III CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (III CIDIA)

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

CLARA CARDOSO MACHADO JABORANDY

LIZIANE PAIXAO SILVA OLIVEIRA

EDGAR GASTÓN JACOBS FLORES FILHO

T255
Tecnologias disruptivas, direito e proteção de dados II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito e Inteligência Artificial (III CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Clara Cardoso Machado Jaborandy, Liziane Paixão e Edgar Gastón Jacobs Flores Filho – Belo Horizonte: Skema Business School, 2022.

Inclui bibliografia
ISBN: 978-65-5648-516-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: A inteligência artificial e os desafios da inovação no poder judiciário.
1. Disrupção. 2. Tecnologia. 3. Proteção de dados. I. III Congresso Internacional de Direito e Inteligência Artificial (1:2022 : Belo Horizonte, MG).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (III CIDIA)

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

Apresentação

O Congresso Internacional de Direito e Inteligência Artificial (CIDIA) da SKEMA Business School Brasil, que ocorreu em formato híbrido do dia 08 ao dia 10 de junho de 2022, atingiu a maturidade em sua terceira edição. Os dezesseis livros científicos que ora são apresentados à comunidade científica nacional e internacional, que contêm os 206 relatórios de pesquisa aprovados, são fruto das discussões realizadas nos Grupos de Trabalho do evento. São cerca de 1.200 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil, dentre outros temas.

Neste ano, de maneira inédita, professores, grupos de pesquisa e instituições de nível superior puderam propor novos grupos de trabalho. Foram recebidas as excelentes propostas do Professor Doutor Marco Antônio Sousa Alves, da Universidade Federal de Minas Gerais (SIGA-UFMG – Algoritmos, vigilância e desinformação), dos Professores Doutores Bruno Feigelson e Fernanda Telha Ferreira Maymone, da Universidade do Estado do Rio de Janeiro (Metalaw – A Web 3.0 e a transformação do Direito), e do Professor Doutor Valmir Cézar Pozzetti, ligado à Universidade Federal do Amazonas e Universidade do Estado do Amazonas (Biodireito e tutela da vida digna frente às novas tecnologias).

O CIDIA da SKEMA Business School Brasil é, pelo terceiro ano consecutivo, o maior congresso científico de Direito e Tecnologia do Brasil, tendo recebido trabalhos do Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Mato Grosso, Pará, Pernambuco, Piauí, Paraná, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe e São Paulo. Tamanho sucesso não seria possível sem os apoiadores institucionais do evento: o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito, o Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC e o Programa RECAJ-UFMG - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais. Destaca-se, mais uma vez, a presença maciça de pesquisadores do Estado do Amazonas, especialmente os orientandos do Professor Doutor Valmir César Pozzetti.

Grandes nomes do Direito nacional e internacional estiveram presentes nos painéis temáticos do congresso. A abertura ficou a cargo do Prof. Dr. Felipe Calderón-Valencia (Univ. Medelín - Colômbia), com a palestra intitulada “Sistemas de Inteligência Artificial no Poder Judiciário - análise da experiência brasileira e colombiana”. Os Professores Valter Moura do Carmo e Rômulo Soares Valentini promoveram o debate. Um dos maiores civilistas do país, o Prof. Dr. Nelson Rosenvald, conduziu o segundo painel, sobre questões contemporâneas de Responsabilidade Civil e tecnologia. Tivemos as instigantes contribuições dos painelistas José Luiz de Moura Faleiros Júnior, Caitlin Mulholland e Manuel Ortiz Fernández (Espanha).

Momento marcante do congresso foi a participação do Ministro do Tribunal Superior do Trabalho – TST Maurício Godinho Delgado, escritor do mais prestigiado manual de Direito do Trabalho do país. Com a mediação da Profª. Drª. Adriana Goulart de Sena Orsini e participação do Prof. Dr. José Eduardo de Resende Chaves Júnior, parceiros habituais da SKEMA Brasil, foi debatido o tema “Desafios contemporâneos do gerenciamento algorítmico do trabalho”.

Encerrando a programação nacional dos painéis, o Prof. Dr. Caio Augusto Souza Lara, da SKEMA Brasil, dirigiu o de encerramento sobre inovação e Poder Judiciário. No primeiro momento, o juiz Rodrigo Martins Faria e a equipe da Unidade Avançada de Inovação do Tribunal de Justiça do Estado de Minas Gerais contaram sobre o processo de transformação em curso do Judiciário Estadual mineiro. Em seguida, o Prof. Dr. Fabrício Veiga Costa fez brilhante exposição sobre o projeto denominado “Processo Coletivo Eletrônico”, que teve a liderança do Desembargador Federal do Trabalho Vicente de Paula Maciel Júnior (TRT-3ª Região) e que foi o projeto vencedor do 18º Prêmio Innovare. O evento ainda teve um Grupo de Trabalho especial, o “Digital Sovereignty, how to depend less on Big tech?”, proposto pela Profª. Isabelle Bufflier (França) e o momento “Diálogo Brasil-França” com Prof. Frédéric Marty.

Os dezesseis Grupos de Trabalho contaram com a contribuição de 46 proeminentes professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo, os quais eram compostos por pesquisadores que submeteram os seus resumos expandidos pelo processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI.

Desta forma, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com ela, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da CAPES. Promoveu-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Foi lançada a nossa pós-graduação lato sensu em Direito e Tecnologia, com destacados professores e profissionais da área. No segundo semestre, teremos também o nosso primeiro processo seletivo para a graduação em Direito, que recebeu conceito 5 (nota máxima) na avaliação do Ministério da Educação - MEC. Nosso grupo de pesquisa, o Normative Experimentalism and Technology Law Lab – NEXT LAW LAB, também iniciará as suas atividades em breve.

Externamos os nossos agradecimentos a todas as pesquisadoras e a todos os pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 20 de junho de 2022.

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

SPYWARE: O CONFLITO ENTRE SEGURANÇA NACIONAL E DIREITOS INDIVIDUAIS

SPYWARE: THE CONFLICT BETWEEN NATIONAL SECURITY AND INDIVIDUAL RIGHTS

Anna Carolina Alves Moreira de Lacerda [1]
Daniele Pabline Sousa Costa [2]

Resumo

A presente pesquisa aborda a temática dos programas de espionagem e o desenvolvimento tecnológico, bem como a evolução vivenciada na sociedade atual. Desse modo, pretende esclarecer como esse tipo de software afeta os direitos básicos dos cidadãos, como a privacidade e a intimidade, destacando a necessidade da proteção de dados. A pesquisa proposta pertence à vertente metodológica jurídico-sociológica. Quanto à investigação, o tipo jurídico-projetivo. Predominará o raciocínio dialético.

Palavras-chave: Spyware, Direito, Proteção de dados

Abstract/Resumen/Résumé

This research addresses the issue of espionage programs and technological development, as well as the evolution experienced in today's society. In this way, it intends to clarify how this type of software affects the basic rights of citizens, such as privacy and intimacy, highlighting the need for data protection. The proposed research belongs to the legal-sociological methodological aspect. As for the investigation, the legal-projective type. Dialectical reasoning will predominate.

Keywords/Palabras-claves/Mots-clés: Spyware, Right, Data protection

[1] Graduanda em Direito, modalidade Integral, e integrante da Iniciação Científica “Teoria do Crime” pela Escola Superior Dom Helder Câmara. Email: 000annalacerda@gmail.com. Currículo Lattes: http://lattes.cnpq.br /7638885643757353

[2] Graduanda em Direito Integral pela Escola Superior Dom Helder Câmara e Investigação Forense e Perícia Criminal, integrante do grupo de iniciação Científica “Direito e Tecnologia”; email: pscdani7@gmail.com

1. CONSIDERAÇÕES INICIAIS

O interesse da pesquisa adveio da reportagem publicada pelo Jornal El País, intitulada "Embargo dos EUA contra o software espião Pegasus não torna ambiente cibernético mais seguro". Nesse sentido, essa aborda o programa de espionagem desenvolvido pela *NSO Group*, empresa israelense, com a finalidade de venda para entidades de segurança e defesa, como agências de inteligência, exército, entre outros, e utilizado em diversos países. Apesar de ainda não ser empregado no Brasil, a presente pesquisa busca explicitar pontos positivos e negativos desses tipos de *softwares*, a partir da legislação brasileira, em vista da possibilidade de aplicação futura (CABRAL, 2021).

Nesse sentido, é evidente a evolução da internet e dos *softwares* nas últimas décadas. Com o surgimento de computadores e celulares, houve ampla expansão desse mercado, alcançando quase a totalidade da população global. Desse modo, as inovações se tornaram constantes, sendo desenvolvidos programas que muitas vezes podem afetar direitos básicos dos cidadãos. Faz-se, consequentemente, necessárias pesquisas e debates em relação a esse assunto.

Em consonância, nota-se a precisão de se conceituar termos como ciberespaço e indústria *spyware*. O ciberespaço pode ser definido como "ciberespaço é o conjunto de rede de computadores na qual todo o tipo de informação é circulada. Gibson define ciberespaço como um espaço existente no mundo da comunicação" (LIGIA, 2016), destacando o distanciamento do mundo físico para o espaço digital. Por conseguinte, a indústria spyware é o nicho de mercado voltado para o desenvolvimento de programas que têm como finalidade se infiltrar em aparelhos eletrônicos de forma silenciosa, permitindo acesso ao conteúdo presente e até mesmo registrando e rastreando a atividade realizado no dispositivo (LIGIA, 2016).

Por fim, a pesquisa a que se propõe encontra-se em estágio inicial de desenvolvimento, pertencendo à classificação de Gustin, Dias e Nicácio (2020), mais especificamente, à vertente metodológica jurídico-social. No tocante ao tipo genérico de pesquisa, foi escolhido o tipo jurídico-projetivo. O raciocínio desenvolvido na pesquisa foi, predominantemente, dialético e quanto ao gênero de pesquisa, foi adotada a pesquisa teórica. Assim, a pesquisa se propõe a esclarecer como o programa de *spyware* afeta os direitos básicos dos cidadãos brasileiros, além de demonstrar pontos positivos e negativos desse tipo de programa.

2. INDÚSTRIA SPYWARE E PROGRAMAS DE ESPIONAGEM

A evolução tecnológica tem ocorrido em uma velocidade cada vez maior. No contexto histórico, partindo de uma análise do passado, o surgimento da internet, nos anos 90, e, sua posterior popularização nos anos 2000, foi essencial para alcançar o estágio avançado atual. Dessa forma, o ciberespaço foi criado como meio para construção das relações humanas à longa distância. Para além do planejado de conectar as pessoas, na sociedade moderna, os aparelhos eletrônicos armazenam milhares de dados, como fotos, senhas e até mesmo aplicativos de bancos e cartões de créditos digitais (EVOLUÇÃO, 2020).

Como resultado, surgiu uma nova modalidade de crime, o denominado crime cibernético, que se tornou comum na comunidade contemporânea. Nesse ponto, ainda que não exista consenso a respeito de uma única conceituação, esse pode ser explicitado como crimes que envolvem qualquer atividade ou prática ilícita na rede, abordando infrações que somente se concretizam de modo virtual ou, ainda, que se utilizam do ambiente digital como meio de praticar o tipo penal. Em conformidade, destaca-se que muitos possuem o caráter transnacional, "o que dificulta as investigações e a apuração de provas contra o acusado" (NASCIMENTO, 2014).

Nessa perspectiva, as infrações passaram a ser cometidas digitalmente, podendo ser citado a pornografia infantil, pirataria, lavagem de dinheiro, entre outros. No entanto, novos termos tiveram que ser criados para abranger novas condutas realizadas, como o ciberterrorismo e o ciberativismo. Desse modo, o primeiro configura-se como a prática de ações, com viés político, contra governos, partidos, instituições governamentais, civis, etc. Já o ciberativismo pode ser explicado como "crime praticado contra organizações que defendem determinadas causas. Esse cibercrime envolve roubo de informações e manipulações nos materiais que são divulgados ao público e à imprensa" (NASCIMENTO, 2014).

Ante ao exposto, prevaleceu a necessidade de criar meios de defesa contra tais ilícitos, por exemplo, o tão polêmico programa de *spyware*. Como demonstrado pelo Jornal El País, o *software* mencionado possui finalidade importante, comercializado para forças de segurança, como polícia, exército, serviço de inteligência, entre outros, não sendo a sua venda proibida. O programa espião pode monitorar crianças de forma a garantir sua segurança no ambiente virtual ou até mesmo atingir caráter nacional, evitando ataques cibernéticos a agências do governo e prevenindo que dados pessoais dos indivíduos sejam vazados (SEGUIN, 2022).

Todavia, apesar de possuir pontos positivos, quanto a sua utilização de forma adequada, esse expõe os usuários a diversos riscos, os quais serão explicitados no tópico seguinte.

3. AS INCERTEZAS DAS NOVAS TECNOLOGIAS

Como exposto anteriormente, a atualidade é marcada pelo uso das novas tecnologias, de modo que técnicas evoluem continuamente para auxílio do ser humano em diversas áreas, como no controle de determinados crimes. A partir disso, destaca-se, por exemplo, uma ferramenta introduzida no Instagram do Reino Unido e da Europa que consegue perceber sites que divulgam conteúdo agressivo. Nisso, a partir da inteligência artificial conseguem captar padrões e evidenciar imagens e palavras que violam as regras das plataformas. No mesmo sentido, atua o *software* de espionagem, porém, embora esses artifícios se demonstrem promissores em alguns aspectos, apresentam incertezas, como quanto à proteção de dados, do direito à privacidade e intimidade.

Nessa perspectiva, urge analisar como o ordenamento jurídico brasileiro orienta a temática do direito à intimidade. A princípio, a Constituição da República Federativa do Brasil de 1988 estabelece que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [...]” (BRASIL, 1988). Sob esse viés, compreende-se que o direito à intimidade é reconhecido no rol dos direitos e garantias fundamentais da Constituição Cidadã. Assim, a abrangência da vida privada e intimidade é assegurada constitucionalmente, de modo a garantir o “direito de estar só, porque salvaguardam a esfera de reserva do ser humano, insuscetível de intromissões externas" (BULOS, 2020).

Além disso, o direito à intimidade é um dos direitos da personalidade, previsto no Código Civil em vigor. A referida legislação estabelece que “a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2002). Logo, a proteção da intimidade da vida privada da pessoa natural é, mais uma vez, ressaltada nos ordenamentos jurídicos vigentes, o que demonstra a importância do tema abordado.

No mesmo sentido, a Lei nº 13.709, de 14 de agosto de 2018, mais conhecida por LGPD (Lei Geral de proteção de dados), regula as atividades de tratamento de dados pessoais, apresentando como um dos fundamentos o respeito à privacidade, assim como a inviolabilidade da intimidade, da honra e da imagem. Desse modo, a partir da exposição das normas constitucionais e da ordem supralegal, sobre o direito à intimidade e privacidade dos indivíduos,

questiona-se sobre a possibilidade de violação desses direitos, por meio de aplicativo de espionagem. Afinal, como supracitado, a partir da inteligência artificial, diversos aspectos podem ser captados, até mesmo variados atributos pessoais, como traços de personalidade, inteligência, felicidade, uso viciante de substâncias, idade e gênero, como apresentado por um estudo conduzido por Michal Kosinski, David Stillwell e Thore Graepel (2013), citado por Lara (2019).

Logo, o ponto sensível da utilização de *software* para espionar pessoas é que essa técnica poderia ser desvirtuada, sendo utilizada para captar outros pontos que não fossem crimes que causam grande impacto na sociedade. Há um destaque para aplicação da técnica com a finalidade de manter determinado regime no poder, ou seja, podem monitorar a ideia política. O caso do jornalista Jamal Khashoggi é um exemplo da extrapolação dessa nova tecnologia, porque evidências apontam que o mesmo havia sido monitorado com o uso do Pegasus, o que facilitou a operação que culminou na morte do cidadão (CABRAL, 2021).

Desse modo, percebe-se que há um potencial risco de violar não só o direito à privacidade e intimidade, como ameaçar o direito à liberdade de expressão, direito garantido constitucionalmente, no Art. 5º, IX. Afinal, como não há uma garantia de como essas técnicas estão sendo utilizadas, surge uma vulnerabilidade quanto ao controle social, contexto que é visualizável na China. No Estado mencionado, há uma vigilância algorítmica de modo que os indivíduos estão proibidos de usar a Internet para prejudicar a segurança nacional, ferir os interesses do Estado ou da sociedade, que promove a derrubada do governo ou do sistema socialista, por exemplo (MEYER, 2017).

Por fim, o sociólogo Byung-Chul Han, marco-teórico da pesquisa, na obra titulada *No enxame*, ressalta que:

> Hoje não somos mais destinatários e consumidores passivos de informação, mas sim remetentes e produtores ativos. Não nos contentamos mais em consumir informações passivamente, mas sim queremos produzi-las e comunicá-las ativamente nós mesmos. Somos simultaneamente consumidores e produtores. Esse duplo papel aumenta enormemente a quantidade de informação. A mídia não oferece apenas uma janela para o assistir passivo, mas sim também portas através das quais passamos informações produzidas por nós mesmos (2020, p. 36).

Em conformidade, as pessoas deixaram de ser meras ouvintes para produtoras de informação. Nisso, o Direito e suas estruturas tradicionais apresentam um contexto complexo e dinâmico, o que exige constantes inovações para encaminhar soluções mais adequadas (BERWIG, et al. 2019). Logo, é acertado dizer que essas informações estão sendo utilizadas para produzirem dados e serem utilizadas por algoritmos, sendo preciso que a espionagem

supracitada seja coibida pelos órgãos fiscalizadores, a fim de que não haja ameaça ou violação do direito à privacidade, intimidade, assim como à liberdade de expressão.

4. CONSIDERAÇÕES FINAIS

A partir da pesquisa apresentada, ficou evidente a evolução tecnológica vivenciada na sociedade atual. Nesse sentido, foi explicitado o contexto atual da presença constante da internet, softwares, inteligência artificial, entre outros. Desse modo, foi abordada a temática da espionagem digital e dos programas de *spyware*, bem como de que modo a sua utilização afeta os direitos básicos dos cidadãos garantidos pela legislação brasileira. Em consequência, expôs a necessidade de se preservar a privacidade e a intimidade.

Por um lado, foi possível constatar que o benefício dessas técnicas de espionagem é utilizar como meio de defesa contra ilícitos, assim como pode ser instrumento de monitoramento, a fim de garantir segurança no ambiente virtual ou até mesmo evitar ataques cibernéticos a agências do governo. No entanto, é possível afirmar preliminarmente que embora promissora, a inovação traz incertezas, principalmente quanto a possível violação aos direitos da privacidade, intimidade, além da ameaça à liberdade de expressão, devido ao fácil controle social.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BERWIG, Juliane Altmann; ENGELMANN, Wilson; WEYERMULLER, André Rafael. Direito ambiental e nanotecnologias: desafios aos novos riscos da inovação. *Veredas do Direito*: Direito Ambiental e Desenvolvimento Sustentável, Belo Horizonte, v. 16, n. 36, p. 217- 246, dez. 2019. Disponível em: http://revista.domhelder.edu.br/index.php/veredas/article/view/1553. Acesso em: 30 abr. 2022.

BULOS, Uadi Lammêgo. *Curso de direito constitucional.* 13. ed. São Paulo: Saraiva Educação, 2020.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 mar. 2021.

BRASIL. Lei n. 10.406, 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406compilada.htm;. Acesso em: 06 abr. 2022

CABRAL, Carlos. *Embargo dos EUA contra o software espião Pegasus não torna ambiente cibernético mais seguro*. 12 de 2021. Disponível em: https://brasil.elpais.com/opiniao/2021-12-12/embargo-dos-eua-contra-o-software-espiao-pegasus-nao-torna-ambiente-cibernetico-mais-seguro.html. Acesso em: 25 maio 2022.

EVOLUÇÃO do uso da tecnologia ao longo dos últimos anos. 29 out. 2020. Disponível em: https://blog.sled.com.br/evolucao-do-uso-da-tecnologia-ao-longo-dos-ultimos-anos/. Acesso em: 20 maio. 2022.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. *(Re)pensando a pesquisa jurídica: teoria e prática.* 5ª. ed. São Paulo: Almedina, 2020.

HAN, Byung-Chul. *No enxame: Perspectivas do Digital*. 3ª ed. Petrópolis - Rio de Janeiro: Editora Vozes. 2020.

LARA, Caio Augusto Souza. O acesso tecnológico à justiça: por um uso contra-hegemônico do big data e dos algoritmos. Belo Horizonte, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/DIRS-BC6UDB/1/tese___caio_augusto_souza_lara___2015655391____vers_o_final.pdf. Acesso em: 30 abr. 2022.

LÍGIA, Ana. *Entenda o que é ciberespaço e como surgiu a expressão*. 18 out. 2016. Disponível em: https://www.estudopratico.com.br/entenda-o-que-e-ciberespaco-e-como-surgiu-a-expressao/. Acesso em: 17 maio. 2022.

MEYER, Maximiliano. Como funciona a censura e o acesso à internet da China. 16 ago 2017. Disponível em: https://www.oficinadanet.com.br/tecnologia/19933-como-funciona-o-acesso-a-censura-na-internet-da-china. Acesso em: 30 abr. 2022.

NASCIMENTO, Anderson. *O que é cibercrime?*. 11 jul. 2014. Disponível em: https://canaltech.com.br/seguranca/O-que-e-cibercrime/. Acesso em: 20 maio. 2022.

SEGUIN, Patrick. *Spyware: Detecção, prevenção e remoção*. 9 maio. 2022. Disponível em: https://www.avast.com/pt-br/c-spyware. Acesso em: 17 maio. 2022.