste congresso com a formação de novos pesquisadores na seara interdisciplinar entre o Direito e a tecnologia, uma vez que o número de graduandos que apresentaram trabalhos de qualidade foi expressivo. Destaca-se a presença maciça de pesquisadores do Estado do Amazonas, especialmente os orientandos do Professor Doutor Valmir César Pozzetti vinculados à Universidade Federal do Amazonas e à Universidade Estadual do Amazonas.

O Programa RECAJ-UFMG, que desde 2007 atua em atividades de ensino, pesquisa e extensão em acesso à justiça pela via dos direitos e soluções de conflitos, nos últimos anos adota linha investigativa a respeito da conexão entre o acesso à justiça e a tecnologia, com pesquisas de mestrado e doutorado concluídas. Em 25 de junho deste ano, celebrou um termo de cooperação técnica com o Grupo de Pesquisa Normative Experimentalism and Technology Law Lab – NEXT LAW LAB da SKEMA Business School Brasil, que prevê o intercâmbio permanente das pesquisas científicas produzidas pelo NEXT LAW LAB e pelo Programa RECAJ-UFMG na área do Direito e Tecnologia, especialmente as voltadas ao estudo do acesso tecnológico à justiça e a adoção da inteligência artificial no campo do Direito. Desta parceria nascerá, seguramente, novos projetos importes para a comunidade científica deste campo.

Com o sentimento de dever cumprido, agradecemos a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 28 de novembro de 2021.

Prof. Drª. Adriana Goulart de Sena Orsini

Coordenadora do Programa RECAJ-UFMG

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School Brasil

Prof. Dr. Caio Augusto Souza Lara

Professor da SKEMA Business School Brasil e Pós-doutorando vinculado ao Programa RECAJ-UFMG

ESPIÃO PEGASUS À LUZ DOS DIREITOS HUMANOS, DIREITO À PRIVACIDADE E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

PEGASUS SPY IN LIGHT OF HUMAN RIGHTS, RIGHT TO PRIVACY AND THE GENERAL PERSONAL DATA PROTECTION LAW (LGPD)

Fernanda Daniele de Abreu Pereira [1]
Guilherme Augusto Dias Reis [2]

Resumo

O presente trabalho tem como objetivo analisar o caso espião Pegasus à luz do ordenamento brasileiro. Um spyware desenvolvido para venda e uso por agências governamentais, com o potencial para infectar telefones, enviando dados de volta, incluindo fotos, mensagens e gravações de áudio/vídeo, sendo supostamente irrastreável e ideal para atividades de vigilância em operações clandestinas. A vista dessa potencialidade, analisamos o uso do spyware no país e suas implicações nos direitos humanos, direito à privacidade e a LGPD. Para desenvolvimento da pesquisa usamos o método bibliográfico-documental junto à investigação crítico-analítica na análise da bibliografia e notícias sobre o tema.

Palavras-chave: Espião pegasus, Lgpd, Direitos humanos, Direito à privacidade, Soberania

Abstract/Resumen/Résumé

The present work aims to analyze the Pegasus spyware case in the light of the Brazilian law. A spyware developed for sale and use by government agencies, with the potential to infect phones by sending back data including photos, messages and audio/video recordings, it is supposedly untraceable. In view of this potential, we analyze the use of spyware in the country and its implications for human rights, right to privacy and the LGPD. To develop the research we used the bibliographic-documental method together with the critical-analytical investigation in the analysis of bibliography and news on the subject.

Keywords/Palabras-claves/Mots-clés: Pegasus spyware, Lgpd, Human rights, Right to privacy

[1] Advogada, pesquisadora na área de Direito Constitucional, Direito Administrativo, Tecnologias do conhecimento e Blockchaim. Mestre em Educação Tecnológica pelo CEFET-MG.

[2] Engenheiro de Software, Professor de Blockchain, Lider de Cybersegurança na White Hack.

INTRODUÇÃO

Apesar de não ter sido um fato conhecido somente agora, em meados de 2021 o caso do *software* Pegasus, produto criado pela empresa israelense NSO *Group*, voltou a atenção da mídia e dos pesquisadores, diante de novas denúncias e alegações quanto ao seu uso indevido para perseguição de opositores políticos e intimidação de jornalistas. Além disso, a informação que o *spyware* teria sido utilizado por uma agência governamental contra o jornalista assassinado Jamal Khashoggi, conforme notícias publicadas em veículos de notícia internacionais, tais como o "The Washington Post", "Le Monde" e "The Guardian".

Liderado pelo *Forbidden Stories*, uma organização de jornalistas que trabalha em histórias depois que os repórteres originais foram silenciados de alguma forma, a Anistia Internacional executou análises forenses detalhadas. Desse modo, foram analisados 67 smartphones para procurar evidências de que foram alvejados pelo programa Pegasus, tendo descoberto a incidência do espião em 37 desses telefones.

Mesmo no Brasil o interesse pelo programa pelo governo brasileiro foi amplamente divulgado em maio deste ano, quando houve a realização pelo Ministério da Justiça do pregão eletrônico nº 3/21. Medida que foi fortemente criticada e não logrou êxito em seu intento.

Nesse estudo, propomos algumas considerações sobre do que se trata o produto oferecido pelo NSO *Group*, quais são suas potencialidades e a ilegalidade de seu uso no território nacional, com vista ao respeito a Direitos Fundamentais, previsto na Constituição vigente, outras legislações, assim como em Tratados Internacionais em que o Brasil configura signatário.

Por fim, apresentamos algumas possibilidades de solução ou ao menos mitigação, da questão da cibersegurança e proteção de dados na atualidade brasileira.

O que é Pegasus e quem ou o que é o NSO *Group*? Uma questão de cibersegurança

O Pegasus é um spyware desenvolvido por uma empresa privada para uso por agências governamentais. Segundo o desenvolvedor do Pegasus, uma empresa israelense chamada NSO *Group*, o papel de seus produtos, conforme informado em seu site funda-se na possibilidade das "agências de inteligência governamental e policiais a usar tecnologia para enfrentar os desafios da criptografia" durante o terrorismo e investigações criminais. Ainda segundo a empresa, o *software* não pode ser rastreado até mesmo pelo governo que o usa, sendo portanto, um recurso crucial para operações clandestinas. Entre as funcionalidades deste produto, o programa tem capacidade para

infectar o telefone de um alvo, sem a necessidade de qualquer ação do indivíduo, que sem seu consentimento ou conhecimento, envia dados de volta, incluindo fotos, mensagens e gravações de áudio/vídeo.

Ou seja, basicamente o NSO *Group* fabrica produtos que permitem aos governos espionar os cidadãos. Em que resta patente sua ilegalidade, em que pese, o argumento da empresa que seu *software* tenha como objetivo somente o uso para combate ao terrorismo e investigações criminais. E também, a informação da empresa, quanto a disponibilização seus produtos para somente para agências governamentais, que havendo evidências de abuso em seu uso, teriam o acesso ao produto cortado, como já ocorreu em outras oportunidades.

Por óbvio, esta poderosa ferramenta, causa estranhamento, medos e incertezas, uma vez que, poderia ser facilmente utilizada por governos opressores para perseguição a opositores e jornalistas, que denunciam que o espião Pegasus, infringiria à liberdade de expressão, aos direitos fundamentais e até mesmo a soberania entre os Estados. Por este motivo, a empresa NSO *Group* já foi alvo de diversos processos judiciais, inclusive em litígio com grandes empresas como *Facebook* e *Google*.

Embora o caso não seja recente e tenha sido noticiado desde 2015, é surpreendente o conhecimento de que versões recentes dele têm sido capazes de espionar, sem que o usuário faça nada – um link é enviado ao telefone, sem notificação e o Pegasus começa a coletar informações. Em outros casos, a Pegasus supostamente confia nos usuários para clicar em links de *phishing* que então entregam a carga útil do Pegasus.

De acordo com o *The Washington Post*, o *spyware* pode roubar dados privados de um telefone, enviando mensagens, senhas, contatos, fotos e muito mais para quem iniciou a vigilância. Ele pode até ligar as câmeras ou microfones do telefone para criar gravações secretas. Estas informações são publicas e publicitadas pela empresa que oferece o produto, inclusive, um documento da NSO descreve as capacidades do *software* com mais detalhes.

Em suma, apesar das denúncias e das polêmicas envolvidas, a NSO parece ver seu *software* como uma parte necessária, embora desagradável, da vigilância moderna, como a declaração de seu CEO ao *The Washington Post* que "alguém tem que fazer o trabalho sujo" e que o Pegasus está "acostumado a lidar literalmente com o pior que este planeta tem a oferecer."

1.1 O espião Pegasus à luz do ordenamento brasileiro

Diante do exposto, fica evidente as consequências que o uso do *spyware* poderia acarretar na vida dos brasileiros, mesmo que este fosse utilizado apenas por órgãos governamentais, com o intuito de investigar e combater o terrorismo e demais crimes. Isto porque, suas funcionalidades e a forma auspiciosa de seu funcionamento sem o conhecimento dos indivíduos que tem sua privacidade violada, vão de encontro com a legislação brasileira.

Apesar disso, o governo brasileiro demonstrou interesse na compra do programa, caso que foi amplamente divulgado em maio deste ano, quando houve a realização pelo Ministério da Justiça do pregão eletrônico nº 3/21. A articulação para compra do software foi fortemente criticada, sendo alvo de Ação popular contra a compra pelo senador Alessando Vieira (Cidadania-SE) proposta à Justiça Federal, por uma Ação Judicial protocolada pelo advogado do parlamentar, Renato Ribeiro de Almeida contra a União e o protocolo de denúncias contra o pregão por cinco organizações ligadas aos Diretos Humanos, perante, o TCU (Tribunal de Contas da União).

Sobre o tema, o Ministério da Justiça afirmou que o processo de licitação não visava a contratação de "sistema de espionagem", e sim a "aquisição de ferramenta de busca e consulta de dados em fontes abertas para ser usado, pelo ministério e por órgãos de segurança pública, nos trabalhos de enfrentamento ao crime organizado". Com todo o estardalhaço ocorrido, a compra não logrou êxito.

A utilização do programa no país é ilegal, ao permitir a interceptação de dados privados sem o atendimento a requisitos básicos de um devido processo legal e determinação judicial (art. 5˚, XII, CRFB/88), a utilização de um sistema desproporcionalmente invasivo seria totalmente contrária ao ordenamento constitucional brasileiro – que possui os princípios da legalidade (art. 5˚, II, CRFB/88) e da presunção de inocência (art. 5˚, LVII, CRFB/88) como elementos basilares. O sigilo das comunicações (art. 5˚, XII, CRFB/88) também é direito fundamental garantido pela Constituição brasileira.

Por isso, a inviolabilidade da correspondência e o sigilo das comunicações só poderiam ser restringidos em hipóteses excepcionalíssimas, como na vigência de estado de sítio (art. 139, III, CRFB/88). Sobre o tema a lei de interceptação telefônica (Lei nº 9296/96) é imperiosa ao determinar: "a interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça" Grifo nosso. E também, ao destacar "comunicações de qualquer natureza", a legislação abrange, inequivocamente, as comunicações virtuais.

Insta destacar, o Direito à privacidade trata-se de um direito intrínseco do individuo, inerente à sua esfera íntima e a personalidade, cabendo sua mantença não somente um dever do Estado, mas um dever de todos, quanto o cuidado a não intromissão da vida privada.

Também ressalta-se, o Direito à privacidade sofreu gradativamente alterações no tempo, de modo que se a princípio levava em conta a não intromissão na vida privada, na família, no domicílio e nas correspondências[1], foi sendo ampliado até incluir as informações pessoais e o direito de controle de seus próprios dados. Sobre isso Rodotá esclarece:

> Partindo dessa constatação, pode-se dizer que hoje a sequência quantitativamente mais relevante é "pessoa-informação-circulação- controle", e não mais apenas "pessoa-informação-sigilo", em torno do qual foi construída a noção clássica de privacidade. O titular do direito à privacidade pode exigir formas de "circulação controlada", e não somente interromper o fluxo de informações que lhe digam respeito. (RODOTÁ, 2008, p. 93)

Na Europa, antes da LGPD ser aprovada no Brasil, o Regulamento Europeu de Proteção de Dados Pessoais, chamado de *General Data Protection Regulation* (GDPR), editado em 2016, teve papel importante para a concretização de medidas nesse sentido no país. Pois, a partir de sua aprovação, empresas europeias passaram a exigir atenção a regulação para realização negócios com empresas brasileiras. Portanto, a regulação da Europa é considerada uma norma relevante quanto a proteção de dados, porquanto, colocou a privacidade como núcleo valorativo desse direito, concentrando-se no indivíduo titular detentor dos dados.

Quanto à LGPD, ainda que o legislador tenha destacado em seu artigo 4º, inciso III, alínea "a", à não aplicação da lei no âmbito da segurança pública, ressaltou que seus princípios norteadores, também deverão abarcar a legislação superveniente, tendo em vista a compreensão de que privacidade e proteção de dados pessoais são direitos fundamentais. Desse modo, em seu parágrafo 1˚ do artigo 4º dispõe a lei:

> o tratamento de dados pessoais previsto no inciso III [tratamento de dados realizado para fins de: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais] será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Portanto, princípios de devido processo, necessidade e proporcionalidade, não podem deixar de serem observados, no âmbito da persecução penal e de fins investigativos. Mais que isso, a finalidade, a adequação, a necessidade e os demais princípios da proteção de dados definidos na

[1] Declaração Universal dos Direitos Humanos de 1948.

LGPD, bem como os direitos de acesso, retificação, cancelamento etc. determinados pela lei, deverão ser observados.

Ademais, comparando a LGPD e o GPDR, conforme leciona Patrícia Peck (PECK, 2008), ambas as legislações têm como objetivo o regramento do tratamento de dados pessoais buscando em si a defesa dos direitos fundamentais das pessoas naturais. Dado que essas legislações determinam o que são dados pessoais e outros conceitos de grande relevância, estabelecendo o consentimento como um dos fatores centrais nas relações que envolvam dados pessoais, com a devida previsão de aplicações de medidas de segurança e sanções no caso de descumprimento, prevendo um órgão competente para fiscalizar e zelar pela proteção dos dados pessoais e da privacidade.

CONSIDERAÇÕES FINAIS

Em suma, neste trabalho, buscamos trazer importantes apontamentos sobre o *software* Pegasus, explicando acerca da sua funcionalidade e dos objetivos que ensejaram sua criação pela empresa desenvolvedora, NSO *Group*.

Pelo exposto, indo ao encontro da legislação brasileira demonstramos como a compra do programa e sua utilização no território nacional, inclusive pelo governo brasileiro, acarretaria em ilegalidade, visto que infringiria a direitos fundamentais dos cidadãos, tais como o direito à privacidade, o princípio da legalidade, a presunção de inocência, o devido processo legal, o sigilo das comunicações e a inviolabilidade das correspondências.

Portanto, é preciso destacar a responsabilidade do Estado brasileiro, assim como os demais Estados, posto que, o problema transpassa a qualquer barreira territorial, bem como, o dever das empresas, em proteger e respeitar os direitos humanos e trabalhar para remediar e mitigar que violações como as aqui demonstradas ocorram. Para tanto, é imprescindível a existência de um arcabouço jurídico atualizado e em consonância com os problemas advindos das tecnologias na realidade de vida das pessoas, com condão para permitir enfrentar os desafios da vigilância digital.

Todavia, salientamos que no caso do Pegasus, supondo que a pessoa não seja um jornalista trabalhando em matérias delicadas, um líder mundial ou em alguma posição que possa ameaçar os poderes governamentais, seria muito improvável que alguém pagaria milhares ou dezenas de milhares de dólares para vigiá-lo através do *software*. Dito isso, é obviamente preocupante que esses tipos de ataques sejam possíveis e que possam cair nas mãos de *hackers* que buscam atingir uma gama muito mais ampla de pessoas.

Como acontece com todas as medidas relacionadas à segurança, é importante ser realista sobre as ameaças que podemos enfrentar e o que se pode fazer a respeito. Para a maioria das pessoas

que provavelmente não serão visadas por um ator no nível de um estado-nação, a maior ameaça à privacidade vem dos corretores de dados, que operam legalmente e em maior escala. Por outro lado, se alguém realmente está sendo alvo de governos, com todos os recursos à disposição deles, provavelmente por enquanto não há muito que possa-se fazer para manter seus dados digitais privados.

Contudo, não dispensamos a ideia da necessidade de uma educação digital da sociedade, para que consigam se conscientizar sobre privacidade e autonomia dos dados, para que possam compreender o que verdadeiramente está em jogo quando optamos pela personalização de conteúdo. Portanto, o uso malicioso de dados pessoais, sem a finalidade devida, o abismo informacional e a assimetria que permite vícios de consentimento, precisam ser objetos de regulação. Cabendo nesse ponto, que as instituições públicas e órgãos regulatórios pertinentes, tais como a ANPD, a SENACON, o CADE, o MPF, entre outros, venham à intervir.

REFERÊNCIAS

BITAR, Carlos Alberto. Os Direitos da Personalidade. 8. ed. São Paulo: Saraiva, 2015.

BRASIL. Constituição da República Federativa do Brasil de 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acesso em 28 de outubro de 2021.

BRASIL. Lei nº 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm Acesso em 28 de outubro de 2021.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direito e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htmAcesso em: 26 de outubro de 2021

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 28 de outubro de 2021.

BRASIL. Decreto nº 10.748 de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022 Acesso em: 28 de outubro de 2021.

MARCZAK, Bill; SCOTT-RAILTON, John; MCKUNE, Sarah; RAZZAK, Bahr Abdul and DEIBERT, Ron. “Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries,” Citizen Lab Research Report No. 113, University of Toronto, September 2018.

PINHEIRO, Patrícia Peck. Direito Digital. 2° ed.. São Paulo: Saraiva, 2008.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais. Comentários à lei 13.709/2018 (LGPD). São Paulo: Saraiva Jur, 2018.

PRIEST, Dana; TIMBERG, Craig e MEKHENNET, Souad. Private Israeli spyware used to hack cellphones of journalists, activists worldwide. The Washington Post. 2021. Disponível em: https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ Acesso em: 28 de outubro de 2021

RODOTÁ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

VALENÇA, Lucas. UOL News. Empresa de software espião Pegasus abandona licitação do governo. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/25/empresa-de-software-espiaopegasus-deixa-edital-que-e-rodeado-de-incertezas.htm Acesso em: 26 de outubro de 2021