A INTERCEPTAÇÃO TELEFÔNICA NA ERA PÓS-DIGITAL: AS IMPLICAÇÕES LEGAIS E OPERACIONAIS DO *SOFTWARE PEGASUS* NAS ATIVIDADES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA NO CENÁRIO BRASILEIRO

José Batista dos Santos[1]
Eliseu Gonçalves[2]
Clarindo Alves de Castro[3]

RESUMO

Esta pesquisa teve por objetivo analisar o *Software Pegasus* como meio de obtenção de dados pela Segurança Pública do Brasil. A partir da revolução digital, buscou-se responder: quais implicações operacionais e legais que o *Software Pegasus* teria ao ser usado para interceptação telefônica nas Atividades de Inteligência de Segurança Pública brasileira? A hipótese foi de que as tecnologias de comunicação desenvolveram-se demasiadamente, contudo o Sistema de Inteligência do Brasil não as acompanhou na mesma proporção. A fim de obter respostas à questão proposta, utilizou-se o método hipotético-dedutivo. A pesquisa teve abordagem qualiquantitativa em questionário, aplicando a Escala Likert, Lógica Booleana e questões abertas endereçadas aos profissionais de Inteligência de Segurança Pública pela plataforma *Google Forms*. Os resultados confirmam as hipóteses de necessidade de tecnologias avançadas como meios de obtenção de dados, e o *Software Pegasus* como solução para suprir essa demanda.

Palavras-chave: *Inteligência de Segurança Pública. Inteligência Eletrônica. Interceptação telefônica. Obtenção de dados. Software Pegasus.*

ABSTRACT

This research aimed to analyze the Pegasus Software as a means of obtaining data by the Public Security of Brazil. From the digital revolution, we sought to answer: what operational and legal implications would the Pegasus Software have when used for telephone interception in Brazilian Public Security Intelligence Activities? The hypothesis was that communication technologies have developed too much, however the Brazilian Intelligence System has not followed them in the same proportion. In order to obtain answers to the proposed question, the hypothetical-deductive method was used. The research had a qualitative and quantitative approach in a questionnaire, applying the Likert Scale, Boolean Logic and open questions addressed to Public Security Intelligence professionals through the Google Forms platform. The results confirm the hypotheses of the need for advanced technologies as a means of obtaining data, and the Pegasus Software as a solution to meet this demand.

Keywords: *Public Security Intelligence. Electronic Intelligence. Telephone Interception. Data acquisition. Pegasus Software.*

---

[1] Capitão da Polícia Militar do Estado do Paraná, Oficial Aluno do Curso de Aperfeiçoamento de Oficiais - CAO/EGSP/PMMT/2021-2022 da Academia de Polícia Militar Costa Verde – APMCV.

[2] Capitão da Polícia Militar do Estado do Paraná, Oficial Aluno do Curso de Aperfeiçoamento de Oficiais - CAO/EGSP/PMMT/2021-2022 da Academia de Polícia Militar Costa Verde – APMCV.

[3] Coronel da Polícia Militar do Estado de Mato Grosso, Mestre em Educação pela Universidade Federal de Mato Grosso – Professor Orientador.

INTRODUÇÃO

O objeto de estudo esta pesquisa é o *Software Pegasus* como recurso tecnológico para a obtenção de dados de dispositivos eletrônicos pela Inteligência de Segurança Pública do Brasil. Para isso, serão analisadas as implicações operacionais e legais de sua implementação e demonstrado que esse produto desenvolvido pela empresa *NSO Group* está na vanguarda da tecnologia de interceptação telefônica, telemática e de dados.

A escolha desse tema decorre da necessidade de atualização dos meios de obtenção de dados pela Inteligência de Segurança Pública (ISP) visando a produção de conhecimento, bem como em ações e operações de prevenção e repressão da criminalidade.

No desenvolvimento da pesquisa, apresenta-se, de forma sucinta, a maneira como se deu a revolução digital e a recente popularização dos *smartphones* como meio de comunicação. Além da função do clássico telefone, os *smartphones* agregam a praticidade da *internet*, o uso de aplicativos, comunicação por textos, arquivos, imagens, vídeos, sons, grande capacidade de armazenamento e transmissão de dados, em tempo real e ao alcance da mão.

Enquanto os aplicativos de comunicação buscam fornecer privacidade aos usuários, as atividades de ISP necessitam de meios de obtenção de dados em situações que prescindem dessa ação. O problema está no questionamento de quais implicações operacionais e legais o *Software Pegasus* teria no emprego de interceptação telefônica nas Atividades de ISP no cenário brasileiro.

Nesse contexto, a hipótese é de que a revolução pós-digital, fenômeno ainda em curso, transformou o sistema de comunicação em tecnologia altamente avançada, no entanto esse desenvolvimento não foi acompanhado de forma simultânea pelo Sistema de ISP do Brasil para permitir a realização de interceptações telefônicas das atuais tecnologias, nem mesmo houve adequação legislativa para tanto. O *Pegasus* é apresentado como solução de tecnologia de ponta para a produção de conhecimento, instrução processual penal e investigação criminal, possibilitando ações preventivas e/ou repressivas em Segurança Pública.

O objetivo geral da pesquisa é analisar as implicações operacionais e legais para a implantação do *Pegasus,* (assim denominado a partir daqui), como meio de obtenção de dados de ISP. Os objetivos específicos estão em discorrer brevemente sobre revolução digital, conceitos doutrinários de Inteligência de Segurança Pública e interceptação telefônica pertinentes ao objeto de pesquisa, realizar análise da legislação específica das interceptações telefônicas previstas na Lei nº 9.296/1996, cadeia de custódia de provas, além de identificar as carências dos meios de obtenção de dados relatados no questionário aplicado aos Profissionais de ISP.

Este artigo estrutura-se, inicialmente, com o breve esclarecimento sobre a evolução da *internet* como meio de comunicação, sua popularização a partir da década de 1990 e o crescente uso dos *smartphones* na última década. Também foi discorrido acerca das importantes categorias em torno da Inteligência de Segurança Pública, comunicação e interceptação telefônica.

Passada essa fundamentação teórica preliminar, o conteúdo trata de maneira específica do *Pegasus* como importante e poderoso meio de obtenção de dados eletrônicos de sinais, imagens e demais arquivos transmitidos e armazenados nos *smartphones.*

O método da pesquisa foi hipotético-dedutivo, sendo realizada pesquisa bibliográfica e leitura de conteúdos doutrinários, legislação e jurisprudência, bem como pesquisa de campo, por abordagem qualiquantitativa (FLICK, 2009), com os Profissionais de ISP que responderam um questionário com questões objetivas pela plataforma do *Google Forms*. O questionário foi estruturado, conforme Escala Likert, em até 5 níveis para mensuração de respostas objetivas (LIKERT, 1932) e por perguntas de afirmação ou negação, conforme Função Boleana (MORAIS FILHO, 2007), além de questões abertas.

O fator de inclusão dos participantes foi a atuação com o Profissionais de ISP em âmbito nacional, sejam Policiais Militares, Policiais Civis, Membros do Poder Judiciário Estadual ou Federal, Ministério Público Estadual ou Federal, Agência Brasileira de Inteligência, Forças Armadas e Secretaria de Segurança Pública. Além do perfil do participante, foi questionado sobre as companhias telefônicas, legislações, meios de obtenção de dados e do *Pegasus* em si.

O Projeto de Pesquisa foi encaminhado para análise do Comitê de Ética em Pesquisa do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso – IFMT, acompanhado do Termo de Consentimento Livre e Esclarecido (TCLE), Cronograma, Orçamento, Termo de Anuência, Declaração de Responsabilidade e Questionário.

A apresentação da análise dos dados foi realizada de maneira descritiva. Ao final deste artigo, apresenta-se a conclusão da pesquisa sobre a implementação do *Pegasus*, classificado preliminarmente como poderoso meio de obtenção de dados. Esta pesquisa contribui para o debate sobre a utilização de recursos eletrônicos para obtenção de dados. Envolve o avanço tecnológico e a ponderação de Direitos Fundamentais, Segurança Pública e Atividade de ISP. Não há, portanto, qualquer intenção ou condição de esgotamento do tema, cujas fontes de pesquisa trazem certo grau de sigilo sobre o *Pegasus* e sua utilização pela atividade de ISP.

A REVOLUÇÃO DIGITAL E DA *INTERNET* COMO MEIO DE COMUNICAÇÃO

A Revolução Digital tem início a partir da década de 1960, no transcorrer da Guerra Fria, época em que Estados Unidos e União Soviética lutavam pela hegemonia global em várias áreas, inclusive na de tecnologia de comunicações. Nesse cenário, surgem a microinformática e os primeiros computadores como suportes nas telecomunicações analógicas de rádio, televisão, imprensa, cinema por integrarem a produção, a difusão e o estoque de informação midiática (LEMOS, 2013).

No ano de 1969, o Departamento de Defesa dos Estados Unidos instituiu a ARPA[4] que se transformou na ARPANET[5]. Inicialmente foram conectados quatro computadores de diferentes Universidades: Califórnia de Los Angeles; Califórnia de Santa Barbara; *Stanford Research Institute* e Universidade de Utah (ALMEIDA, 2005).

4 *Advanced Research Projects Agency*. Tradução livre para língua portuguesa: Agência de Projetos de Pesquisas Avançadas.

5 *Advanced Research Projects Agency Network.* Tradução livre para a língua portuguesa: Rede de Agências de Projetos de Pesquisas Avançadas.

Nessa época, a conexão foi feita a partir da rede telefônica por circuitos, mas, entre 1973 e 1978, criou-se um protocolo para a interconexão de redes de computadores, o TCP/IP[6], o qual substituiu, a partir de 1983, todo o sistema utilizado até então, dando origem à *internet,* denominação popularizada na década de 1990, quando a ARPANET foi substituída pela NSF[7] (ALMEIDA, 2005).

A *internet* começou a ser implantada no Brasil em 1989, concretizou-se na década de 1990, quando passou a ser comercializada e expandiu-se rapidamente. Em 1996, existiam 7,5 mil domínios; no ano de 2000, eram 170 mil; chegou à casa de um milhão no ano de 2006 e, em 2014, já possuía três milhões e meio de domínios, ou endereços de sítios da *internet* (LINS, 2013).

A história recente da *internet* pode ser descrita por quatro períodos distintos: o primeiro de uso privado e restrito das redes; o segundo, pela disponibilidade ao público pela rede discada mediante provedor; o terceiro, pelo acesso em banda larga por aumentar-lhe o desempenho, possibilitar o uso e o compartilhamento de vídeos, áudios, imagens e interações. O quarto período caracteriza-se pela diversificação das telas, especialmente dos *smartphones,* os quais envolvem as rotinas das pessoas e permitem o envio de qualquer tipo de informação aos demais equipamentos eletrônicos (LINS 2013, p. 13-14).

Ao tratar da coexistência das mídias tradicionais e atuais, Jenkins (2009, p. 32) relata que compraria um telefone com função única de realizar tão somente chamada telefônica, sem preocupar-se com qual botão apertar ou qual recurso tecnológico utilizar. Os vendedores riram e disseram que não havia mais venda desse tipo de aparelho, porque ninguém mais os queria. Diante dessa afirmativa, ele confirmou a convergência das mídias em torno do *smartphone* para diversas soluções ao alcance da mão.

A tecnologia digital e seus arquivos de múltiplas utilizações criaram um corte histórico, visto que a Era Pós-digital surge entre 50 e 100 anos de consolidação da Era Digital, iniciada na década de 1960. A Era Pós-digital define o atual momento, quando a tecnologia passou a integrar a rotina humana em um ambiente no qual as

6 *Transmission Control Protocol and Internet Protocol*. Tradução livre para a língua portuguesa: Protocolo de Controle de Transmissão e Protocolo de Rede de Computadores.
7*National Science Foundation*. Tradução livre para a língua portuguesa: Fundação Nacional de Ciências.

redes sociais alteram realidades de maneira imediata. Pessoas e diversos ambientes nunca estiveram tão conectados. O espaço digital está difundido e interativo, sendo um novo espaço de relação amplo e imediato (LONGO, 2021).

Produto da Era Pós-digital, os *smartphones* são meios de comunicação que não se resumem a ligações telefônicas, pois aglutinam aplicativos contendo som, imagem, vídeo, mídias sociais, jogos e outras funções num único aparelho (KWON *et al,* 2013).

Por essa razão, o debate da Atividade de ISP sobre a obtenção de dados com o uso de novas tecnologias se faz necessário, em virtude do acesso à *internet* por meio dos *smartphones* cujo uso aumentou consideravelmente na última década, "a densidade de dispositivos digitais era de 50% em 2010. Em junho de 2021, já é de mais de 200%, ou seja, dois dispositivos por habitante" (MEIRELLES, 2021, p. 93).

Em uma década, os *smartfhones* tornaram-se a primeira opção de acesso à rede e principais responsáveis por sua expansão, ficando à frente dos computadores. Embora já existissem nos anos de 2010, esses aparelhos ocupavam uma insignificante porcentagem em relação ao uso predominante de computadores. No ano de 2015, o número de dispositivos digitais passava de 300 milhões, cujo uso era de 50% para cada um deles. Em maio de 2021, o Brasil possuía 440 milhões desses dispositivos, dos quais 198 milhões eram computadores, e 242 milhões eram *smartphones,* 53% do total. (MEIRELLES, 2021, p. 93).

De acordo com o IBGE (2018, p. 1), 64,7% das pessoas e 69,3% dos domicílios brasileiros têm acesso à *internet*; 94,2% dos entrevistados nessa pesquisa, utilizam-na para acessar aplicativos de conversação que transmitem mensagens de texto, voz ou imagens, diferentes de e-mail; 73,3% do total geral utilizam o *smartphone* para conversar por chamadas de voz ou vídeo.

A grande quantidade de dispositivos digitais se assemelha a um enxame digital, por isso a identificação do usuário pode ser difícil, favorecendo o anonimato do homem digital no cometimento de crimes e na sensação de impunidade (HAN, 2014, p. 8 e 17). Sob essa perspectiva, a obtenção de dados por vias tradicionais é uma ação complexa.

Com base nos dados acima apresentados, é possível afirmar que os *smartphones* têm sido o dispositivo digital mais utilizado atualmente. Seus usuários estão ao alcance da Lei nº 9.296/1996, no entanto, diante dessa tecnologia avançada, fazem-se necessários meios de obtenção de dados eficazes e atualizados para a produção do conhecimento e enfrentamento da criminalidade por ações preventivas e/ou repressivas.

INTELIGÊNCIA DE SEGURANÇA PÚBLICA E OBTENÇÃO DE DADOS

A palavra Inteligência, que compõe a denominação acima, pode ser compreendida sob três acepções: a primeira como tipo de conhecimento produzido, a segunda como organização institucional administrativa e a terceira como atividade ou processo desenvolvido pela organização de inteligência para obtenção de dados.

A atividade de inteligência é o esforço simples e natural para obter o tipo de conhecimento sobre o qual se pode basear um curso de ação bem-sucedido (KENT, 1965, p. xxii-xiii).

De acordo com a Doutrina Nacional de Segurança Pública (BRASIL, 2014, p. 19) "[…] a atividade de ISP centra-se na produção e salvaguarda de conhecimentos utilizados no assessoramento de uma tomada de decisão de interesse da Segurança Pública".

Rondon Filho (2009, p. 50) define Inteligência de Polícia como sendo "[...] uma característica de uma polícia dotada de metodologia e técnicas apropriadas à produção do conhecimento pretendido para a consecução de sua missão constitucional". Em linhas gerais, "[...] a Inteligência não busca, como foco principal, o esclarecimento de autoria e materialidade de um fato típico penal por meio da prova, mas sim a busca e a antecipação ao fenômeno conhecendo-o, bem como a sua intrínseca relação econômico-político-social com atores estatais e não estatais" (ANDRADE, 2017, p. 108).

O conceito de Atividade de Inteligência de Segurança Pública (ISP) é formulado pela DNISP, segundo a qual:

> [...] é o exercício permanente e sistemático de ações especializadas para identificar, avaliar e acompanhar ameaças reais ou potenciais na esfera de Segurança Pública, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os tomadores de decisão, para o planejamento e execução de uma política de Segurança Pública e das ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza que atentem à ordem pública, à incolumidade das pessoas e do patrimônio (BRASIL, 2014, p. 13).

A definição de Atividade de ISP foi reformulada pelo Plano Nacional de Inteligência Pública, conforme se verifica abaixo:

> [...] o exercício permanente e sistemático de ações especializadas destinadas à identificação, à avaliação e ao acompanhamento de ameaças reais e potenciais no âmbito da segurança pública, orientadas para a produção e a salvaguarda de conhecimentos necessários ao processo decisório no curso do planejamento e da execução da PNSPDS e das ações destinadas à prevenção, à neutralização e à repressão de atos criminosos de qualquer natureza que atentem contra a ordem pública, a incolumidade das pessoas e do patrimônio." (BRASIL, 2021)

A Atividade de ISP divide-se nos ramos de Inteligência e Contrainteligência de Segurança Pública, a primeira com vistas à produção e à difusão de conhecimentos, a última relacionada a prevenção, detecção, neutralização e obstrução de ações que constituam ameaças (BRASIL, 2021). De acordo com a DNISP (BRASIL, 2014, p. 16), "os dois ramos, intrinsecamente ligados, não possuem limites precisos, uma vez que se interpenetram, inter-relacionam-se e interdependem.

As ações de ISP são exercidas por Profissionais de ISP, os quais são assim definidos:

> São elementos orgânicos de Agência de Inteligência (AI) recrutados administrativamente e devidamente capacitados. As duas funções essenciais diretamente envolvidas na produção do conhecimento são os Analistas, responsáveis pela produção do conhecimento, e os

> Agentes, responsáveis pela obtenção dos dados negados (BRASIL, 2014, p. 16).

Em princípio, os profissionais de ISP "[...] não executam ações ostensivas, prisões ou flagrantes, visando preservar a segurança de seus integrantes e garantir o sigilo e a compartimentação (BRASIL, 2014, p. 17), cabendo às equipes ostensivas tais ações.

A DNISP prevê algumas espécies de ISP: "[...] a Inteligência Policial Judiciária, Inteligência Policial Militar, Inteligência Bombeiro Militar, Inteligência Policial Rodoviária" (BRASIL, 2014, p. 17). Cada uma delas está ligada à sua função originária, mas com um importante ponto de atenção. Em referência ao tema desta pesquisa, explicita-se que a atividade de Inteligência Policial Judiciária está voltada para a produção de conhecimento e excepcionalmente à produção de provas, enquanto a Investigação Policial está contida na persecução penal prevista e regulamentada na norma processual para a produção de provas na busca por autoria e materialidade (BRASIL, 2014, p. 18).

Sabendo-se que a atividade de ISP produz conhecimento, é preciso esclarecer que o dado ainda não foi submetido à metodologia de Produção do Conhecimento, enquanto o conhecimento é o resultado expresso escrito ou oralmente, conforme Metodologia de Produção de Conhecimento (BRASIL, 2014, p. 19). Ocorre que as fontes de dados podem ser abertas (livre acesso) ou fechadas (dados negados ou protegidos). Para a obtenção desses dados, quando o dado é negado, exige-se operação, no caso de dado protegido, exige-se credenciamento para acesso (BRASIL, 2014, p. 24-25). Considerando a tecnologia dos *smartphones* e o direito ao sigilo de comunicação (discutido à frente), os dados de um aparelho dessa natureza, em princípio, já podem ser classificados como dados negados.

Existem dois meios de obtenção de dados, os humanos e os eletrônicos. O último diz respeito à atividade de Inteligência Eletrônica, cujo "[...] foco central é o uso de equipamentos eletrônicos ou sistemas informatizados, inclusive aqueles conectados à rede mundial de computadores, para obtenção de dados" (BRASIL, 2014, p. 25). A Inteligência Eletrônica pode ser classificada como Inteligência de sinais, imagens e de dados, conforme abaixo explicado:

> a) **Inteligência de Sinais:** é responsável pela interceptação e análise de comunicações, telecomunicações, telemática, radares, telemetria entre outros.
> b) **Inteligência de Imagens:** envolve a obtenção e o processamento de imagens por meio de fotografias, satélites, sensores infravermelhos, dentre outros.
> c) **Inteligência de Dados:** envolve a obtenção de dados por meio de dispositivos ou sistemas de informática. Implica, ainda, no processamento de grandes volumes de dados, cuja complexidade para análise exige metodologia especializada (DNISP. 2014, p. 25, negrito no original).

As ações para a busca de dados que necessitam de autorização judicial são classificadas como "[...] ações de Inteligência Policial Judiciária. Tais ações são de natureza sigilosa e envolvem o emprego de técnicas especiais visando à obtenção de dados (indícios, evidências ou provas de autoria ou materialidade de um crime)" (BRASIL, 2014, p. 34). Rondon Filho (2009, p. 119) ressalta que a vigilância e a tecnologia de informação (TI) são fontes de informações para a produção de conhecimento, assim como os informantes selecionados. Esclarecem que a vigilância complementa o mecanismo de interceptação de sinais e comunicação, e a tecnologia de informação (TI) constitui-se como base da atividade de ISP, sem descartar outras técnicas.

De acordo com Moretti (2009, p. 85), "a utilização de novos e modernos procedimentos de investigação em todo o mundo, baseados em técnicas desenvolvidas pelos serviços de inteligência, decorre da necessidade de enfrentamento eficaz do crime organizado". Moretti (2009, p. 86) destaca que "havendo observância das garantias e liberdades individuais, são perfeitamente aplicáveis os procedimentos de persecução penal inspirados em técnicas características das atividades de inteligência".

INTERCEPTAÇÃO TELEFÔNICA

Entre as acepções de interceptação está o ato de "interromper o curso de: [...] barrar o acesso ou passagem por; [...] captar ou apreender (aquilo que é dirigido a outrem) sem que isso se apercebam os que o emitem e recebem" (HOUAISS, 2022). Nucci (2017, p. 561) afirma que a interceptação "[...] tem o significado de interferência, com o fito de colheita de informes".

Alguns conceitos ligados à interceptação devem ser diferenciados:

> a) **Comunicação telefônica**: abrange não apenas a conversa por telefone, mas também a transmissão, emissão de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia, estática, ou móvel (celular). [...]
> b) **Comunicação ambiental**: refere-se às comunicações realizadas diretamente no meio ambiente, sem transmissão e recepção por meios físicos, artificiais, como fios elétricos, cabos óticos etc. [...]
> c) **Interceptação telefônica**: consiste na captação da comunicação telefônica alheia por um terceiro, sem o conhecimento de nenhum dos comunicadores; [...]
> d) **Escuta telefônica**: é a captação da comunicação telefônica por terceiro, com o conhecimento de um dos comunicadores e desconhecimento do outro. [...]
> e) **Gravação telefônica clandestina**: é a gravação da comunicação telefônica por um dos comunicadores, ou seja, trata-se de uma autogravação (ou gravação da própria comunicação). (LIMA, 2020, p. 812, negrito no original)

Tanto a interceptação telefônica quanto a escuta podem ser determinadas pela autoridade judiciária quando houver justa causa. As comunicações telefônicas são meios de prova, enquanto a interceptação telefônica é meio para obtenção da prova, já a gravação é o resultado da operação e materialização da prova. A transcrição é o meio de prova por um documento específico (LIMA, 2020, p. 814).

É considerado lícito o uso de gravação clandestina que comprove inocência do acusado ou quando houver investida criminosa. A afirmação de que gravações clandestinas são ilícitas por serem violações ao direito da intimidade não prospera, pois, toda pessoa tem o direito de gravar sua própria conversa. Assim a gravação clandestina considera-se válida, salvo se o conteúdo se referir a assunto decorrente de sigilo profissional (LIMA, 2020, p. 815-816).

A definição de interceptação telefônica pode ser distinguida em dois sentidos:

> Em sentido lato, define-se "interceptação telefônica" como qualquer ato de interferência nas comunicações telefônicas alheias, quer com a finalidade de impedi-las, quer com a finalidade de delas tomar conhecimento. [...] Em sentido estrito, indica a captação de comunicação telefônica entre duas pessoas, diversas do interceptador, sendo que, pelo menos, uma delas desconhece a existência da intromissão; a escuta pode ser documentada fonograficamente através de meios mecânicos. (GRINOVER, 2013, p. 255)

Segundo Grinover (2013, p. 259), as Interceptações Telefônicas caracterizam-se "[...] como operação técnica que visa colocar à disposição do juiz o conteúdo de uma conversa telefônica; equipara-se à apreensão dos elementos fonéticos que constituem a conversação; tais elementos fonéticos, resultado da operação técnica, configuram fonte de prova".

A interceptação telefônica tem a finalidade de investigação criminal ou instrução processual penal e depende de ordem de juiz competente (BRASIL, 1996), no entanto "[...] não se admite a decretação de interceptação para processo civil, processo administrativo ou inquérito civil, todavia, o resultado da interceptação poderá ser utilizado como elemento probatório emprestado" (GARZELLA, *et al.*, 2021, p. 32), como no caso de encontro fortuito de provas.

Esse encontro de provas fortuito pode ser de primeiro grau, quando o delito encontrado se conecta com o caso investigado e praticado pelo investigado; pode ser em segundo grau, quando a obtenção inesperada de prova referir-se a outra pessoa diversa do investigado e sem conexão com o crime. No primeiro caso, a prova pode ser utilizada em processo penal; no segundo caso seria motivo para instaurar mais uma investigação do crime descoberto. Em caso de descobrimento de prática de crime futuro, a autoridade deve prevenir sua concretização, apurando eventuais condutas criminosas (GARZELLA *et al.*, 2021, p. 44).

Aspectos legais das interceptações telefônicas

O Código Brasileiro de Telecomunicações, Lei nº 4.117/1962, previa como crime de violação de telecomunicação o ato de receber, divulgar ou utilizar de telecomunicação interceptada (art. 56, § único), mas não constituía violação de telecomunicação a interceptação autorizada por Juiz competente, mediante requisição ou intimação (BRASIL, 1962).

A Constituição Federal de 1988 (CF/1988), em seu art. 5º, incisos X e XII (BRASIL, 1988), discorre sobre os direitos e as garantias individuais, em tese, invioláveis. No inciso XII, trata do sigilo de correspondência, das comunicações telegráficas, telefônicas e de dados. Tal direito pode ser excetuado por força de ordem judicial, para investigação criminal ou instrução processual, previsto em lei. Sobre dispositivo constitucional que trata de inviolabilidade, Lima (2020, p. 809) ressalta que "não há que se falar em direito fundamental absoluto. Todos os direitos fundamentais devem ser submetidos a um juízo de ponderação quando entram em rota de colisão com outros direitos fundamentais, preponderando aquele de maior relevância".

Grinover (1997, p. 114) destaca que, depois de promulgada a CF/1988, o Supremo Tribunal Federal exigiu o amparo legal que legitimasse as interceptações telefônicas, mas que aconteceu somente com a publicação da Lei 9.296/1996.

A Lei nº 9.296/1996 dispõe os pressupostos para realização de interceptações, sendo eles: a autorização por Juiz competente, requerimento de autoridade policial na investigação ou Ministério Público, imprescritibilidade da interceptação para apuração da infração e fundamentação da autorização, podendo ser por quinze dias e prorrogáveis por igual período (BRASIL, 1996).

A denominação autoridade policial é no sentido amplo. Tanto que o Supremo Tribunal Federal já se manifestou reconhecendo a realização de interceptações telefônicas pela Polícia Militar (BRASIL, 2012), assim como o Tribunal de Justiça do Estado do Paraná decidiu que "[...] não é nula a interceptação telefônica autorizada por Juiz competente, a pedido da Polícia Militar" (PARANÁ, 2015, p. 16).

Exige-se, ainda, conforme análise do art. 2º da Lei nº 9.269/1996, a existência de indícios razoáveis de autoria ou participação na infração penal, quando

não houver outros meios disponíveis para a obtenção de dados e quando o fato investigado for punível com pena de no mínimo, reclusão, devendo apresentar descrição objetiva dos investigados e a imputabilidade penal do agente. A impossibilidade de qualquer indicativo deve ser manifestada por escrito (BRASIL, 1996).

A Lei nº 12.850/2013, que trata de organizações criminosas, inovou ao dispor um capítulo para tratar da investigação e de meios de obtenção de prova, prevendo que, em qualquer fase da persecução penal, serão permitidas interceptações de comunicações telefônicas e telemáticas, nos termos legais (BRASIL, 2013). De um modo geral, Andrade (2017, p. 122) destaca a necessidade de legislação mais aprimorada para a atividade de ISP, tendo em vista as transformações atreladas aos crimes transnacionais, terrorismo e outros nocivos ao País.

A validação do ciclo de obtenção de dados por interceptação finaliza-se com o armazenamento dos dados por uma segura Cadeia de Custódia que consiste em um "[...] mecanismo garantidor da autenticidade das evidências coletadas e examinadas, assegurando que correspondem ao caso investigado, sem que haja lugar para qualquer tipo de adulteração" (LIMA, 2020, p. 718). Gomes destaca que "[...] a cadeia de custódia é um dispositivo que busca assegurar a integridade dos elementos probatórios, além de evitar a inclusão de prova ilícita" (2021, p. 41).

A Cadeia de Custódia foi conceituada recentemente pela Lei nº 13.964/2019 como o "conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte" (BRASIL, 2019).

A evolução do conceito de comunicação e da interceptação telefônica

No passado, a telefonia era definida legalmente como "processo de telecomunicação destinado à transmissão da palavra falada ou de sons" (BRASIL, 1962). Tal conceito está desatualizado, pois hoje telecomunicação abrange

"transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza" (BRASIL, 1997).

A Lei nº 9.296/1996 tem como objeto as comunicações telefônicas de qualquer natureza, inclusive interceptação de comunicações em sistemas de informática e telemática (BRASIL, 1996). Sobre isso, Lima (2020, p. 818) afirma que "é possível a interceptação de qualquer comunicação via telefone, conjugada ou não a informática, o que compreende aquelas realizadas direta (fax, *modens*) e indiretamente (*internet*, *e-mail,* correios eletrônicos)".

A CF/1988 autoriza a interceptação telefônica de modo restrito, mas "não se pode ficar alheio aos avanços tecnológicos-culturais, ampliando as formas de comunicações, privando os órgãos de persecução penal de um importante instrumento de investigação e busca da verdade" (LIMA, 2020, p. 819), sendo válidas como provas as interceptações de conversas em sítios de *internet*, *e-mails*, aplicativos ou conversações durante jogos eletrônicos, autorizadas judicialmente.

A interceptação telefônica diz respeito ao que acontece no presente, já a quebra de sigilo de dados telefônicos se refere a um fato ocorrido no passado. Os dados cadastrais são registros decorrentes da criação de conta telefônica e contêm o número da linha e a qualificação pessoal do proprietário, enquanto os dados telefônicos são registros de uso da linha telefônica, abrange mensagens e transmissão de sinais (GARZELLA *et al.* 2021, p. 27).

A utilização de aplicativos por dados móveis já se tornou habitual, e os mais comuns são "[...] o *WhatsApp, Telegram e Facebook Messenger*. Nesse imo, inexoravelmente, a atuação investigativa diligente deverá encetar ações destinadas a devassar conteúdo também já recebido em mensagens por meio eletrônico" (GARZELLA *et al.* 2021, p. 39). Nesse sentido, Garzella *et al.* (2021, p. 41) reconhecem que há argumentos contrários à utilização de mensagens armazenadas em período pretérito, uma vez que inexiste legislação que estabeleça a utilização de uma figura híbrida que trate da interceptação pretérita e futura do fluxo das comunicações telemáticas.

A execução da interceptação telefônica e recursos utilizados

A interceptação telefônica deve seguir sob segredo de justiça, ou seja, "[...] a pessoa investigada não pode ter conhecimento da realização das diligências, pois, do contrário seria totalmente frustrada a possível eficácia desse meio de investigação" (LIMA, 2020, p. 842). Em caso de arguição de ampla defesa ou contraditório pelo acesso aos dados obtidos, esses serão devidos após serem concluídas as diligências pertinentes (BRASIL, 2019).

De acordo com Garzella *et al.* (2021, p. 75 a 105), em um aspecto prático procedimental, existe uma sequência de fatos/atos na interceptação telefônica: o contexto fático do delito, a apuração preliminar, a representação, o deferimento, a implementação, o acompanhamento, a prorrogação, a investigação telemática e o desfecho.

Para a interceptação do fluxo das comunicações telemáticas e o afastamento do sigilo dos dados, Garzella *et al.* (2021, p. 119-138) explicam que essas práticas também exigem da empresa de comunicação, o fornecimento de *login* e senha para os policiais criarem contas espelho e acessar os dados armazenados, destacando empresas como a *Microsoft, Yahoo, Locaweb, Dropbox, Google, Facebook, Instagram, WhatsApp e Apple*.

Entre as soluções apresentadas pelos autores como recursos tecnológicos aplicados na interceptação, são elencados os *softwares Nuix Voice,* Gestão de Interceptação Legal, o Guardião, *RSA NETWITNESS SUITE, VERIFAC,* brevemente esclarecidos abaixo.

O sistema *Nuix Voice* "promove de forma rápida e automatizada a transcrição, sendo possível realizar a transcrição de áudios de correio de voz, sistema de gravação telefônica, *smartphones,* anotadores digitais e câmeras variadas" (GARZELLA *et al.*, 2021, p. 139).

A Gestão de Interceptação Legal é da empresa *Suntech*, possui o sistema VIGIA para a retenção de dados, identificação e localização de chamadas ou SMS e a localização para acompanhamento (GARZELLA *et al.*, 2021, p. 140).

O GUARDIÃO é um equipamento da empresa Dígitro, utilizado na receptação, análise de conteúdos e monitoramento em tempo real, bem como interceptação de fluxo de comunicações telefônicas, informática, dados armazenados em nuvens de computação móvel, fontes de notícias, redes sociais e fontes públicas. (GARZELLA *et al.*, 2021, p. 141).

A *RSA NETWITNESS SUITE* "é uma plataforma de detecção e respostas a ameaças que permite, dentro de muitas possibilidades, realizar a captura de dados em tempo real, de *logs* e de pacotes de rede" (GARZELLA *et al*, 2021, p. 142)

A VERIFAC "é uma plataforma *on line* que permite a captura e preservação técnica de fatos ocorridos no ambiente *on line* acessados através de *websites*, automatizando práticas comuns na área forense digital e medidas técnicas efetivas contra fraudes e manipulação" (GARZELLA *et al*, 2021, p. 142).

Todos esses *softwares* dizem respeito à interceptação de sistemas, mas sem a devassa do equipamento de modo remoto e necessitam do intermédio das empresas operadoras, diferente do *Pegasus* objeto deste estudo.

O *SOFTWARE PEGASUS* COMO MEIO DE OBTENÇÃO DE DADOS NA ATIVIDADE DE ISP

O poderoso Pégaso[8], cavalo alado da mitologia grega, cumpridor missões do Olimpo (BULFINCK, 2002), surge agora como poderosa arma cibernética capaz de obter dados dos mais desenvolvidos *smartphones* (BLACKHAT, 2016).

Foucault (2004) alertava que a vigilância de ambientes, de modo ostensivo e permanente, pelo sistema panóptico no fim século XVIII era simples e eficiente, mas perigosa se houvesse desvio de utilidade. Isso vale ao *Pegasus*, tão poderoso que pode causar danos se utilizado de maneira indiscriminada, ilegal ou arbitrária. Não por acaso, tem havido grande polêmica sobre seu uso em âmbito jurídico e na imprensa, seja nacional (GAZETA DO POVO, 2021) ou internacional (THE NEW YORK TIMES, 2021).

8 Em conformidade com Língua Portuguesa, diferente da palavra *Pegasus*, a qual diz respeito ao *software* pesquisado.

Como já esclarecido, o protagonismo da *internet* como meio de comunicação da sociedade é demonstrado pelo seu desenvolvimento nas últimas décadas, tão popular quanto o equipamento de comunicação denominado *smartphone* que, ao prometer sigilo em suas comunicações, pode ser um facilitador para a prática de delitos. O *Pegasus* utiliza de pouquíssimas falhas desses *smartphones* para invadi-los e coletar dados de seu sistema, imediatamente e em tempo real, sem a necessidade ação direta do usuário ou de operadoras (SAFE, 2021).

O *Pegasus* teria sido utilizado contra jornalistas, ativistas de direitos humanos, políticos, servidores públicos civis e militares de diversos governos, é o que aponta estudo do consórcio *Pegasus Project,* criado em 2021. Foram realizadas entrevistas e análises de 64 *smartphones* suspeitos de terem sido atacados pelo *software*, dos quais 23 foram infectados com sucesso e outros 14 tinham sinais de invasão. Não foram identificados vestígios do *Pegasus* nos demais aparelhos analisados, não que deixaram de ser invadidos, pois o *software* tem a capacidade de destruir os rastros de suas ações. Dos 37 *smartphones,* 34 eram da *marca Apple* com sistema operacional *IOS,* gerando uma ação judicial da *Apple* contra a *NSO Group* pelo uso indiscriminado do *Pegasus*. Esses telefones estariam na lista dos 50 mil números vigiados pela *NSO Group* (*WASHINGTON POST,* 2021*).*

A empresa responsável pelo *WhatsApp* também impetrou ação judicial contra a *NSO Group* por interceptar seu aplicativo e obter dados de aproximadamente 1400 *smartphones*, violando legislações dos Estados Unidos, no entanto a *NSO Group* alega que goza de imunidade estendida aos Estados Soberanos, uma vez que fornece tecnologia para aplicação da lei e auxilia na Segurança Pública (ALJAZEERA, 2022).

O *Pegasus* retira o anonimato digital do usuário, combate a sensação de impunidade e a criminalidade. As críticas de sua interferência na liberdade da sociedade ganham eco e figuram simultaneamente entre as notícias de natureza política e tecnológica (THE HACK, 2021).

Das funcionalidades do *Software Pegasus*

O *Pegasus* é desenvolvido pela *NorthPole Nesco Sarl* (*NSO Group*), um grupo de solução de *software* de segurança cibernética e inteligência para agências governamentais, voltada à interceptações para alvos que representam ameaças locais ou globais. As operações financeiras da *NSO Group* ocorrem normalmente em Israel, Bulgária e Chipre (MOODY´S, 2021).

De acordo com o descritivo do produto, o *Pegasus* é uma solução de inteligência cibernética, a qual permite às agências governamentais extraírem informações de maneira remota e secreta de praticamente qualquer dispositivo móvel. A solução foi desenvolvida por veteranos de agências de inteligência para fornecer uma opção eficaz de enfrentamento aos novos desafios de interceptação de comunicações no campo de batalha cibernético (*NSO GROUP*, 2014, p. 7).

A *NSO GROUP* destaca que o mercado da comunicação móvel teve um crescimento muito rápido. Somados a isso, alguns fatores prejudicam as ações das organizações de inteligência, tais como a criptografia, excesso de aplicativos, alvos fora do domínio nacional de interceptação, mascaramento de identidades virtuais, substituições de cartão SIM[9], além da morosidade e burocracia das operadoras (*NSO GROUP*, 2014, p. 7).

Quando não há atualização dos sistemas de interceptação, os obstáculos amparam a conduta de crimes e terrorismo, principalmente se as soluções de interceptações tradicionais persistirem, especificamente a interceptação passiva, interceptação tática por GSM[10] e o *software* malicioso (*malware).* Na interceptação passiva, ocorre o relacionamento estreito com prestadores de serviços locais de *internet* ou telefonia, mas a criptografia dificulta o acesso a esse tipo de comunicação. A interceptação por GSM monitora as chamadas por voz e por texto, sendo pouco utilizada atualmente. Já o *malware* exige a participação do dispositivo do alvo e pode enfrentar um eficiente *software* do tipo *anti-spyware* (*NSO GROUP*, 2014).

Segundo a *NSO Group* (2014), o *Pegasus* implanta seu agente no dispositivo de destino, extrai e transmite os dados para análise de maneira remota, não requer

9 *Subscriber Identify Module.* Tradução livre para a língua portuguesa em: modulo de identificação de assinante.
10 *Global System form Mobile.* Tradução livre para a língua portuguesa em: sistema global para comunicações móveis

nenhuma ação do alvo e não deixa vestígio no dispositivo. A empresa descreve os seguintes benefícios do *Pegasus:*

> • **Acesso ilimitado aos dispositivos móveis do alvo**: Coleta remotamente e secretamente informações sobre os relacionamentos, localização, ligações, planos e atividades – quando e onde quer que estejam;
> • **Intercepta chamadas**: Monitora chamadas de voz e VoIP de forma transparente em tempo real;
> • **Preenche lacunas de inteligência:** Coleta tipos únicos e novos de informações (contatos, arquivos, escuta ambiental, senhas etc.)[...]
> • **Intercepta conteúdo e dispositivos criptografados**: Supera a criptografia, proprietário de protocolos e qualquer obstáculo introduzido pela tecnologias de comunicações;
> • **Monitoramento de aplicativos**: Monitora uma infinidade de aplicativos, incluindo *Skype*, *WhatsApp, Viber, Facebook e Blackberry Messenger* (BBM);
> • **Identifica alvos:** Rastreia alvos e obtém informações precisas de posicionamento usando GPS;
> • **Independência do provedor de serviços**: Não é necessária a cooperação com as operadoras de rede móvel locais;
> • **Descobre identidades virtuais**: Monitora constantemente o dispositivo sem se preocupar com troca frequente de identidades virtuais e substituição de cartões SIM;
> • **Evita riscos desnecessários**: Elimina a necessidade de aproximação física do alvo ou dispositivo [...] (*NSO GROUP,* 2014, p. 9, negrito no original, tradução nossa).

Os destaques da tecnologia *Pegasus* são elencados no fato de penetrar em dispositivos de *Android*, *BlackBerry*, IOS e *Symbiam*, extrair contatos, mensagens, e-mails, fotos, arquivos, locais, senhas, processos, lista ou outros dados do dispositivo; acessar os dispositivos protegidos por senha; para o alvo, é uma ação invisível e não deixa rastros; não interfere no consumo da bateria, memória e dados; possui mecanismo de autodestruição em caso de risco de exposição e recupera qualquer arquivo do dispositivo para análise profunda (*NSO GROUP,* 2014, p. 10).

A arquitetura do *Pegasus* é projetada por camadas de ações definidas para a instalação nos dispositivos: coleta e extração de dados, monitoramento passivo, coleta de dados pela ativação de câmera e microfone, GPS, coleta de dados programada por eventos ou características, transmissão de dados, apresentação e análise de dados por alvos distintos, conexões ocultas, dados por georeferência,

regras de alertas e a administração do sistema para gerenciar as permissões, a segurança e o funcionamento de todos os componentes (*NSO GROUP*, 2014, p. 10).

A instalação do agente oculto é destacada como a fase mais sensível e importante da operação de inteligência, podendo ser realizada de quatro formas: *over-the-air,* por mensagem, proximidade do alvo e física. A instalação do tipo o*ver-the-air* acontece por mensagem enviada ao dispositivo, sendo instalado sem qualquer cooperação ou envolvimento do alvo, mas nada aparece no dispositivo, pois é silenciosa e invisível. A instalação por mensagem acontece por envio de SMS ou e-mail que atraem o alvo a abri-lo, um clique no *link* basta para instalar o agente oculto. Na instalação por proximidade do alvo, utiliza-se um equipamento tático de rede com estação transceptor, o número do terminal é identificado remotamente e resulta na completa instalação. A instalação física deve ser feita próximo do alvo, quando for a única opção, pode ser efetivada manualmente em menos de 5 minutos, a partir daí toda operação é desenvolvida remotamente (*NSO GROUP,* 2014).

O agente do *software* ingressa no dispositivo, coleta as informações e transmite os dados para servidores do *Pegasus* de maneira oculta e contínua. Instalado o agente oculto, qualquer criptografia não tem mais importância. A principal diferença do *Pegasus* em relação com outras plataformas é a instalação *over-the-air* (*NSO GROUP,* 2014), tradução livre "pelo ar" ou, popularmente conhecida, interceptação "zero clique", pois independe de qualquer ação do alvo e raramente deixa vestígios.

A coleta de dados pelo *Pegasus* é dividida em três níveis: extração de dados e registros pretéritos, monitoramento passivo futuro, e a coleta ativa por GPS, chamadas, recuperação de arquivos ocultos, gravação de som, câmera fotográfica ou vídeo e captura de tela. Na fase de coleta ativa, o dispositivo pode ser utilizado em todos os aplicativos e demais funções do aparelho, sendo tudo transmitido e salvo nos servidores do *Pegasus* em tempo real (*NSO GROUP,* 2014).

A ação de coleta de dados dos alvos do *Pegasus* gera muito material a ser visualizado, apresentados e analisados. Por isso são disponibilizadas ferramentas de análise geográfica, regras de alertas, marcação de eventos favoritos, painel de inteligência estatística, gestão de alvos por grupos, análise por períodos e pesquisa

avançada por busca de palavras-chave. Por ser de fácil utilização e visualização, pode ser personalizado (*NSO GROUP,* 2014).

A manutenção e a atualização do *Pegasus* devem ser feitas a fim de oferecer novos recursos e configurações, dando suporte ao aperfeiçoamento dos agentes ocultos, o que deve acontecer em poucos minutos. A desinstalação pode ocorrer quando a operação é finalizada ou quando não existe mais interesse na interceptação do alvo e executada de forma rápida mediante uma única solicitação do usuário. Existe ainda a possibilidade de autodestruição do agente instalado em caso de risco de exposição ou quando o agente não responde por um longo período (*NSO GROUP,* 2014).

Algumas informações finais devem ser destacadas. A *NSO GROUP* é o responsável por implantar e configurar o *hardware* e *software Pegasus*, sem nenhum envolvimento das operadoras de rede móvel local. A partir do momento em que os dados trafegam pelas redes públicas, eles são captados pelo agente. O anonimato é garantido pela empresa, visto que os dados percorrem vários locais do mundo antes de chegar ao servidor *Pegasus,* o qual trabalha com grandes quantidades de dados e de forma ininterrupta. (*NSO GROUP,* 2014).

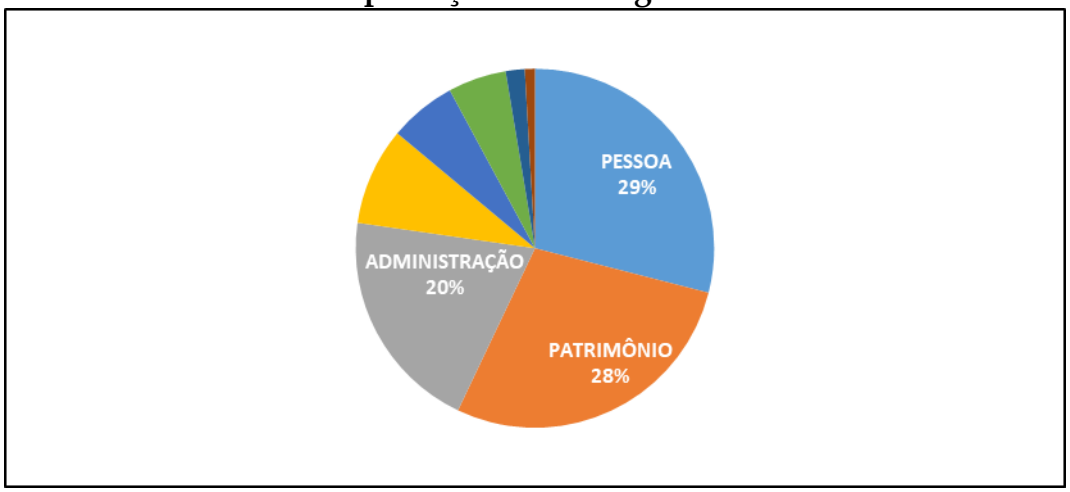
RESULTADOS E DISCUSSÃO DOS DADOS

A pesquisa de campo foi realizada por meio de um questionário contendo 36 questões amplas e abrangentes, sendo 5 dissertativas e 31 objetivas, sendo todas respondidas, foram trazidas à baila as mais relevantes para a composição do artigo.

O primeiro item no questionário foi o Termo de Consentimento Livre e Esclarecido (TCLE), sendo registradas todas as pessoas que aceitaram o TCLE (45), no entanto somente 39 identificaram-se como Profissionais de ISP e puderam dar seguimento. Os participantes eram Policiais Militares (27), do Ministério Público Estadual (4), Policiais Civis (3), Poder Judiciário Estadual (2), Policiais Federais (2), Força Aérea Brasileira (1). A maioria dos Profissionais de ISP atuam Paraná (82,1%), os demais são do Distrito Federal (7,7%), Mato Grosso (5,1%), Minas Gerais (2,6%) e Rio Grande do Norte (2,6%).

Sendo perguntado os tipos de crimes contidos no Código Penal interceptados, foi respondido que os crimes mais interceptados foram contra pessoa, patrimônio e administração:

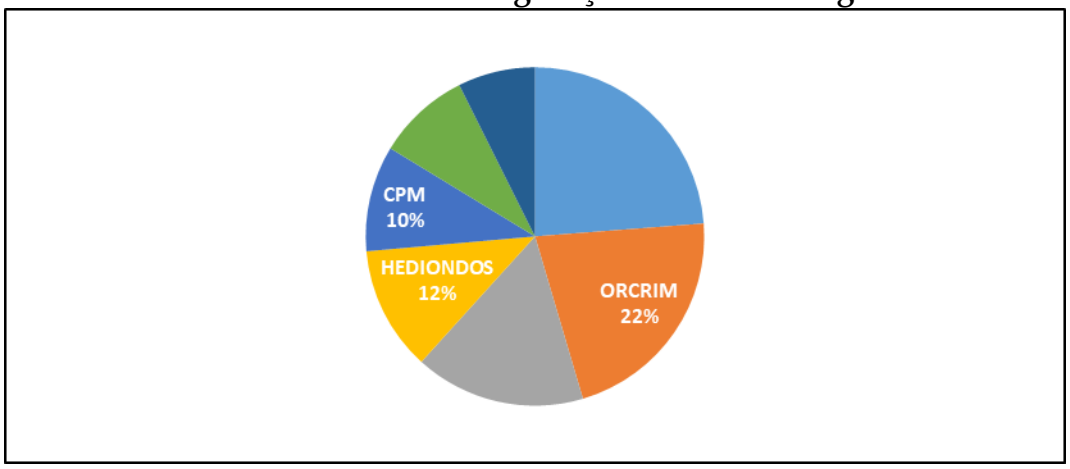
Gráfico 01 – **Tipificações do Código Penal**



Fonte: os autores (2022)

Sobre as legislações penais extravagantes que fundamentaram as interceptações, houve as seguintes respostas:

Gráfico 02 – **Legislação Penal Extravagante**



Fonte: os autores (2022)

Destacam-se assim, as leis que tratam do tráfico de entorpecentes, organização criminosa, o desarmamento, dos crimes hediondos e o Código Penal Militar.

À pergunta sobre o tipo de equipamento durante as ações, responderam utilizarem: equipamentos híbridos (*hardware* e *software*) foram utilizados em 37% das ações, os digitais (26%), *software* (16%), *hardware* (10%) e analógicos (10%). Considerando que os mais desenvolvidos são do tipo híbrido, percebe-se a defasagem tecnológica dos equipamentos em uso.

A necessidade de intermediação de companhias telefônicas nas interceptações é uma realidade para 94,5% dos entrevistados. Essa situação pode gerar morosidade nas ações e consequências trágicas pela falta de celeridade, tanto que 89,7% concordaram que a interceptação telefônica poderia ser realizada sem a participação das operadoras.

Perguntado se o equipamento utilizado pelo participante era capaz de interceptar dados de *smartphones,* somente 10,3% concordavam totalmente, e outros 28,2% concordaram parcialmente, aparentemente demonstrando que tais equipamentos estão tecnologicamente defasados. Sendo perguntado sobre a possibilidade de utilizar os *smartphones* dos alvos como microfone e câmeras, 65,8% responderam que não gravam nada, e 26,3% responderam que não ter conhecimento sobre essa função.

A insatisfação do equipamento disponível ficou demonstrada quando somente 7,7% dos entrevistados responderam estarem muito satisfeitos com o equipamento utilizado, enquanto 15,4% muito insatisfeitos, 33,3% insatisfeitos, 7,7% indiferentes e 35,9% pouco satisfeitos.

Numa das questões dissertativas, foi solicitado citar as principais funcionalidades dos equipamentos utilizados, obtendo as seguintes respostas: captura de áudio, mensagens de texto, localização em tempo real, extração dos dados dos aparelhos apreendidos, acesso a registros de chamadas e mensagens SMS, interceptação de conversações telefônicas e gravação das chamadas, histórico de ligações e obtenção de dados telemáticos, praticidade básica. Essas funções clássicas coincidem com o que a *NSO GROUP* (2014) destaca como obstáculos e falta de atualização dos sistemas de interceptação, assim como as deficiências destacadas pelos entrevistados, os quais elencaram: poucas funções para uso, ausência de manutenção e reparo, não fornece localização com precisão, não capta imagens e sons

ambiente, dificuldade de acesso aos vínculos dos alvos, pouco acesso aos *smartphones*, aplicativos criptografados, sem acesso a chamadas por IP, restrição de dados vinculados à *internet* e tecnologia ultrapassada.

Os participantes sugeriram funções essenciais ou desejáveis nos equipamentos de interceptação, sendo destacadas: acesso aos aplicativos e funções dos *smartphones;* acesso a dados, imagens, áudios e localização com horários, em tempo real ou posterior; acesso às contas em nuvens e *e-mail*s; monitoramento remoto; armazenamento e velocidade de processamento das informações; gravação de vídeo e som ambiente, quebra de criptografias; extratos de chamadas; dados cadastrais do terminal do alvo e interlocutores; desvio de chamada em tempo real.

Na pesquisa realizada com os profissionais de ISP, ficou evidente que os equipamentos disponíveis atualmente possuem deficiências ou necessitam de atualização para o amplo acesso aos *smartphones,* sobretudo, aos aplicativos, microfones e câmeras em tempo real, dados armazenados remotamente. Sendo possível tais ações com os equipamentos disponíveis somente de maneira física, depois de apreender o *smartphone*.

Perguntado sobre a funcionalidade do *Pegasus*. 59% dos entrevistados responderam que o desconhecem, 28% que o conhecem pouco, e 12% que o conhecem. Nenhuma pessoa respondeu que conhece bem ou conhece todo o funcionamento do *Pegasus*. Isso demonstra que esse *software* é uma novidade para os Profissionais de ISP do Brasil.

Nenhum dos participantes (00%) possui o *Pegasus* em seu setor de trabalho e somente um deles teve acesso ao *software.*

Foram listados, no enunciado de uma pergunta, os principais benefícios do *Pegasus:* interceptação remota, coleta completa de dados de *smartphone*, acesso sem intermédio de companhia telefônica, uso de microfone e câmera. Em seguida, afirmou-se que o *Pegasus* era ideal para a atividade de ISP. A maioria concordou (92,9%), 01 participante respondeu ser indiferentes (2,6%), e 2 discordaram parcialmente (5,1%).

Sobre a necessidade de adequação da Lei nº 9.296/1996, 89,70% concordaram que a Lei deve passar por adequações, (84,6% totalmente e 5,1 %

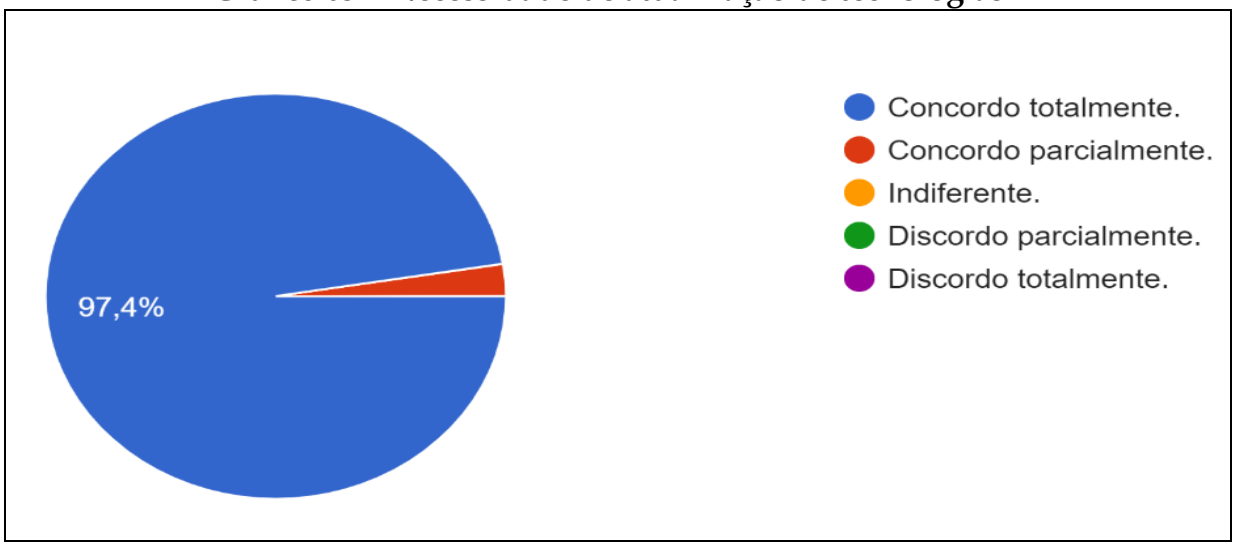
parcialmente), 7,7% discordaram parcialmente e os demais responderam ser indiferentes (2,6%).

Ao serem questionados sobre a necessidade de alterações na Lei nº 9.296/1996, os profissionais de ISP sugeriram as seguintes mudanças: retirada das operadoras de telefonia do processo de interceptação devido à burocracia e à morosidade; em casos de urgência e emergência, acesso à localização por ERB sem necessidade de ordem judicial ou criação de plantão judicial; aumento do prazo de interceptação telefônica que hoje é de 15 dias; mecanismos para que as empresas sediadas em outros países sejam obrigadas a fornecer os dados solicitados; previsão legal para os policiais militares executarem interceptações telefônicas em cumprimento da missão constitucional de Segurança Pública.

Perguntado se a interceptação telefônica é indispensável para o combate à criminalidade, havendo concordância em 100% das respostas, pois (89,7% concordam totalmente e 10,3% concordam parcialmente).

Por fim, da afirmativa de que é extremamente necessária a atualização constante de tecnologia na interceptação telefônica, sendo respondido o seguinte:

Gráfico 03 – **Necessidade de atualização de tecnologias**



Fonte: os autores (2022)

Os dados anteriores demonstram a necessidade da evolução tecnológica para o exercício das funções inerentes à ISP no combate à criminalidade.

CONCLUSÃO

O artigo demonstra o advento da evolução tecnológica e dos meios de comunicação ocorrida nos últimos anos. A rede *internet* democratizou informações em todos os campos de atuação. Os aparelhos de telefone evoluíram com o desenvolvimento dos *smartphones,* agregando telefonia e transmissão de dados, trazendo a informação para a palma da mão de seus usuários, em atividades lícitas e ilícitas.

Considerando que a Atividade de ISP tem em seu arcabouço de atuação a Produção de Conhecimento e necessita de meios de obtenção de dados, o objetivo geral da pesquisa foi analisar as implicações operacionais e legais para a implantação do *Pegasus* como meio de obtenção de dados, sendo alcançado o objetivo sob os dois aspectos, operacional e legal.

Os objetivos específicos também foram alcançados, à medida que foi contextualizado o tema à revolução digital, analisados os conceitos das principais categorias do estudo, analisada a Lei nº 9.296/1996, identificadas as principais formas de interceptações, esclarecida a legalidade de ações de interceptação telefônica, as principais carências legislativas e deficiências dos meios de obtenção de dados disponíveis pela pesquisa de campo.

Para compreender a necessidade de uso de um equipamento eficiente como o *Pegasus*, foram abordados importantes conceitos relacionados à Inteligência, a qual é dividida em Inteligência e Contrainteligência. Tais atividades atuam na Produção de Conhecimento e uma de suas fases é a obtenção de dados, que pode ser obtida pela interceptação de sinais, imagens ou dados.

Respeitada a inviolabilidade do sigilo de comunicações, em casos específicos, tal garantia pode ser ponderada e excepcionalizada, principalmente em casos de determinação judicial. Legal e doutrinariamente, a Interceptação Telefônica abrange a comunicação pelo clássico telefone e pelos tecnológicos *smartphones* conjugados aos aplicativos de comunicação e *internet.*

Operacionalmente, os meios de obtenção de dados utilizados atualmente dependem das companhias telefônicas e de outras empresas para ações de

interceptação telefônica, telemática e de dados, resultando em limitação e morosidade nessas ações, tendo em vista a restrição às mídias da *internet*, os dados são repassados pelas empresas ou disponibilizados por *login* e senha.

Verificou-se que a principal legislação sobre interceptação telefônica, Lei nº 9.296/1996, impõe condições para realizá-la, no entanto ela não foi atualizada para a oportunidade e imediatismo em que acontecem os fatos, dificultando que haja pronta resposta por parte da Atividade de ISP no enfrentamento da criminalidade.

De acordo com o contido na pesquisa, o *Pegasus* possibilita o acesso ilimitado aos dispositivos, interceptação de chamadas, quebra de criptografia, monitoramento de aplicativos, utilização de câmera e microfone, ação invisível e sem necessitar do intermédio das operadoras de telefonia. Esses fatores agilizariam as ações de ISP em benefício da coletividade no enfrentamento a condutas ilícitas, mas seu uso precisa ser limitado e regulamentado para evitar uso ilegal ou arbitrário como relataram as notícias expostas.

A instalação do agente oculto no dispositivo digital pode acontecer de várias maneiras, mas destaca-se a instalação *over-the-air* que acontece sem a participação do usuário, conhecido como zero clique, além das quebras de criptografias e dispositivos de segurança.

Pela pesquisa de campo, foi possível constatar as maiores incidências de tipificações pelo Código Penal sujeitas a interceptação, sendo: crimes contra pessoa, patrimônio e administração. As decorrentes de legislação extravagantes são: crimes de tráfico de entorpecentes, organização criminosa, estatuto do desarmamento, crimes hediondos, financeiros, licitações e crimes militares.

Constatou-se que os equipamentos utilizados pela ISP estão ultrapassados e necessitam de intermédio das operadoras. A maioria dos meios disponíveis não gravam som e/ou imagem do dispositivo, nem mesmo tem acesso aos aplicativos dos *smartphones*.

Foram colhidas sugestões de funções para os meios de obtenção de dados, as quais estão descritas nas funcionalidades do *Pegasus.* Quase a totalidade dos participantes afirmaram que o *Pegasus* seria ideal para a atividade de ISP.

Sobre a legislação para interceptação telefônica, foi constatada a necessidade de adequação da atual legislação, tendo havido sugestões de relativização de autorização judicial para determinadas necessidades ou criação de plantão judicial para casos de urgência, medidas que sujeitem as empresas estrangeiras fornecerem dados e previsão legal para policiais militares executarem interceptações em ações de Segurança Pública. Todos os participantes concordaram que a interceptação telefônica é indispensável para o combate à criminalidade, por isso é extremamente necessária a atualização dos equipamentos da ISP.

Muito embora o tema seja polêmico, ainda é pouco debatido, demonstra a vulnerabilidade dos meios de comunicação e se relaciona com a Atividade de ISP, a qual tem o sigilo como característica em determinadas situações, fazendo com que a obtenção e socialização de conhecimentos seja um grande desafio.

Considerando que o tema abordado tem um aspecto interdisciplinar, abre-se um vasto campo de perspectivas para a realização de novas pesquisas relacionadas ao assunto, no aspecto ativo ou passivo, na condição de investigador ou investigado, na condição de Profissional de ISP, Profissional alvo detentor de direitos, desde a garantia da legalidade ou desvio de função.

Podem ser realizados estudos futuros sobre as funções do *Pegasus*, ou sobre os aspectos relacionados às consequências de seu uso no campo das Ciências Policiais. Não há de se olvidar do poderio do *Pegasus*, sendo necessárias novas pesquisas do regime jurídico das interceptações, destacando os Direitos e Garantias Fundamentais de inviolabilidade de comunicação, intimidade, vida privada e imagem de pessoas. Outro importante objeto de pesquisa é sobre o papel do Estado no controle de comunicações frente a empresas privadas.

A contribuição científica resume-se em somar o pensamento crítico do atual momento às tecnologias de comunicação, afirmando que não existe sigilo absoluto, pois os dados já são compartilhados de várias formas. O *Pegasus* é um poderoso meio de obtenção de dados, não é o único. O desenvolvimento dessas tecnologias é natural, resta-nos estudar tais fenômenos.

Os resultados da pesquisa comprovaram a hipótese de que houve grande desenvolvimento tecnológico dos meios de comunicação e não houve

acompanhamento tecnológico na mesma proporção para ações de interceptação telefônica.

Finalmente, o estudo confirma que o *Pegasus* possui grande poder de interceptação de dados, pode ser recepcionado para a atividade de ISP do Brasil, tendo grandes expectativas para resultados positivos, sem descartar a necessidade de atualização legislativa de regulamentação.

REFERÊNCIAS

ALJAZEERA. ***WhatsApp can sue Israeli firm NSO Group, US appeals court rules.*** Disponível em: https://www.aljazeera.com/news/2021/11/8/whatsapp-can-sue-israeli-firm-nso-group-us-appeals-court-rules. Acesso em 24 mar. 2022.

ALMEIDA, José Maria Fernandes. Breve História da Internet**. Caderno Legis,** Brasília, n. 48. p. 11-45, Janeiro/Abril, 2013. Editora Universidade do Minho. Departamento de Sistemas de Informação. 2005. Disponível em: http://hdl.handle.net/1822/3396. Acesso em: 30 out. 2021.

ANDRADE, Felipe Scarpelli. Inteligência, Interceptação e Soberania: viabilidade jurídica do monitoramento de sinais sobre estrangeiros nocivos ao país. *In:* HAMADA, H. H. MOREIRA, R. P. **Inteligência de segurança pública: contribuições doutrinarias para o cotidiano policial**. Belo Horizonte. Editora D´Plácido, 2017. p. 107-124.

BLACKHAT. ***Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks.*** 2016. Disponível em: https://www.blackhat.com/docs/eu-16/materials/eu-16-Bazaliy-Mobile-Espionage-in-the-Wild-Pegasus-and-Nation-State-Level-Attacks.pdf. Acesso em: 30 out. 2021.

BRASIL, Supremo Tribunal Federal. (2. Turma). **Habeas Corpus nº 96986/MG**. Relator: Min. Gilmar Mendes, 15 maio. 2012. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur214433/false. Acesso em 30 mar. 2022

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 30 out. 2021.

BRASIL. **Decreto nº 10.777, de 24 de agosto de 2021. Institui a Política Nacional de Inteligência de Segurança Pública.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10777.htm> Acesso em: 30 out. 2021.

BRASIL. **Lei nº 12850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, meios de prova, infrações penais e correlatas e o procedimento criminal.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm Acesso em 21 mar. 2022.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 30 mar. 2022

BRASIL. **Lei nº 4.117, de 27 de agosto de 1962. Institui o Código Brasileiro de Telecomunicações.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4117compilada.htm. Acesso em: 16 fev, 2022.

BRASIL. **Lei nº 9296, 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 30 mar. 2022

BRASIL. Ministério da Justiça **Doutrina Nacional de Inteligência de Segurança Pública – DNISP.** 4. ed. rev. e atual. Brasília. Secretaria Nacional de Segurança Pública, 2014.

BULFINCH, Thomas. **O livro de ouro da mitologia (a idade da fábula):** história de deuses e heróis. Tradução de David Jardim Junior. 26.ed. Rio de Janeiro. Ediouro, 2002. Título Original: *The Age of Fable.*

FLICK, Uwe. **Uma introdução à pesquisa qualitativa.** Tradução Joic Elia Costa. 3. ed. Porto Alegre: Bookman, 2009. Título Original: *Qualitative Sozialforschung. Eine Einführung*.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Tradução Raquel Ramalhete. Vozes. Petrópolis, 2004. Título Original: *Surveiller er punir*.

GARZELLA, Oleno Carlos Faria *et al.* **Manual de Interceptação Telefônica e Telemática.** 2 ed. rev., atual. e ampl. São Paulo. Editora JusPodivm, 2021.

GAZETA DO POVO. ***Pegasus*: o que se sabe sobre o *software* que teria sido usado para espionar jornalistas e ativistas.** Disponível em: https://www.gazetadopovo.com.br/mundo/pegasus-o-que-se-sabe-sobre-o-software-que-teria-sido-usado-para-espionar-jornalistas-e-ativistas/. Acesso em: 17 out. 2021.

GOMES, Raimundo de Albuquerque. **Cadeia de Custódia das Interceptações Telefônicas: forma de controle epistemológico da prova no processo penal.** Londrina, PR, Thoth, 2021.

GRINOVER, Ada Pelegrini. O Regime brasileiro das interceptações telefônicas. *In:* **Revista de direito administrativo,** n. 207, jan./mar. 1997. São Paulo. Revista dos Tribunais. p. 21-38.

GRINOVER, Ada Pellegrini. **Provas ilícitas, interceptação e escutas.** Brasília: Gazeta Jurídica, 2013.

HAN, Byung-Chul. ***En el enjambre.*** *Traducción de* Raul Gabás. Barcelona. Herder, 2014. Título Original: *Im Schwarm*.

HOUAISS. **Grande Dicionário Houaiss.** Disponível em: https://houaiss.uol.com.br/corporativo/apps/uol_www/v6-0/html/index.php#0. Acesso em 30 mar.2022

IBGE. **Pesquisa Nacional por amostra de Domicílios Contínua - PNAD**. 2018**.** Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101543.pdf. Acesso em: 30 out. 2021.

JENKINS, Henry. **Cultura da Convergência.** 2. ed. Tradução Susana Alexandria. Editora Aleph. São Paulo, 2009. Titulo original: *Convergenceculture*.

KENT, Sherman. ***Strategic Intelligence:*** *for American World Policy.* Hamden, Connecticut. Archon Books, 1965.

KWON, Min. *et al*. ***Development and validation of a smartphone addiction scale.*** Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0056936. Acesso em: 25 mar. 2022.

LEMOS, André. **Cibercultura:** tecnologia e vida social na cultura contemporânea. Porto Alegre. Sulina, 2013.

LIKERT, Rensis. ***A Technique for the Measurement of Attitudes.*** v. 140. New York. R. S. Woodwort, 1932. Disponível em: https://legacy.voteview.com/pdf/Likert_1932.pdf. Acesso em 02 fev. 2022.

LIMA, Renato Brasileiro de. **Manual de Processo Penal.** Volume único. 8. ed. Salvador. Editora JusPodivm, 2020.

LINS, Bernardo Felipe Estellita. **A evolução da *Internet:*** uma perspectiva histórica. Associação dos Consultores Legislativos e de Orçamento e Fiscalização Financeira da Câmara dos Deputados, 2013. Disponível em: https://bd.camara.leg.br/bd/handle/bdcamara/33179. Acesso em 30 mar. 2022.
LONGO, Walter. ***Marketing*** **e comunicação na era pós-digital:** as regras mudaram. São Paulo, HSM do Brasil. 2014.

MEIRELLES, Fernando de Souza. **Uso da TI - Tecnologia de Informação nas Empresas:** Pesquisa Anual do FGVcia 32. ed. 2021. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2021pesti-relatorio.pdf. Acesso em: 17 out. 2021.

MOODY´S. ***Rating Action: Moody's downgrades NSO to B3 with negative outlook.*** Disponível em: https://www.moodys.com/research/Moodys-downgrades-NSO-to-B3-with-negative-outlook--PR_446947. Acesso em: 20 mar. 2022.

MORAIS FILHO, Daniel Cordeiro de. **Um convite à matemática.** Campina Grande. EDUFCG, 2007.

MORETTI, Alessandro. **Inteligência no Combate ao crime organizado.** 2009. 161 p. Monografia (Especialização em Inteligência de Estado e Inteligência de Segurança Pública com Inteligência Competitiva) - Escola Superior do Ministério Público de Minas Gerais e Centro Universitário Newton Paiva. Belo Horizonte, 2009.

NSO GROUP. ***Pegasus - Product Description.*** **2**014. Disponível em: https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf. Acesso em: 20 mar. 2022.

NUCCI, Guilherme de Souza. **Curso de Direito Processual Penal**. 15 ed. Rio de Janeiro: Editora Forense, 2017.

PANANÁ. Tribunal de Justiça do Estado do Paraná. **Habeas Corpus nº 1.602.684-7 (Acórdão).** 5ª Câmara Criminal. Relatora Desembargadora Maria Thereza de Assis Moura. 3 jul. 2015. Disponível em: https://tj-pr.jusbrasil.com.br/jurisprudencia/421816067/habeas-corpus-hc-16026847-pr-1602684-7-acordao. Acesso em 30 mar. 2022.

RONDON FILHO, Edson Benedito. As matrizes de Inteligências. *In:* CASTRO, Clarindo Alves de; RONDON FILHO, Edson Benedito (coord.). **Inteligência de Segurança Pública.** 1. ed. Curitiba. Juruá, 2009. p. 41-58.

RONDON FILHO, Edson Benedito. Processo Cíclico de Inteligência. *In:* CASTRO, Clarindo Alves de; RONDON FILHO, Edson Benedito (coord.). **Inteligência de Segurança Pública.** 1. ed. Curitiba. Juruá, 2009. p. 113-136.

SAFE. ***Detecting and protecting your smartphone from PEGASUS Spyware.*** Disponível em: http://www.terralogic.com/detect-and-protect-your-smartphone-from-pegasus-software/. Acesso em 30 out. 2021.

THE HACK. ***Pegasus*****: vazamento de dados de *spyware israelense revela mais de 50 mil vítimas de governos autoritários.*** Disponível em: https://thehack.com.br/vazamento-de-dados-de-mais-de-50-mil-vitimas-revela-spyware-israelense-usado-para-atingir-ativistas-jornalistas-e-lideres-politicos-em-todo-o-mundo/. Acesso em: 30 out 2021.

THE NEW YORK TIMES**.** ***Israeli Spyware Maker Is in Spotlight Amid Reports of Wide Abuses.*** Disponível em:

https://www.nytimes.com/2021/07/18/world/middleeast/israel-nso-pegasus-spyware.html. Acesso em 17 de out. de 2021.

THE WASHINGTON POST. ***The Pegasus Project: A global investigation -*** *Q&A: A guide to 'spyware'.* Disponível em: https://www.washingtonpost.com/technology/2021/07/18/what-to-know-spyware-pegasus/. Acesso em: 20 mar. 2022.