REVISTA ESMAT
26

INVESTIGAÇÃO CRIMINAL TECNOLÓGICA: A ATUAÇÃO DA POLÍCIA JUDICIÁRIA CIVIL DO TOCANTINS NA INVESTIGAÇÃO DO ESTUPRO VIRTUAL

TECHNOLOGICAL CRIMINAL INVESTIGATION: THE ROLE OF THE TOCANTINS CIVIL JUDICIAL POLICE IN INVESTIGATING VIRTUAL RAPE

Luís Gonzaga da Silva Neto

Mestre em Prestação Jurisdicional e Direitos Humanos, pela Escola Superior da Magistratura Tocantinense (ESMAT) e Universidade Federal do Tocantins (UFT). Mestrando em Gestão de Políticas Públicas, pela Universidade Federal do Tocantins (UFT). Especialista em Ciências Criminais, pela Pontifícia Universidade Católica de Minas Gerais (PUC/Minas). Especialista em Direito de Polícia Judiciária, pela Academia Nacional de Polícia (ANP). Especialista em Gestão Política e Gestão em Segurança Pública, pela Universidade Federal do Tocantins (UFT). Graduado em Direito pela Faculdade de Alagoas (FAL). Delegado de Polícia Civil no Estado do Tocantins

RESUMO

O presente artigo analisa desafios enfrentados pela Polícia Judiciária do Tocantins no âmbito da investigação criminal do estupro virtual, o que inclui a coleta da evidência digital e demais atividades de perícia criminal. Utiliza abordagem qualitativa, por meio da análise da doutrina e jurisprudência atual sobre o tema. Os crimes que ocorriam exclusivamente no mundo físico-material migraram para o ciberespaço, o que trouxe novos desafios para sua devida adequação ilícito-típica. No caso dos crimes sexuais não foi diferente, uma vez que a gama de condutas delituosas violadoras da dignidade sexual passaram a ser cometidas em grande escala no ambiente cibernético, dentre elas o "estupro virtual". Em cotejo com o princípio da legalidade, o artigo apura se o tipo penal de estupro (arts. 213 e 217-A do Código Penal), pode se materializar no ciberespaço. Verifica obstáculos enfrentados pela Polícia Civil do Tocantins na investigação de crimes sexuais virtuais. Investiga as técnicas e as ferramentas utilizadas pela Polícia Judiciária na investigação de tais crimes. Como resultados, aponta que a doutrina e a jurisprudência admitem a prática do crime de estupro em sua forma virtual, em face da prescindibilidade do contato físico entre autor e vítima para sua consumação, apesar da necessidade de melhor tipificação

legislativa da conduta, em observância ao princípio da taxatividade. Conclui que o estupro virtual é possível devido à natureza do delito e à desnecessidade de contato corporal entre autor e vítima, embora ressalte a necessidade de aprimoramento da legislação para melhor enfrentar os desafios impostos pelos crimes cibernéticos.

Palavras-Chave: Polícia Judiciária. Polícia Civil do Tocantins. Estupro Virtual. Investigação Criminal.

ABSTRACT

This article analyzes challenges faced by the judicial police of Tocantins in the context of the criminal investigation of virtual rape, which includes the collection of digital evidence and other activities of criminal expertise. It uses a qualitative approach, through the analysis of current doctrine and jurisprudence on the subject. Crimes that occurred exclusively in the physical-material world migrated to cyberspace, which brought new challenges for their proper illicit-typical adequacy. In the case of sexual crimes, it was no different, since the range of criminal conducts that violate sexual dignity began to be committed on a large scale in the cyber environment, among them "virtual rape". In comparison with the principle of legality, the article investigates whether the criminal type of rape (arts. 213 and 217-A of the Penal Code) can materialize in cyberspace. It verifies obstacles faced by the Civil Police of Tocantins, in the investigation of virtual sexual crimes. It investigates the techniques and tools used by the judicial police in the investigation of such crimes. As a result, it points out that the doctrine and jurisprudence admit the practice of the crime of rape in its virtual form, in view of the dispensability of physical contact between author and victim for its consummation, despite the need for a better legislative typification of the conduct, in compliance with the taxation principle. It concludes that virtual rape is possible due to the nature of the crime and the lack of body contact between author and victim, although it emphasizes the need to improve legislation to better face the challenges posed by cyber crimes.

Keywords: Judiciary Police. Civil Police of Tocantins. Virtual Rape. Criminal Investigation.

1 INTRODUÇÃO

Contemporaneamente, a criminalidade tem buscado aperfeiçoar as suas condutas delituosas, migrando as suas ações para outros ambientes, como é o caso do ciberespaço que passou a ser o campo de atuação de vários criminosos, fato este que reclama um adequado preparo das forças policiais, seja em relação à estrutura material ou mesmo à capacitação dos respectivos policiais, buscando com isso assegurar mais eficiência no trabalho investigativo.

A Polícia Judiciária deve buscar atuar no ciberespaço com expertise e eficiência investigativas, pois resta latente que os crimes cometidos no ambiente cibernético são cada vez mais frequentes e com elevado grau de sofisticação, exigindo dos órgãos estatais de investigação o uso de instrumentos adequados para combater referida criminalidade moderna.

No cerne dos crimes cometidos no ambiente cibernético, discute-se sobre a possibilidade da prática do crime de estupro virtual, e o debate gira em torno da ausência de contato físico-sexual entre autor e vítima, além da possível violação ao princípio da legalidade, especificamente da taxatividade legal, pois o tipo penal do crime de estupro não abarcaria o seu respectivo cometimento no ciberespaço.

Ademais, é de suma importância a análise da jurisprudência em relação à admissibilidade da prática do crime de estupro no ambiente virtual, averiguando casos concretos ocorridos no Brasil e no Tocantins onde se discutiu referida possibilidade. Logo, o presente artigo se desenvolverá por meio da verificação da doutrina e da jurisprudência em relação à admissibilidade dos crimes de estupro e estupro de vulnerável no ambiente cibernético, tratando-se de uma pesquisa de cunho qualitativo.

De mais a mais, procedeu-se a entrevistas de campo[1], citadas no decorrer do artigo, sendo estas realizadas com as chefias da Divisão de Repressão a Crimes Cibernéticos (DRCC), do Núcleo de Computação Forense, ambos da Polícia Civil do Estado do Tocantins, além das delegadas titulares da 8ª Delegacia Especializada de Atendimento à Mulher e Vulneráveis (DEAMV), de Porto Nacional/TO, e da Divisão de Inteligência do Núcleo de Inteligência e Segurança Institucional do Tribunal de Justiça do Estado do Tocantins, e do delegado-geral da Polícia Civil do Tocantins, com o escopo de compreender os desafios enfrentados pela Polícia

1 Entrevistas concedidas por Lucas Brito Santana, Leila Diniz Alves, Fernanda de Siqueira Correia, Milena Santana de Araújo Lima e Claudemir Luiz Ferreira, em Palmas/TO, nos meses de julho e agosto de 2023. O Sr. Santana é delegado-chefe da Divisão de Repressão a Crimes Cibernéticos (DRCC) de Palmas/TO, a Sra. Alves é perita-chefa do Núcleo de Computação Forense da Polícia Civil do Tocantins, a Sra. Correia é delegada-chefa da 8ª Delegacia Especializada de Atendimento à Mulher e Vulneráveis de Porto Nacional/TO, a Sra Lima é lotada na Divisão de Inteligência do Núcleo de Inteligência e Segurança Institucional do Tribunal de Justiça do Estado do Tocantins e o Sr. Ferreira é delegado-geral da Polícia Civil do Tocantins.

Judiciária civil tocantinense na investigação de crimes sexuais cometidos no ambiente cibernético, especialmente o crime de estupro virtual, além das ferramentas disponíveis para os deslindes investigativo e pericial.

Da mesma forma, a reunião de elementos probatórios para fins de comprovação da prática delitiva trata-se de grande desafio para a Polícia Judiciária, porque se analisa a existência de possíveis obstáculos para a asseguração da cadeia de custódia da evidência digital, tendo como recorte a verificação do quadro estrutural e de qualificação de pessoal da Polícia Civil do Estado do Tocantins.

Ainda, analisam-se os tipos penais dos crimes de estupro (art. 213 do Código Penal) e de estupro de vulnerável (art. 217-A), no que tange à compatibilidade como o meio de execução perpetrado no ambiente cibernético. Será proposto um aprimoramento dos respectivos tipos penais, visando com isso aniquilar proposições que levantam uma suposta violação à legalidade penal em seu corolário da taxatividade, trazendo segurança jurídica e estabilidade legal.

Outrossim, será tratado sobre a questão que gira em torno da extorsão sexual em relação ao crime de extorsão (delito patrimonial) quando praticada com o fim de obtenção de lucro, ainda que ocorra paralelamente o delito sexual.

Posto isso, este artigo trata sobre o conceito, características e a tipificação do estupro virtual, além de serem apresentadas técnicas e ferramentas utilizadas pela Polícia Judiciária na investigação da prática delituosa em tela. Na mesma toada, analisar-se-á a legislação atual no que se refere ao tratamento do estupro praticado no ciberespaço, e serão propostas melhorias no texto legal com o escopo de fortalecer a investigação e combate à prática delituosa em epígrafe.

Ainda, busca-se identificar os desafios enfrentados pela Polícia Civil do Tocantins na coleta de provas digitais e em relação ao rastreamento de criminosos, como também proceder-se-á à avaliação da efetividade das ações da Polícia Judiciária tocantinense no que tange à proteção das vítimas de estupro virtual.

2 ANÁLISE DA LEGISLAÇÃO ATUAL EM RELAÇÃO À TIPIFICAÇÃO DO CRIME DE ESTUPRO VIRTUAL

Os crimes sexuais consistem em temática bastante relevante no âmbito dos tipos penais incriminadores, especialmente por tutelar o bem jurídico "dignidade sexual"; até pouco tempo referido grupo de condutas delituosas eram classificadas pelo legislador como "crimes contra os costumes". Ocorre que, com o advento da Lei nº 12.015, de 2009, houve uma mudança paradigmática de visão jurídica e social sobre referido espectro legislativo, passando a ser levado em consideração o aspecto da dignidade sexual, conectando-se à noção de dignidade humana, como sendo algo inerente a todo ser humano.

Ao discorrer sobre a mudança legislativa alhures, Masson (2018) ressalta que a expressão "crimes contra os costumes" era excessivamente conservadora, ha-

vendo certa imposição por parte do Estado da forma como a sociedade deveria se comportar no campo sexual, além de revelar-se bastante preconceituosa referida visão, cujo foco principal recaía sobre as mulheres. De fato, apenas a chamada "mulher honesta" era protegida por poucos tipos penais, não sendo dada exigência comportamental sobreposta aos homens.

A Lei nº 12.015, de 2009, também promoveu a revogação do tipo penal do atentado violento ao pudor, que era descrito no art. 214 do Código Penal, tratando-se de revogação puramente formal, tendo em vista que a conduta típica, em seu aspecto material, permaneceu incriminada, mas agora sob nova roupagem, migrando os seus elementos típicos para o crime de estupro tipificado no art. 213, materializando-se o fenômeno da continuidade normativo-típica.

A novel legislação citada inseriu no diploma penal o crime de estupro de vulnerável no art. 217-A, abolindo-se a presunção de violência nos crimes sexuais, por meio da revogação do art. 224 do Código Penal. No estupro com violência presumida, a adequação típica era mediata, pois se cumulava o disposto no art. 213 com a norma de extensão prevista no art. 224 do Código Penal.

Atualmente, com as mudanças empreendidas pela Lei nº 12.015, de 2009, há dois crimes diversos, cuja incidência dependerá do perfil do sujeito passivo. Na hipótese de a vítima ser pessoa vulnerável, aplica-se o art. 217-A, nas demais situações será aplicado o tipo penal do art. 213, ambos do Código Penal. Analisando os tipos penais em tela, percebe-se que não há previsão expressa de suas respectivas práticas no âmbito do ciberespaço. Sendo assim, passemos à análise acurada de cada um deles, com vista a verificar a possibilidade do cometimento no ambiente virtual.

2.1 Estupro (art. 213 do Código Penal)

O crime de estupro encontra-se tipificado no art. 213 do Código Penal, cuja redação afirma, *in verbis:* "Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso". Trata-se de crime bicomum, podendo ser praticado por qualquer pessoa, não exigindo nenhuma qualidade específica do sujeito ativo do crime, como também qualquer pessoa poderá figurar como vítima do estupro.

Além disso, o crime em tela é material ou causal, pois para a sua consumação é imprescindível a ocorrência do resultado naturalístico. Ainda, trata-se de crime de forma livre, pois o legislador não previu forma vinculada para a sua prática, comportando qualquer meio de execução capaz de ocasionar a prática delituosa.

Conforme já debatido, há uma grande celeuma jurídica em torno da viabilidade da prática do crime de estupro no ambiente virtual, residindo o debate na (in)observância do princípio da legalidade. Como é de conhecimento geral, só

há crime quando definido em lei, e se verificarmos toda a legislação, não há nada previsto sobre o crime de estupro virtual.

O *nomen iuris* "estupro virtual", de acordo com o já exposto, é bastante criticado, primeiro porque o crime de estupro cometido no ambiente cibernético é conduta real e não algo metafísico (virtual); segundo, o estupro é real porque apenas a forma de sua execução é que se dá no meio virtual, não havendo o surgimento de uma nova conduta criminosa, até mesmo porque a incriminação de novas condutas depende de lei em sentido estrito.

Apesar da problemática existente, não se mostra necessária a criação de um novo tipo penal tipificando o crime de estupro virtual, tendo em vista que o disposto no art. 213 é suficiente para abarcar a conduta cometida no ambiente cibernético, especialmente pelo fato de que, conforme será analisado adiante, a doutrina e a jurisprudência são uníssonas no que se refere à prescindibilidade do contato físico-erótico entre autor e vítima, o que permite a admissão da prática delituosa à distância, com a conectividade entre autor e vítima pela rede mundial de computadores.

Ademais, para espancar qualquer tipo de questionamento, seria de bom alvitre a previsão expressa da possibilidade de prática do estupro no ambiente virtual, o que poderia vir disposto no próprio caput do art. 213 ou mesmo em um parágrafo prevendo o cometimento da conduta no ambiente virtual, podendo ser da seguinte maneira: "Incorre na mesma pena do caput a conduta de constranger alguém, mediante grave ameaça, por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, a praticar ou permitir que com ele se pratique ato libidinoso".

2.2 Estupro de Vulnerável (art. 217-A do Código Penal)

O crime de estupro de vulnerável encontra-se previsto no art. 217-A do Código Penal, cuja redação dispõe, *in verbis*: "Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos (...) Incorre na mesma pena quem pratica as ações descritas no caput com alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência".

Diferentemente do crime de estupro tipificado no art. 213 do Código Penal, o estupro de vulnerável não prevê como elementos do tipo penal a conduta de constranger alguém mediante violência ou grave ameaça, bastando que o sujeito ativo pratique ato libidinoso com alguma das vítimas dispostas no dispositivo incriminador e desde que se enquadrem na condição de vulnerável.

O estupro de vulnerável é crime comum, podendo ser praticado por qualquer pessoa, não exigindo nenhuma qualidade específica do sujeito ativo. No que se

refere ao sujeito passivo, trata-se de crime próprio, pois apenas a pessoa considerada vulnerável poderá figurar como vítima do crime em epígrafe.

Da mesma forma que o crime de estupro do art. 213, o delito de estupro de vulnerável é crime de forma livre, admitindo-se a sua prática com a utilização de qualquer meio e execução. Logo, é plenamente possível o cometimento do crime por meio do ambiente virtual, especialmente por não se exigir o contato corporal entre autor e vítima, adequando-se a espécie às mesmas observações delineadas para o crime de estupro do art. 213 do Código Penal.

No estupro de vulnerável, a própria descrição do tipo penal é viabilizadora do seu cometimento por meio virtual, pois basta que o autor venha a praticar ato libidinoso com vítima vulnerável, não exigindo nenhum tipo de constrangimento, até mesmo o fato de a vítima consentir com o ato é irrelevante para a configuração do crime, conforme expressamente previsto no § 5º do art. 217-A do Código Penal.

Neste § 5º poderia constar a previsão da prática do crime em tela no ambiente virtual, o que facilitaria a aceitabilidade de referido meio de execução, afastando dúvidas em relação à possível violação ao princípio da legalidade penal. Desta feita, o referido dispositivo poderia ser complementado nestes termos: "As penas previstas no caput e nos §§ 1º, 3º e 4º deste artigo aplicam-se independentemente do consentimento da vítima ou do fato de ela ter mantido relações sexuais anteriormente ao crime, como também da circunstância de o crime ter sido praticado por meio de dispositivo eletrônico ou informático, conectado, ou não, à rede de computadores, a praticar ou permitir que com ele se pratique ato libidinoso".

2.3 Projeto de Lei nº 1.891, de 2023.

Corroborando com o posicionamento retro, tramita na Câmara dos Deputados o Projeto de Lei nº 1.891, de 2023, que busca inserir os parágrafos 3º e 6º nos arts. 213 e 217-A do Código Penal, respectivamente. Os novos dispositivos tratam de condutas equiparadas, com as seguintes redações:

> Art. 213. (...)
> Estupro Virtual
> § 3º As penas previstas neste artigo são aplicadas mesmo que o crime seja praticado à distância, inclusive pelos meios digitais, como sites da rede mundial de computadores e aplicações de internet.
> Art. 217- A. (...)
> Estupro Virtual de Vulnerável
> § 6º As penas previstas neste artigo são aplicadas mesmo que o crime seja praticado à distância, inclusive pelos meios digitais, como sites da rede mundial de computadores e aplicações de internet.

A finalidade desses novos dispositivos é a de dar segurança jurídica para as vítimas e para o Poder Judiciário no momento de decidir quando da tipificação do crime de estupro virtual, não deixando as decisões à mercê apenas do entendimento de doutrinas ou jurisprudências, além de afastar qualquer questionamento no que tange à possível violação ao princípio da legalidade, em seu viés da taxatividade.

3 ESTUPRO VIRTUAL

A criminalidade cibernética vem crescendo ano após ano, fato este fomentado pelo avanço tecnológico que suprimiu toda fronteira existente no globo, possibilitando que um indivíduo residente na cidade de Berlim, na Alemanha, consiga aplicar um golpe virtual em detrimento de uma vítima brasileira moradora da cidade de Araguaína-TO.

Na visão de Silva Neto (2023), a criminalidade intensificou suas ações no ciberespaço, impulsionada pelas facilidades existentes, como o anonimato, que beneficia o criminoso, e a complexidade investigativa, residindo aqui o grande gargalo das forças policiais brasileiras, especialmente das Polícias Civis que comumente detêm grandes problemas de estrutura tecnológica e de pessoal adequadamente capacitado para operacionalizar investigações no ambiente virtual.

O avanço tecnológico, alavancado pela disseminação da Internet, ocasionou a abertura de vasto espaço para o compartilhamento de conteúdo de cunho sexual, propiciando o cometimento de crimes sexuais no ambiente cibernético; já se falando sobre sexo por mensagem de texto, tal circunstância é representada na língua inglesa pela expressão *sexting,* fruto da junção das palavras *sex* (sexo) e *texting* (envio de mensagem de texto).

No que se refere ao *sexting,* Machado e Pereira (2013) compreendem que se cuida de uma expressão decorrente da junção das palavras *sex* (sexo) e *"texting"* (envio de mensagens de texto), numa tradução *ipsis litteris* da língua inglesa significa sexo por mensagens de texto, demonstrando a problemática decorrente do avanço tecnológico e sua influência nas relações humanas.

Neste quadro, abarca-se a conduta do estupro cometido no ciberespaço, especialmente no que diz respeito ao fato de tratar-se de crime de forma livre e pela desnecessidade de contato físico-sexual entre autor e vítimas, circunstâncias que serão objeto de análise nos tópicos seguintes.

3.1 Breve análise sobre a possibilidade de tipificação do estupro virtual

A discussão em torno do surgimento da figura do estupro virtual teve como gênese dois casos ocorridos no Piauí e em Minas Gerais, cujo *modus operandi* fora o mesmo em ambos. Nestes, os autores detinham em sua posse fotos e vídeos

íntimos das vítimas, sendo referido conteúdo utilizado para constrangê-las, sob a ameaça de divulgação, a praticar atos libidinosos em si mesmas, com o escopo de satisfazer as lascívias dos ciberdelinquentes.

Em Minas Gerais, conforme Vale (2017), em reportagem do Jornal Estado de Minas, um jovem de 19 anos, com o fim de constranger mulheres por meio de ameaças, criou um perfil falso (*fake*) em uma rede social. Inicialmente, ele convencia as vítimas a lhe enviar fotos e vídeos de conteúdo pornográfico, sendo estas contracenadas pela própria vítima. Posteriormente, o criminoso chantageava as mulheres para que lhe enviassem mais conteúdo íntimo, sob pena de divulgar as fotos e os vídeos, já por ele recebido das vítimas, na Internet. Conforme as investigações, cinco vítimas tinham idade entre 16 e 24 anos.

No Piauí, segundo Gomes (2017), um indivíduo, com o mesmo *modus operandi*, criou um perfil falso no Facebook, onde também influenciava as vítimas a lhe enviarem fotos e vídeos íntimos, e, de posse desse conteúdo, passava a constrangê-las, ameaçando divulgar tudo na Internet caso não lhe enviassem novas fotos e novos vídeos pornográficos. De acordo com as investigações, o criminoso exigia fotos desnudas das vítimas, introduzindo objetos na vagina ou mesmo se masturbando. O juiz, ao decretar a prisão preventiva, justificou que, embora não tenha havido contato físico entre autor e vítima, esta fora constrangida a praticar ato libidinoso em si mesma, restando clara a tipificação do crime de estupro.

O estupro virtual é representado pela conduta do agente que, utilizando-se de meios tecnológicos à sua disposição, estando a vítima fisicamente ausente, a constrange mediante grave ameaça a praticar ou permitir que com ela se pratique conjunção carnal ou outro ato libidinoso. No mesmo caminho, Meireles (2017) destaca que o estupro virtual nada mais é que uma das modalidades de *sextorsão,* expressão originária da junção das palavras *sexo* e *extorsão*, trazendo à baila uma modalidade de exploração sexual em que o criminoso chantageia a vítima, seja por meio de uma imagem ou até mesmo um vídeo dela em contexto íntimo, podendo abarcar fotos em que a vítima aparece nua ou seminua, ou vídeos de cunho pornográfico.

Podemos visualizar a prática delitiva em tela por meio do seguinte exemplo idealizado por Silva Neto (2023): uma mulher conhece um homem por meio do Facebook e passa a trocar fotos íntimas com essa pessoa e até mesmo encaminhar vídeos eróticos. Num dado momento, o homem que esta mulher estava se relacionando virtualmente passa a proferir ameaças, afirmando que caso a mulher não se submeta aos seus desejos, passará a divulgar as fotos e os vídeos íntimos que a vítima lhe enviou. Buscando evitar que sua família e amigos tenham acesso ao material retro, a vítima submete-se às ameaças perpetradas pelo cibercriminoso, sendo constrangida, numa videochamada ao vivo, a despir-se e a se masturbar, satisfazendo assim a lascívia do homem que a ameaçou.

A admissibilidade da ocorrência da prática delituosa em tela ganha reforço pela prescindibilidade do contato físico-erótico entre autor e vítima, sendo necessário destacar que o estupro é classificado como crime de forma livre, sendo assim admite qualquer meio de execução, não havendo nenhuma especificidade posta abstratamente pelo legislador no tipo penal descritivo.

Conforme explica Silva (2020), o estupro virtual é uma consequência do avanço tecnológico e social que se teve nas últimas décadas. Com a área da informática crescendo e apresentando novas formas de se relacionar, além das mídias sociais (WhatsApp, Facebook, Instagram etc.), o crime de estupro se aperfeiçoou e hoje é praticado não apenas pela conjunção carnal, mas também pelo espaço virtual. Essa forma de cometimento do crime de estupro é bastante recente, tendo poucos casos ainda julgados pelo Poder Judiciário. Isso pode ser explicado pelo fato de que muitas vítimas ainda têm medo de denunciar, fazendo com que esse crime ocorra frequentemente sem que haja punibilidade ou mesmo registro.

Dessa forma, pode-se admitir a prática do estupro virtual, mas questiona-se sobre uma possível violação ao princípio da legalidade, especificamente no seu viés da taxatividade, tendo em vista a ausência de tipificação penal específica, em que a atual redação descritiva da conduta configurada como estupro seria supostamente insuficiente para abarcar a conduta praticada no ambiente cibernético.

Em relação à impossibilidade do estupro virtual, por violação à legalidade, Silva (2020) aponta o equívoco em referido posicionamento, levando em consideração que a adequação típica da conduta do estupro perpetrado no meio virtual se enquadra linearmente com os tipos penais descritos nos arts. 213 (estupro) e 217-A (estupro de vulnerável) do Código Penal. O agente, conforme a autora, age de maneira dolosa, dirigindo a sua ação para constranger a vítima a praticar atos libidinosos sob grave ameaça, não havendo que se falar em diversidade com os elementos típicos do crime de estupro, amoldando-se perfeitamente ao tipo penal.

Desta feita, os tipos penais descritivos da conduta do estupro e do estupro de vulnerável não obstaculizam a prática delitiva no ambiente virtual, tendo em vista cuidar-se de crime de forma livre, conforme exposto alhures, não ferindo nenhum aspecto do princípio da legalidade; constata-se apenas um meio empregado na execução do crime, no caso de maneira virtual, não havendo a previsão de nova conduta não prevista na lei penal incriminadora.

Sendo assim, o estupro virtual consiste em conduta típica, em que o sujeito ativo apenas utiliza-se do meio cibernético para o cometimento do delito sexual em tela, sendo plenamente admissível, tendo em vista tratar-se de crime de forma livre e pelo fato de não ser necessário o contato físico entre aturo e vítima, ressaltando que a conduta ocorre no mundo dos fatos, clarificando o seu aspecto de crime material que exige para a sua consumação a ocorrência do resultado naturalístico, qual seja, a prática de conjunção ou de outro ato libidinoso.

Importante afirmar que os meios tecnológicos não podem funcionar como guarida para a prática de condutas criminosas, antes perpetradas no mundo físico-material, mas que gradativamente estão migrando para o universo cibernético, sendo merecedoras da reprimenda penal devida.

3.2 Extorsão sexual e estupro virtual

A extorsão sexual é conhecida pelo termo "sextorsão" originário dos Estados Unidos, em 2010, sendo utilizado pelo *Federal Bureau Investigation (FBI),* num caso investigativo em que um *hacker* chantageou mulheres, ameaçando expor sua intimidade, caso não atendessem às suas exigências, que consistiam no envio de novas fotos nuas.

Ocorre que o termo "extorsão" nos reporta ao crime patrimonial descrito no art. 158 do Código Penal, o qual prevê como delituosa a conduta de constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa.

Na extorsão, a finalidade do autor é patrimonial, não de cunho sexual, o que pode gerar divergências na aceitabilidade da chamada extorsão sexual, por esta tratar-se de uma extorsão patrimonial. Ocorre que se a finalidade do autor for a de satisfazer a sua própria lascívia ou a de terceiro, não há que se falar em crime patrimonial, cuidando-se de verdadeiro delito sexual.

Nesse âmbito, segundo Masson (2018), o crime de extorsão reclama, além do dolo, um elemento subjetivo específico (especial fim de agir), sendo este representado pela expressão "com o intuito de obter para si ou para outrem indevida vantagem econômica", em que esta finalidade específica diferencia a extorsão do crime de estupro; neste último, o núcleo do tipo também é o verbo "constranger".

Ainda segundo Masson (2018), no crime de estupro, diferentemente da extorsão, o constrangimento mediante violência à pessoa ou grave ameaça tem como meta um fim sexual, podendo ser a conjunção carnal ou qualquer outro ato libidinoso.

Logo, se estamos diante de uma extorsão sexual cometida no ambiente cibernético, não há que se falar em crime de extorsão (crime patrimonial) se a finalidade que permeia a conduta do cibercriminoso detiver conotação sexual, pois cuidar-se-á de delito contra a dignidade sexual, como é o caso do estupro virtual, mesmo que secundariamente haja a finalidade de obtenção de lucro patrimonial, por exemplo com a vendagem das fotos e dos vídeos obtidos mediante constrangimento perpetrado contra a vítima.

Consoante o exposto, seria de bom alvitre aperfeiçoar a legislação, ressaltando que o fato de o autor visar a obtenção de lucro patrimonial com a obten-

ção de fotos e de vídeos íntimos da vítima não afastaria a incidência do tipo penal do delito sexual, desde que também tenha como escopo satisfazer a sua própria lascívia ou de terceiro, o que é presumido com o cometimento da conduta descrita nos tipos penais do estupro e do estupro de vulnerável.

3.3 O crime de estupro real

O crime de estupro encontra-se descrito no art. 213 do Código Penal, ressaltando que no art. 217-A do mesmo diploma legal encontra-se tipificado o delito de estupro de vulnerável que também adentra o miolo da discussão em epígrafe.

O tipo penal do estupro detém como elementares típicas a violência e a grave ameaça, podendo ocorrer uma ou outra como maneira de viabilizar o constrangimento emplacado na vítima pelo sujeito ativo no momento da prática delitiva. Ademais, é importante dizer que no caso do estupro de vulneráveis dados elementares não se fazem presentes, bastando que o agente pratique um ato libidinoso, conjunção carnal ou ato libidinoso diverso, com pessoa vulnerável, para fins de enquadramento típico.

Nesse âmbito, importante destacar que o estupro é crime de forma livre, especialmente no que tange à prática de ato libidinoso diverso da conjunção carnal; logo, faz-se necessária a análise da possibilidade de sua prática no ambiente cibernético, em que o ponto nevrálgico da discussão gira em torno da impossibilidade de contato físico entre autor e vítima.

3.4 A prescindibilidade do contato físico como característica distintiva fundamental entre estupro real e estupro virtual

Conforme explica Gonçalves (2018), para a configuração do crime de estupro, o contato físico entre autor e vítima é prescindível, pois o uso da grave ameaça com o escopo de coagir a vítima a se automasturbar ou a utilizar um vibrador no seu órgão genital, por exemplo, é suficiente para a configuração do tipo penal sexual em tela. Logo, o que é salutar para a ocorrência do estupro é a presença do envolvimento corpóreo da vítima no ato libidinoso.

De acordo com o entendimento do Superior Tribunal de Justiça (2016): *"A conduta de contemplar lascivamente, sem contato físico, mediante pagamento, menor de 14 anos desnuda em motel pode permitir a deflagração da ação penal para a apuração do delito de estupro de vulnerável"*. Na visão de Cunha (2016), é desnecessário o contato físico entre autor e vítima, havendo a configuração do crime na conduta do agente que determina que a vítima se masturbe somente para a contemplação do sujeito ativo. No mesmo caminho, Cavalcante (2023) discorre que o mero ato de o agente ficar contemplando a vítima nua com o fim

de satisfazer sua lascívia (contemplação lasciva) mostra-se como sendo suficiente à configuração do crime de estupro (art. 213 do Código Penal) ou de estupro de vulnerável (art. 217-A do Código Penal).

Depreende-se dos argumentos trazidos à baila que a tipificação do crime de estupro não reclama como algo imprescindível o contato físico-sexual entre o agressor e a vítima, pavimentando o caminho para o surgimento do chamado "estupro virtual". Nesse cerne, Masson (2018) aduz que é plenamente possível a prática à distância do crime de estupro, dando espaço para a viabilidade do seu cometimento no ciberespaço por meio da utilização de algum meio eletrônico (Skype, Whatsapp, Facetime etc.).

Ademais, no que se refere à expressão *estupro virtual*, permeiam no seio da doutrina, como é o caso de Meireles (2017) e Pereira (2017), algumas críticas, pois aponta-se um equívoco no termo *virtual*, tendo em vista tratar-se de estupro real, em que o aspecto virtual se refere apenas ao modo de execução, por meio da grave ameaça, sendo os atos libidinosos praticados fisicamente, funcionando o ciberespaço apenas como um meio de interconexão entre autor e vítima.

Para Pereira (2017), o tipo penal previsto no art. 213 do Código Penal não comporta a prática do estupro virtual, para quem seria necessário modificar a legislação com o fim de ajustá-la ao novel dinamismo social. Para o referido autor, o estupro virtual configuraria em crime de constrangimento ilegal, tipificado no art. 146 do Estatuto Repressivo.

Divergimos neste ponto, pois constrangimento ilegal cuida-se de crime subsidiário, em que a sua incidência se condiciona ao não cometimento de crime mais grave por parte do agente do delito. Ocorre que, se o constrangimento tem como fim a prática de ato sexual ou permissibilidade deste por parte da vítima, não há como admitir a não incidência do tipo penal do crime de estupro, dando lugar à aplicação de delito menos grave e elemento típico do crime sexual, fato este que representaria uma inversão da lógica jurídica que permeia a incidência típica-criminal regente do âmago do Estatuto Repressivo pátrio.

Na visão de Martins (2017), o estupro virtual nada mais é que o cometimento do crime de estupro por meio da utilização da Internet como meio para alcançar a consumação delitiva, em que pela grande rede opera-se o constrangimento, mediante grave ameaça, para que a vítima se submeta aos desejos libidinosos do cibercriminoso sexual.

O cometimento do crime de estupro virtual apenas comporta a grave ameaça, pois, conforme aduz Meireles (2017), a prática do delito por meio da conjunção carnal revela-se incabível no âmbito cibernético, tendo em vista que a própria definição de conjunção carnal demonstra ser imprescindível o contato físico, ocorrendo a introdução do pênis na vagina. No que se refere à grave ameaça, conforme exposto alhures, é plenamente cabível, configurando a conduta delituosa com a

prática de qualquer ato por *vis compulsiva* ou *vis corporalis* para satisfazer a lascívia do criminoso.

Nesse caminho, o Superior Tribunal de Justiça (2016), no âmbito do julgamento do Habeas Corpus nº 70976/MS, decidiu que *"a maior parte da doutrina penalista pátria orienta no sentido de que a contemplação lasciva configura o ato libidinoso constitutivo dos tipos dos artigos 213 e 217-A do Código Penal, sendo irrelevante, para a consumação dos delitos, que haja contato físico entre ofensor e ofendido"*.

Dessa forma, no âmbito da segunda modalidade do estupro, logo o cometimento de ato libidinoso diverso da conjunção carnal, especificamente em relação à conduta praticar, não há a exigência constante da presença física do sujeito ativo, pois a implementação da grave ameaça pode ser operada à distância, exigindo-se apenas o envolvimento do corpo da vítima no ato sexual, concedendo espaço para o cometimento do referido delito no ambiente cibernético, não havendo que se falar em ausência de tipificação legal ou mesmo de violação à legalidade estrita.

4 INVESTIGAÇÃO DO ESTUPRO VIRTUAL PELA POLÍCIA JUDICIÁRIA

A criminalidade contemporânea passou a migrar a sua atuação delituosa para o ciberespaço, tratando-se de movimento que atraiu diversos desafios para os órgãos de segurança pública, pois as investigações passaram a exigir uma análise extremamente técnica, além das dificuldades em detectar a autoria delitiva, tendo em vista a asseguração da impunidade residente no âmago do cibercriminoso, mas, conforme será exposto neste tópico, houve diversos avanços no campo investigativo, especialmente pela utilização de ferramentas tecnológicas no cerne do desvendamento da novel forma de criminalidade.

A Polícia Judiciária brasileira, durante bastante tempo, operacionalizou as investigações de forma nuclear pela colheita de depoimentos testemunhais, tratando-se do principal meio de obtenção de provas utilizado, sendo toda a marcha investigativa alicerçada em argumentos e percepções pessoais de indivíduos que, supostamente, teriam presenciado o cometimento da conduta delituosa.

A criminalidade contemporânea passou a migrar as suas ações do mundo físico para o ambiente virtual, em que os órgãos de investigação passaram a ter de buscar um aperfeiçoamento com vista a acompanhar o avanço da prática de crimes no ciberespaço.

Inicialmente, é de suma importância a análise de casos concretos em que fora constatada a ocorrência do estupro virtual, em que a investigação vislumbrou a tipificação criminal, enquadrando nos dispositivos postos no Código Penal.

4.1 Caso de estupro virtual em Porto Alegre/RS

Na cidade de Porto Alegre/RS, um estudante de medicina de 24 anos de idade comunicava-se com um menino de 10 anos, que morava em São Paulo/SP, por meio de uma rede social, em que utilizava um *software* de áudio e de vídeo. O estudante mantinha diálogos de cunho sexual com a criança, chegando a alguns destes encontros virtuais ocorrerem sem a utilização de vestimentas.

O pai da criança descobriu o que estava acontecendo e imediatamente procurou a polícia que, após uma investigação aprofundada, conseguiu efetuar a prisão do cibercriminoso, havendo até mesmo a descoberta de que o suspeito armazenava em torno de doze mil imagens com pornografia infantil.

A juíza Tainara Gischkow Golbert, da 6ª Vara Criminal do Foro Central de Porto Alegre, afirmou em sua decisão: "A peculiaridade do caso em tela, diz com o reconhecimento da incidência do tipo penal do estupro de vulnerável (artigo 217-A do Código Penal), perpetrado por meio virtual, posto que o réu e a vítima estavam em diferentes estados da federação".

4.2 Caso de estupro virtual em Teresina/PI

Outro caso de estupro virtual ocorreu na cidade de Teresina/PI, em 2017, em que um homem fez imagens de sua ex-namorada despida enquanto dormia, criando um perfil falso em uma rede social e ameaçando divulgar as imagens caso a vítima não lhe enviasse fotos íntimas.

A vítima, temendo que suas fotos fossem divulgadas pelo seu ex-companheiro, acabou aceitando se masturbar usando vibradores, além de introduzir outros objetos em seus órgãos genitais, mostrando as imagens ao criminoso. Nesse caso, o criminoso fora condenado como incurso no crime de estupro (art. 213 do Código Penal).

4.3 Investigação criminal cibernética e o marco civil da Internet

Nos dois casos citados alhures, a polícia chegou até a autoria delitiva pela análise do número de IP atribuído aos computadores dos criminosos. A Lei nº 12.965, de 23 de abril de 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil, tratando-se do chamado "Marco Civil da Internet", define o endereço de protocolo de Internet (endereço IP) como sendo o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (art. 5º, inciso III). Portanto, o endereço de IP permite a identificação do terminal utilizado pelo usuário, isso ocorre pois àquele é atribuído um código, possibilitando a identificação precisa do dispositivo usado.

O Marco Civil da Internet também dispõe sobre os registros de acesso a aplicações da Internet, sendo eles o conjunto de informações referentes à data e à hora de uso de determinada aplicação de Internet a partir de determinado endereço de IP (art. 5º, VIII). Logo, é possível localizar o endereço de IP atribuído ao terminal donde fora praticada a conduta delituosa; por consequência, a autoridade responsável pela investigação poderá verificar os registros de acesso a aplicações de Internet ocorrido em determinado computador ou *smartphone*.

Outrossim, o provedor de aplicações de Internet deverá manter os registros de acesso a aplicações de Internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses. Ainda, ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de Internet que não estão sujeitos ao prazo mencionado alhures a guardarem os registros de acesso a aplicações de Internet, desde que se trate de registros relativos a fatos específicos em período determinado. A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de Internet que os registros de acesso sejam guardados, até mesmo por prazo superior ao previsto em lei.

Noutro ponto, os provedores de conexão deverão manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, ressaltando que a responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros. A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior, em que a autoridade requerente terá o prazo de sessenta dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros.

Conforme exposto, o endereço de protocolo de Internet (endereço IP) trata-se do código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais. O terminal nada mais é do que o computador ou qualquer dispositivo que se conecte à grande rede. Para um terminal se conectar à Internet, deve contar com um provedor de conexão que realizará a atribuição ou autenticação de um endereço IP.

4.4 Diligências importantes na investigação do estupro virtual

4.4.1 A obtenção dos registros de conexão

Ademais, no contexto de uma investigação de cibercrimes sexuais é de fundamental relevância a busca por todo o registro de conexão, cuja diligência tem como escopo verificar para qual usuário aquele IP fora atribuído, no dia e na hora do delito, com o fuso horário respectivo.

De acordo com o Marco Civil da Internet, o registro de conexão consiste no conjunto de informações referentes à data e à hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados. O terminal é o computador ou qualquer dispositivo que se conecte à Internet.

O endereço de protocolo de Internet (endereço IP), trata-se do código atribuído a um terminal de uma rede para permitir sua identificação, definido conforme parâmetros internacionais. Logo, para que um terminal possa se conectar à Internet, é imprescindível a atribuição ou autenticação de um endereço IP, podendo este ser fixo, quando não sofre alterações a cada conexão, ou um IP dinâmico, quando se modifica a cada nova conexão realizada pelo usuário por meio de um terminal.

Nesse cerne, é possível que o número de IP atribuído seja o mesmo para mais de um usuário, isso ocorre devido a dificuldades geradas pelo compartilhamento de endereços IPv4 por parte de provedores de Internet, especificamente por meio da operacionalização de plataformas CG-NAT44.

A plataforma *Carrier Grade Network Address Translation* (CG-NAT), traduzindo para o português significa "Tradução de Endereço de Rede de Nível de Operadora", possibilita o compartilhamento de endereços IPv4 públicos, em que vários usuários poderão, num mesmo instante, acessar a Internet por meio do mesmo endereço IP público. Logo, é de suma importância que a autoridade policial que esteja presidindo a investigação de um crime sexual cibernético requeira, além do IP usado pelo cibercriminoso, a porta lógica do *hardware*.

O esgotamento do IPv4 vem dificultando as investigações, havendo a necessidade de implementação urgente da nova versão do protocolo, tratando-se do IPv6. Com a implementação do IPv6 haverá uma abundância de endereços IP (o que não ocorre com o IPv4), sendo possível atribuir um número identificador específico para cada conexão.

Segundo explica Pereira (2019), este compartilhamento de IPs públicos entre vários usuários consiste em solução adotada de forma transitória e temporária, tendo como escopo circundar a escassez de endereçamento IP padrão IPv4, devido ao atraso na migração para o atualizado e novo padrão IPv6.

Conforme aduz Porto (2023), é estabelecida uma rede entre os usuários, promovida pelo provedor de conexão, o qual atribui àqueles um endereço IP local (privado); para tanto, utiliza a operação de NAT em que se operacionaliza o processo de mapeamento e tradução dos endereços IPs privados dos usuários, para endereços válidos na Internet (endereços IPs públicos). A atribuição de IPs públicos dificulta a identificação do terminal de onde partiu o cibercrime, sendo de fundamental relevância a realização de diligências de campo com o intuito de chegar até o usuário que se conectou à grande rede para a prática da conduta delitiva.

4.4.2 A obtenção dos registros de acesso a aplicações da Internet

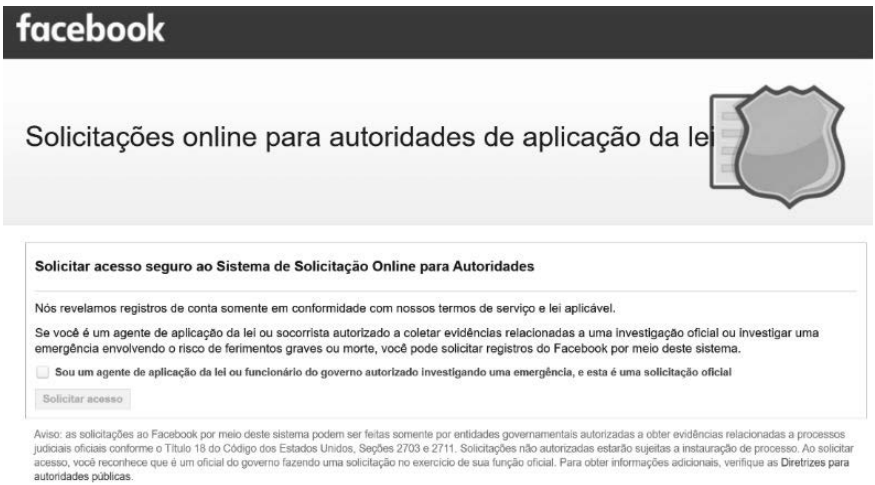
O estupro virtual, comumente, é praticado por meio da utilização de aplicações da Internet, como: Facebook, Instagram, WhatsApp, Twitter, Gmail, dentre outras. As aplicações de Internet, conforme o Marco Civil, é o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet.

Nessa senda, o registro de acesso a aplicações da Internet é o conjunto de funcionalidades referentes à data e à hora de uso de determinada aplicação de Internet a partir de determinado endereço IP.

No que se refere ao Facebook e ao Instagram, a obtenção dos registros de acesso se dá por meio da plataforma law enforcement online, tratando-se do Facebook Records, em que é possível solicitar a preservação cautelar de perfis de usuários e os dados cadastrais respectivos, não necessitando de ordem judicial para tanto.

O acesso à plataforma em epígrafe condiciona-se à circunstância de o solicitante estar encarregado de uma investigação em andamento. Ademais, não será criado um novo perfil da rede social para o solicitante, apenas haverá a vinculação de um e-mail institucional ao caso que será aberto no provedor de aplicação.

Figura 1: Facebook Records[2]

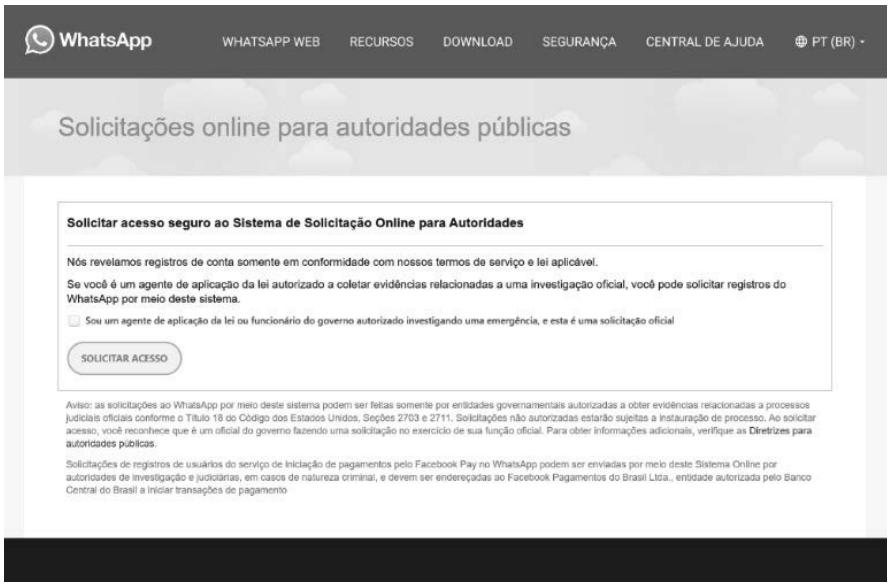


Fonte: Meta, 2023.1

2 Imagem capturada da página da empresa Facebook na Internet para solicitações de autoridades públicas.

Em relação ao WhatsApp, para a solicitação dos registros de acesso à aplicação, como também para a preservação cautelar dos referidos dados do usuário, utiliza-se a plataforma do WhatsApp Records, sendo possível obter informações do usuário, como: contatos, data, hora e dados sobre envio e recebimento de mensagens (endereço de IP, operadora de celular utilizada, versão e número de identificação do dispositivo, informações de configuração do navegador web para acessar o dispositivo e dados de localização no momento da utilização dos serviços).

Figura 2: WhatsApp Records[3]



Fonte: Meta, 2023.1

Na prática do crime de estupro virtual e demais delitos sexuais praticados no ambiente cibernético, os cibercriminosos criam perfis falsos em redes sociais, especialmente no Facebook e no Instagram, pelos quais atraem as vítimas, obtendo fotos e vídeos de conteúdo erótico destas, e pelos quais passam a chantageá-las mediante a ameaça de divulgar o conteúdo, condicionando a não divulgação ao envio de mais e mais fotos e vídeos da mesma natureza.

3 Imagem capturada da página da empresa WhatsApp na Internet para solicitações de autoridades públicas.

4.4.3 Infiltração virtual

Noutro giro, tem-se a infiltração virtual de agentes, tratando-se de uma medida cautelar probatória e importante meio investigativo, que tem como objeto de investigação crimes específicos, seja envolvendo organizações criminosas ou crimes tipificados na Lei nº 8.069, de 1990 (Estatuto da Criança e do Adolescente), ou no Código Penal.

A infiltração virtual sempre será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova. Ainda, dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia, e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas. A infiltração de agentes de polícia na Internet não será admitida se a prova puder ser obtida por outros meios, cuidando de medida de *ultima ratio*.

Ponto importante é que não é prevista a possibilidade de infiltração por agentes de inteligência, pertencente, por exemplo, ao Sistema Brasileiro de Inteligência (SISBIN) ou à Agência Brasileira de Inteligência (ABIN). Isso ocorre porque a infiltração é uma medida para colheita de provas, não sendo uma atividade de Inteligência, pois esta última tem como fim a produção de conhecimento destinado a subsidiar o tomador de decisão.

Dentre os crimes previstos no art. 190-A da Lei nº 8.069, de 1990, que admitem a infiltração virtual de agentes, tem-se a previsão expressa do estupro de vulnerável (art. 217-A do Código Penal), evidenciando que até mesmo o legislador reconhece de forma explícita a possibilidade do estupro de vulnerável praticado no ambiente virtual. Da mesma forma, apesar de não previsto no referido dispositivo, podemos concluir também que tacitamente admite-se a prática do crime de estupro (art. 213 do Código Penal) no ambiente cibernético.

No que tange à infiltração, Lopes (2011) aduz que o agente infiltrado trata-se de um integrante da polícia, que atua mediante prévia autorização judicial, ocultando a sua identidade, em que se insere de maneira estável em determinada organização criminosa, na qual passa a adquirir a confiança dos respectivos integrantes, e com isso, tendo acesso a informações sigilosas, assegura a identificação dos criminosos e os delitos por eles perpetrados.

Segundo explica Sato (2013), a infiltração de agentes deflagrada no ambiente virtual consiste em uma das formas de operacionalização de infiltração de agentes, em que o policial poderá proceder à criação de um perfil fictício, por meio do qual passa a manter contato com os suspeitos da prática de crimes sexuais virtuais perpetrados contra crianças e adolescentes, sendo viável a sua participação em fóruns e grupos de discussão, em que dissimulará a sua identidade, cujo principal

escopo é a angariação de elementos de informação relacionados à sistematização criminosa desenvolvida pelos investigados.

A infiltração virtual também pode ser denominada como *light cover* (capa de luz), tratando-se de uma modalidade de infiltração menos incisiva. Nesse ponto, de acordo com Silva (2016), a criação de um perfil falso de usuário (criação de perfil *fake*), com a ocultação da verdadeira personalidade do investigador na Internet, é classificada pela doutrina americana como operações infiltradas na modalidade de *light cover*, enquadrando-se em uma infiltração branda, de curta duração, não reclamando do agente infiltrado uma imersão contínua e permanente, exigindo um planejamento menos complexo.

4.4.4 Uso de geolocalização na investigação

Outra importante ferramenta de investigação é a pesquisa geolocalizada de postagens por meio da plataforma *Skylens,* que, segundo Caselli (2023), cria uma cerca eletrônica na busca por postagens com indicação de geolocalização na redes sociais Twitter, YouTube, Instagram, dentre outras, sendo eficiente em relação ao alcance de postagens de perfis abertos, não privados, tendo como resultado apresentado um mapa interativo com a indicação da postagem, a data e o local apontado pelo usuário do perfil.

Comumente, no âmbito da *sextorsão*, o criminoso posta fotos e vídeos das vítimas em perfis falsos, mas são páginas de redes sociais abertas (não privadas) o que permite o êxito investigativo por meio do uso da ferramenta de geolocalização em tela.

5 INVESTIGAÇÃO CIBERNÉTICA NO ÂMBITO DA POLÍCIA JUDICIÁRIA CIVIL TOCANTINENSE

No estado do Tocantins, a Polícia Civil, pela sua Escola Superior de Polícia (ESPOL), passou a implementar uma série de capacitações destinadas aos policiais na área de investigação cibernética, buscando trazer eficiência e solidez para a elevada gama de casos de crimes virtuais que aportam diariamente nas delegacias de polícia espalhadas por todo o território tocantinense.

Nos últimos anos, a Escola Superior de Polícia ofertou disciplinas com foco na investigação de crimes virtuais, como: a) investigação criminal tecnológica; b) inteligência e investigação criminal em fontes abertas; c) medidas cautelares no âmbito de investigações cibernéticas; d) ferramentas tecnológicas de extração de dados de dispositivos eletrônicos; e) processamento de dados; dentre outras matérias inerentes à temática em epígrafe.

Outrossim, a Polícia Civil do Tocantins vem avançando na investigação de crimes cibernéticos sexuais, dentre eles o estupro virtual, como também no âmbito da perícia computacional forense, pois o êxito de investigações envolvendo crimes cometidos no ambiente virtual está intrinsecamente imbricado à solidez da atuação da perícia no cerne da cadeia de custódia da evidência digital e na extração de dados de aparelhos eletrônicos.

Posto isso, passamos a analisar aspectos importantes da perícia criminal e da investigação de crimes sexuais praticados no ambiente virtual; para tanto, serão utilizados dados e informações colhidos em entrevistas realizadas com as chefias da Divisão de Repressão e Crimes Cibernéticos e do Núcleo de Computação Forense, ambos setores existentes na estrutura da Polícia Civil do Tocantins.

5.1 Investigação Cibernética do Estupro Virtual no Tocantins

No estado do Tocantins, a Divisão de Repressão a Crimes Cibernéticos (DRCC), localizada na cidade de Palmas, tendo como titular o delegado de polícia Lucas Brito Santana, utiliza-se de técnicas de investigação destinadas ao desvendamento de crimes sexuais virtuais, as quais serão analisadas na sequência, com fulcro em informações fornecidas pela citada autoridade policial na presente pesquisa.

As técnicas de investigação perpassam pelas circunstâncias específicas de cada caso concreto, notadamente quanto ao provedor de aplicações utilizado na prática delituosa, como o WhatsApp, Telegram, Instagram, Facebook, Skype, Tik Tok e Kwai. Conforme explica o doutor Lucas Brito, *"cada uma destas plataformas fornece uma gama de dados que propicia a individualização e localização do usuário responsável pelos acessos criminosos"*.

Nota-se que os elementos fornecidos pelas plataformas citadas alhures são de suma importância para as investigações de fatos delituosos que ocorrem nelas, mas, caso não sejam suficientes, poderão ser complementados por dados obtidos em pesquisas realizadas em fontes abertas, monitoramento de redes sociais, requisições de dados cadastrais e interceptações telefônicas judicialmente autorizadas.

De acordo com o titular da Divisão de Repressão a Crimes Cibernéticos do Tocantins[4], *"como é intrínseco à investigação de qualquer delito em meio virtual, há sempre uma massiva carga de dados a serem analisados, sendo que algumas ferramentas contribuem na sistematização do arcabouço informativo, como o IPED (software utilizado na indexação, processamento e análise de evidências digitais) e o IBM i2 (software de análise visual capaz de reunir, exibir, cruzar e analisar dados por meio de diagramas"*.

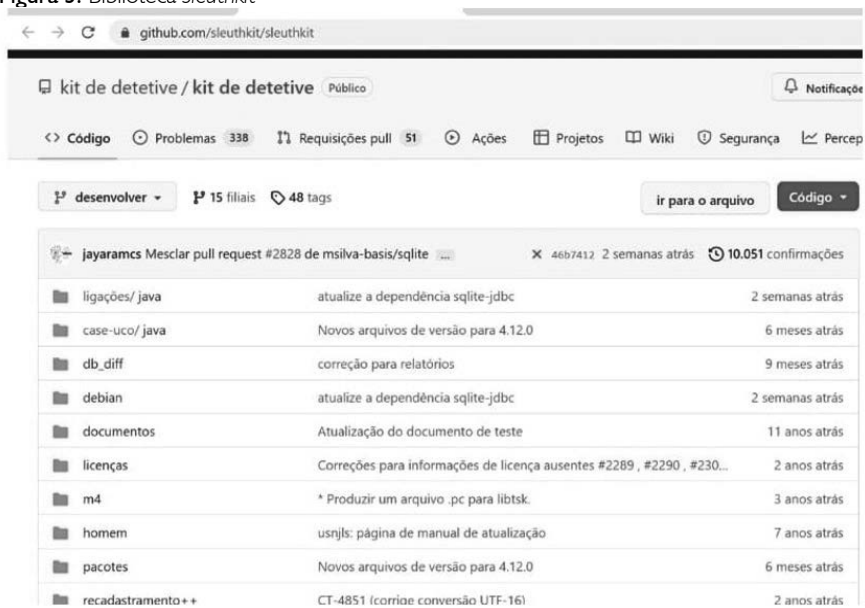
4 Entrevista concedida por Lucas Brito Santana, em 20 de junho de 2023. O Sr. Santana é delegado-chefe da Divisão de Repressão a Crimes Cibernéticos (DRCC).

O Indexador e Processador de Evidências Digitais (IPED) é uma ferramenta forense brasileira desenvolvida pela Polícia Federal em 2012, mas que apenas em 2019 fora disponibilizada para o público em geral, tornando-se um projeto de código aberto público e disponibilizado no GitHub da Polícia Federal.

O Indexador e Processador de Evidências Digitais é implementado em java, cujo objetivo é o de processar dados de forma eficiente e estável, tendo como principais características: a) processamento de dados de linha de comando de caso em lote; b) suporte multiplataforma, testado em sistema Windows e Linux; c) casos portáteis sem instalação, o que permite a execução a partir de unidades removíveis; d) interface de análise integrada e intuitiva; e) alto desempenho *multithread* e suporte para gabinetes grandes, com uma velocidade de processamento de até 400 GB/h utilizando um *hardware* moderno e 135 milhões de itens em um (multi) gabinete, a partir de 12/12/2019.

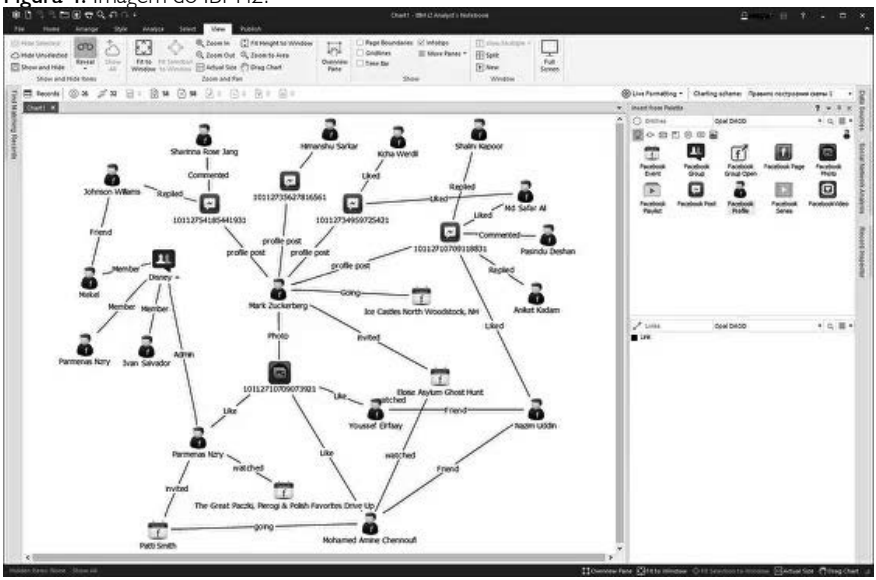
Atualmente, o Indexador e Processador de Evidências Digitais usa a Biblioteca Sleuthkit apenas para decodificar imagens de disco e sistemas de arquivos; portanto, os mesmos formatos de imagem são suportados: RAW/DD, E01, ISO9660, AFF, VHD, VMDK. Também há suporte para os formatos EX01, VHDX, UDF (ISO), AD1 (AccessData) e UFDR (Cellebrite).

Figura 3: Biblioteca *Sleuthkit*



Fonte: Github, 2023.1

Figura 4: Imagem do IBM i2.



Fonte: Social Links, 2023.1

Segundo informado pelo titular da Divisão de Repressão a Crimes Cibernéticos de Palmas/TO, no que tange à utilização das técnicas de investigação expostas alhures, afirma que

> Há êxito repressivo sempre que verificado não apenas o comprometimento dos profissionais envolvidos diretamente nas apurações – os quais necessitam de expertise teórica e prática, além de proatividade e boa dose de obstinação –, mas também o respaldo institucional, em todas as esferas, mediante disponibilização de recursos humanos, materiais e estruturais adequados, na esteira do discorrido nas respostas precedentes. Em síntese, quando esta relação está desequilibrada, surgem as sobrecargas e, por consectário, os gargalos investigativos (Santana, 2023).

A seguir, passemos a analisar alguns casos de estupro virtual objetos de investigação por unidades da Polícia Civil do Tocantins, em que foram entrevistadas as autoridades policiais que presidiram as respectivas investigações.

5.1.1 Estupro Virtual ocorrido na cidade de Porto Nacional/TO

Na cidade de Porto Nacional/TO, conforme o portal Conexão Tocantins (2021), um homem de 25 anos foi indiciado pela Polícia Civil pela prática do crime

de estupro virtual. De acordo com as investigações realizadas pela 8ª Delegacia Especializada de Atendimento à Mulher e Vulneráveis, a vítima conheceu o suspeito no Facebook, e durante as conversas ambos teriam trocado fotos íntimas ("nudes").

No dia 18 de abril de 2021, a vítima e o suspeito decidiram conversar por meio de chamada de vídeo, momento em que a vítima percebeu que a aparência do homem não condizia com a foto que constava no perfil da sua rede social, instante em que a vítima informou que não gostaria mais de continuar conversando com ele.

O suspeito então passou a enviar as fotos íntimas da vítima para o WhatsApp dela, ameaçando-a de que divulgaria as fotos em grupos de conversas caso ela não fizesse uma chamada de vídeo com ele, na qual a vítima teria de mostrar suas partes íntimas. Estando a vítima sob a ameaça gravosa do infrator, acabou por aceitar fazer a videochamada pela qual mostrou suas partes íntimas, sendo que o suspeito também se exibia em situação de nudez.

A delegada titular da 8ª DEAMV[5], ao falar sobre os desafios da investigação, explica:

> O estupro virtual ocorria durante as chamadas de vídeo, quando o autor obrigava a mulher a mostrar suas partes íntimas e se tocar, portanto tais chamadas não ficavam gravadas. Não obstante, havia mensagens no WhatsApp e no Instagram, nas quais o autor deixava claro que possuía as fotos íntimas da vítima, e que as divulgaria, caso a vítima não aceitasse fazer chamadas de vídeo com ele, restando configurada a ameaça. Outras mensagens indicavam o teor das chamadas, corroborando com o relato da vítima (Correia, 2023)

Na investigação, conforme a titular da 8ª DEAMV de Porto Nacional/TO, ao discorrer sobre as técnicas e as ferramentas utilizadas para chegar até a autoria delitiva, fora realizada a extração do conteúdo do celular da vítima. No âmbito do registro do boletim de ocorrência do caso, foram consignados os links das redes sociais utilizadas pelo autor.

De acordo com a autoridade policial, oficiou-se ao Facebook e ao Instagram por meio da plataforma *"Facebook Records",* bem como ao WhatsApp pelo *"WhatsApp Records"*, em que foram solicitados os dados cadastrais das contas utilizadas pelo suspeito. Ademais, também fora oficiado à operadora de telefonia celular, possibilitando o confronto dos dados para chegar à autoria delitiva, sendo descoberto que o suspeito residia na cidade de Natividade/TO, e graças ao apoio

5 Entrevista concedida por Fernanda de Siqueira Correia, em 2 de agosto de 2023. A Sra. Correia é delegada-chefa da 8ª Delegacia Especializada de Atendimento à Mulher e Vulneráveis de Porto Nacional/TO.

prestado por policiais da região obteve-se a localização do indivíduo, sendo este interrogado por carta precatória.

A delegada, ao ser questionada, à luz da investigação presidida, sobre o que poderia melhorar na metodologia de investigação de crimes cibernéticos desenvolvida pela Polícia Judiciária Civil tocantinense, afirma que na época da investigação havia passado por uma capacitação ministrada pela Escola Superior de Polícia do Tocantins (ESPOL/TO), onde se tratou sobre investigação de crimes praticados no ambiente virtual, o que lhe foi crucial, pois quando da ocorrência da investigação detinha o conhecimento necessário para obter os dados cadastrais nas plataformas supracitadas, sendo determinante para chegar até a autoria delitiva.

Entretanto, a delegada faz um alerta sobre a necessidade de extensão da capacitação na investigação de crimes virtuais a todos os demais policiais civis tocantinenses:

> No entanto, esse tipo de capacitação deveria ser estendido aos demais policiais, sobretudo aos agentes de polícia, pois muito ainda desconhecem os caminhos para obter os dados das principais redes sociais. Além de uma capacitação que alcance o maior número de policiais possível, deveria ser formado um grupo de estudos para a elaboração de um manual contendo orientações (passo a passo), modelos de ofício e outras informações necessárias para solicitar tais dados às redes sociais, bancos e outros aplicativos (Correia, 2023).

Nesse âmbito, segundo a titular da 8ª DEAMV de Porto Nacional/TO:

> Já tive outro caso (de tentativa de estupro, praticado por meio de mensagens de aplicativo) em que foi necessário solicitar quebra de sigilo para obtenção de dados de conexão, e somente logrei êxito na diligência após solicitar a ajuda de uma colega que já trabalhava na área de crimes cibernéticos, que me orientou tanto na fase do pedido judicial, como também na análise dos dados, pois realmente é algo que foge ao trabalho cotidiano da delegacia (Correia, 2023).

Ainda, conforme aduz a doutora Fernanda, os policiais que trabalham em Centrais de Atendimento (Centrais de Flagrante) também deveriam receber referida capacitação, especialmente para fazerem constar nos boletins de ocorrência registrados todas as informações necessárias para embasar a investigação, bem como solicitar de imediato a preservação de conteúdo na respectiva plataforma.

5.1.2 Estupro Virtual ocorrido na cidade de Miracema/TO

Na cidade de Miracema/TO, segundo Toledo (2018), uma investigação comandada pela Delegacia Especializada na Repressão a Crimes Cibernéticos

(DRCC), de Palmas/TO, levou à prisão um homem pela prática de estupro no ambiente virtual.

Segundo à investigação, um homem de 23 anos teria se utilizado de redes sociais com perfil falso para entrar em contato com a vítima, uma mulher de 22 anos, em que lhe solicitou fotos íntimas, tendo a vítima atendido aos pedidos do suspeito por certo tempo. Ocorre que a vítima decidiu não mais enviar foto ou vídeo, o que levou o suspeito a chantageá-la, pois se não lhe enviasse novos vídeos e novas fotos divulgaria todo o conteúdo íntimo da vítima, o qual estava em sua posse.

De acordo com a doutora Milena Santana, delegada titular da Delegacia Especializada na Repressão a Crimes Cibernéticos, na época do fato, a vítima cedeu às ameaças perpetradas pelo suspeito, mas depois pediu auxílio à Polícia Civil. O crime teve sua autoria confirmada por meio de provas técnicas formalizadas e posteriormente judicializadas na Comarca de Miracema do Tocantins, local onde residia o suspeito, sendo cumprido mandado de busca e apreensão em sua residência, onde fora apreendido seu aparelho celular.

Nas palavras da titular da Delegacia Especializada na Repressão a Crimes Cibernéticos [6], no que se refere às dificuldades enfrentadas na investigação: "A maioria das evidências digitais haviam sido apagadas pela vítima. As conexões de Internet utilizadas eram por meio de endereço IP, com CGNAT". Logo, resta claro que a identificação da autoria exclusivamente pelo IP atribuído ao terminal de onde partiu a conduta delituosa mostrou-se insuficiente, tendo em vista tratar-se de IP do tipo IPV4 de compartilhamento público via CGNAT, o que dificulta sobremaneira a investigação.

Em relação às técnicas utilizadas, a doutora Milena ressalta que se procedeu à análise de dados telemáticos, cadastrais e respectivos vínculos, juntamente com trabalho de levantamento de campo. No que tange ao método investigativo utilizado, a titular da Delegacia Especializada na Repressão a Crimes Cibernéticos afirma que: "A metodologia foi adequada, dentro das condições de trabalho vivenciadas na época, resultando na identificação da autoria e materialidade delitivas".

Por fim, nas palavras da delegada:

> As pessoas têm, em geral, a ideia de que o anonimato é intangível pela Internet, que na realidade não é, então tudo que você faz pela Internet deixa rastros. A investigação de crimes cometidos em meio eletrônico, pode ser mais complexa, pode ser mais ex-

6 Entrevista concedida por Milena Santana de Araújo Lima, em 4 de agosto de 2023. A Sra. Lima, na época da investigação em epígrafe, era delegada-chefa da Delegacia de Repressão a Crimes Cibernéticos (DRCC), na cidade de Palmas/TO. Atualmente está lotada na Divisão de Inteligência do Núcleo de Inteligência e Segurança Institucional do Tribunal de Justiça do Estado do Tocantins.

> tensa, mas não impede a identificação da autoria delitiva, nem a sua responsabilização penal" (Santana, 2023).

5.1.3 Operação conjunta das Polícias Civis da Bahia e do Tocantins

Segundo Cruz (2021), no dia 5 de abril de 2021, em operação conjunta das Polícias Civis da Bahia e do Tocantins, fora cumprido um mandado de prisão de um homem de 20 anos suspeito de praticar estupro, de forma virtual, de crianças e de adolescentes. No momento do cumprimento do mandado, foram apreendidos aparelhos celulares com imagens e vídeos das vítimas.

O doutor Claudemir Luiz Ferreira, delegado de polícia adjunto da Delegacia de Repressão a Crimes Cibernéticos da época, explica que o suspeito se valia de mais de 80 perfis falsos na rede social Instagram: *"Ele iniciava conversas com crianças e adolescentes, conseguia fotos e vídeos íntimos das vítimas e depois ficava chantageando para que as mesmas continuassem a se exibir sexualmente para ele"*. As investigações apuraram que o homem fez vítimas nos estados do Tocantins, Minas Gerais, Ceará, dentre outros.

Em relação aos desafios e dificuldades enfrentados no desenrolar das investigações do caso em tela, o doutor Claudemir[7] esclarece:

> O caso em questão talvez tenha resultado na primeira prisão e indiciamento pela prática, em tese, do crime de estupro na modalidade virtual no Estado do Tocantins. Aqui vale destacar que a equipe da DRCC – Palmas era e é muito qualificada, e todos se dedicaram ao caso. Acho que a grande dificuldade e desafio no processo investigativo foi demonstrar ao judiciário a necessidade e importância de medidas cautelares (quebras de sigilo telefônico, telemático e prisão) do investigado, pois mesmo estando a milhares de quilômetros da vítima, o autor lhe causava grande sofrimento psicológico (Ferreira, 2023).

No que se refere a técnicas e ferramentas utilizadas para chegar até a autoria delitiva, o adjunto da Delegacia de Repressão a Crimes Cibernéticos explica que a investigação se alicerçou nos dados obtidos por meio das quebras dos sigilos, sendo também de suma importância o monitoramento desenvolvido em tempo real das ligações telefônicas, tendo como consequência a identificação do suspeito e a sua localização no estado da Bahia, evitando que novas condutas delituosas

7 Entrevista concedida por Claudemir Luiz Ferreira, em 9 de agosto de 2023. O Sr. Ferreira, na época da investigação em epígrafe, era delegado adjunto da Delegacia de Repressão a Crimes Cibernéticos (DRCC), na cidade de Palmas/TO. Atualmente ocupa o cargo de delegado-geral da Polícia Civil do Estado do Tocantins.

fossem perpetradas pelo indivíduo, ressaltando que ele estava, contemporaneamente, constrangendo, mediante ameaças, uma adolescente de Minas Gerais.

Ademais, em relação ao que poderia ser aprimorado na investigação de crimes desta natureza, na seara metodológica, desenvolvida pela Polícia Judiciária tocantinense, Claudemir (2023) ressalta que: *"À luz da investigação realizada, em que o processo de análise de dados foi feito praticamente de maneira manual, hoje tenho convicção da importância e necessidade de se investir em tecnologia de modo a facilitar e dinamizar o trabalho dos investigadores".*

Na mesma toada, a autoridade policial destacou a importância em ser feito um trabalho institucional de conscientização aos policiais civis tocantinenses, com vista a buscarem angariar conhecimentos suficientes na seara das investigações de crimes cometidos no ambiente virtual, o que seria de fundamental importância para o desvendamento não somente de crimes virtuais em si, mas também de muitos outros que usam o ciberespaço como trampolim para a operacionalização das mais diversas condutas delituosas.

5.2 Perícia Cibernética do Estupro Virtual no Tocantins

A investigação de crimes sexuais praticados por meio do ambiente virtual demanda aprimorado sistema de perícia criminal voltada à extração e à preservação de evidências digitais, especialmente após a inserção no Código de Processo Penal da sistemática da cadeia de custódia, inaugurada na legislação processual penal brasileira com a entrada em vigor da Lei nº 13.964, de 2019 (Pacote Anticrime). Nesse ponto, passaremos a analisar importantes aspectos procedimentais da perícia criminal no âmbito de investigações de crimes sexuais virtuais.

A perícia técnica da Polícia Civil do Tocantins, no levantamento de vestígios digitais, perpassa por algumas etapas, sendo elas: a) Identificação; b) Isolamento; c) Coleta; d) Preservação (duplicação forense e *hashes*); e) Processamento (data *carving*); f) Análise; g) Relatórios. Analisaremos na sequência essas etapas; para tanto, utilizaremos como base as informações fornecidas pela perita criminal Leila Diniz, chefa do Núcleo de Computação Forense da Polícia Civil do Tocantins[8].

O procedimento inicial, na fase de identificação, consiste na análise *Post Mortem* ou *Live Analysis* (Análise Viva). Na primeira, os procedimentos de análise e de extração são realizados sobre meios de armazenamento não voláteis, como: a) disco rígido, HD externo, pen drive, DVDs, CDs, dentre outros. No que tange à segunda, ressalta-se que algumas evidências digitais somente serão obtidas caso o sistema operacional do dispositivo eletrônico esteja ligado, em que os dados arma-

8 Entrevista concedida por Leila Diniz Alves, em 20 de junho de 2023. A Sra. Alves é perita-chefa do Núcleo de Computação Forense da Polícia Civil do Estado do Tocantins.

zenados na memória RAM, por exemplo, serão perdidos caso haja o desligamento do dispositivo.

Na etapa seguinte, proceder-se-á à duplicação forense, tratando-se de cópia fidedigna do original "bit a bit" da evidência digital, por meio do bloqueio de escrita das evidências, utilizando o algoritmo de *hash* para assegurar a integridade no processo.

São utilizadas para a referida duplicação as seguintes ferramentas: *Encase Imager, FTK Imager* e *TD3 Forensic Imager (Tableau)* e *Hasher* para geração do algoritmo *hash*. Conforme explica Leila (2023): *"O processamento é realizado nas imagens duplicadas utilizando técnicas como data carving (recuperação de arquivos apagados) e indexação de dados".*

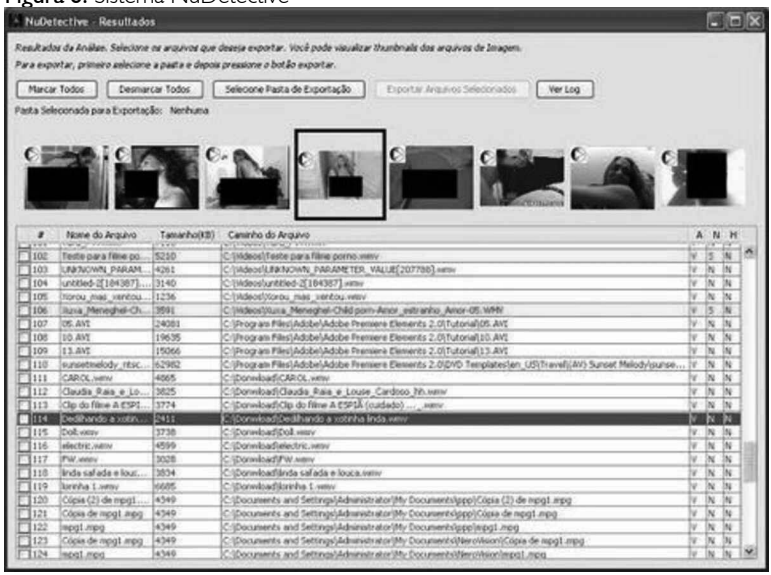
Figura 5: TD3 *Forensic Imager* (Tableau)

Fonte: Officer, 2023.1

De mais a mais, no processamento das imagens duplicadas utiliza-se como técnica também o OCR (*Optical Character Recogniton)*, tratando-se do reconhecimento óptico de caracteres, tecnologia utilizada para reconhecer e extrair textos de diversas origens, comparação de *hashes* entre outras.

No que diz respeito ao processamento e à análise de dados, os peritos criminais tocantinenses utilizam as ferramentas periciais IPED (Indexador e Processador de Evidências Digitais), *Softwares Magnet Axiom* e *Autopsy*, para busca e análise de artefatos de Internet e UFED Physical Analyser (especialmente para dispositivos móveis, como aparelhos celulares). No caso de envolver pornografia infantil, são utilizadas também ferramentas que auxiliam na detecção de imagens de nudez como NuDetective e o Localizador de Evidências Digitais (LED).

Figura 6: Sistema NuDetective



Fonte: Correio do Estado, 2023.1

A perícia computacional forense, na análise de conteúdo pornográfico infantil, utiliza-se de técnicas de classificação de imagens, categorização, marcadores e índices. Após concluída a análise em epígrafe, e de posse dos dados resultantes desta, serão gerados os relatórios que subsidiarão as investigações. No caso do UFED, exposto alhures, a ferramenta de relatório é o UFED Reader.

A utilização das referidas técnicas e ferramentas de perícia cibernética obteve importantes êxitos e resultados no cerne de investigações de dada natureza: a) Operação Luz da Infância (maior operação de combate ao crime contra a dignidade sexual infantojuvenil do Planeta), desencadeada em várias fases, sendo a primeira delas com 100% de efetividade em que todos os alvos foram presos em flagrante; b) Operação Rede Sombria, tendo como resultado a prisão em flagrante de um médico na cidade de Peixe/TO, onde houve uma participação direta da equipe de peritos criminais tocantinenses.

Segundo dados fornecidos pelo Núcleo de Perícia Computacional da Polícia Civil do Tocantins, entre os anos de 2017 e 2022, foram utilizadas as técnicas de perícia cibernética em crimes sexuais em várias investigações, conforme quantitativo a seguir: a) 93 casos de pornografia infantojuvenil; b) 53 casos de estupro de vulnerável; c) 32 casos de estupro; d) 3 casos de importunação sexual. Ainda, foram realizadas pelo referido núcleo 14 operações policiais em apoio às delegacias de polícia do Estado, com o escopo de realização de exames periciais envolvendo crimes contra a dignidade sexual de crianças e de adolescentes.

5.3 Desafios enfrentados pela Polícia Judiciária do Tocantins na coleta de provas digitais e rastreamento de criminosos

No que concerne aos aspectos da investigação, especificamente em relação aos desafios enfrentados pela Polícia Civil do Tocantins na investigação de crimes sexuais cometidos no ambiente cibernético, especialmente o estupro virtual, o doutor Lucas Brito (2023), delegado-chefe da Divisão de Repressão a Crimes Cibernéticos (DRCC), ressalta a importância de ampliação do poder requisitório do delegado de polícia, em que nas palavras da referida autoridade policial: *"O poder requisitório do Delegado de Polícia é deveras restrito, pois muitas investigações ficam engessadas já no nascedouro, carecendo de dados que, atualmente, só podem ser fornecidos mediante autorização judicial".*

No mesmo âmbito, o chefe da Divisão de Repressão a Crimes Cibernéticos destacou a exiguidade dos prazos previstos no Marco Civil da Internet para fins de guarda obrigatória dos registros de conexão e de acesso pelos provedores de conexão e aplicações de Internet, dados essenciais paras as investigações que envolvem crimes sexuais virtuais, neles incluído o estupro virtual. Outro ponto trazido pelo delegado é o não fornecimento das portas lógicas por parte dos provedores de aplicações:

> As portas lógicas são fundamentais na individualização de acessos realizados por meio do CGNAT (Carrier Grade Nate) – faixa dedicada às conexões via protocolo de rede no qual diferentes usuários compartilham simultaneamente o mesmo endereço IP – não são indicadas pelos provedores de aplicação (Santana, 2023).

Comumente os provedores de conexão e de aplicação de Internet fornecem apenas o registro de conexão ou de acesso, respectivamente, não fornecendo as portas lógicas ou mesmo o endereço MAC, que são fundamentais para a identificação do terminal de onde partiu o cometimento da conduta delituosa, tendo a capacidade de identificar o equipamento de hardware utilizado pelo cibercriminoso.

Outra dificuldade enfrentada é a baixa colaboratividade de algumas plataformas, e ainda que demandadas judicialmente muitas delas apresentam respostas insatisfatórias, incompletas ou intempestivas. Ainda, constituiu em enorme barreira ao sucesso de investigações cibernéticas de uma forma geral o baixo número de policiais civis tocantinenses com qualificações específicas para referido espectro de atuação, tendo em vista que o número de policiais qualificados para esse mister é bastante reduzido, sendo comumente adotada a solução paliativa da capacitação "prática" de servidores policiais que demonstrem algum interesse pela área de investigação cibernética.

Apesar dos valorosos esforços de a Escola Superior de Polícia (ESPOL) ofertar cursos de capacitação na área cibernética, ainda, segundo o chefe da Divisão de Repressão a Crimes Cibernéticos, de Palmas/TO, é insuficiente; deveriam ser ofertados de forma periódica, visando ao aprimoramento e à atualização profissional. Da mesma forma, os bancos de dados cujos acessos franqueados à Polícia Civil são obsoletos e limitados, além de, por vezes, desatualizados.

As melhorias apontadas pelo entrevistado perpassam pela solução dos problemas apresentados, como a ampliação expressa do poder requisitório do delegado de polícia, a fim de assegurar legalmente a possibilidade de obtenção administrativa de alguns dados preliminares importantes em investigações de crimes cibernéticos, como registros de conexão para criação de contas/perfis e de acessos específicos. Outro ponto é a necessidade de majoração dos prazos legais dispostos no Marco Civil da Internet, para fins de guarda e disponibilização obrigatória dos registros de conexão e de acesso pelos provedores de conexão e de aplicações de Internet, sendo também necessária a previsão expressa quanto à obrigatoriedade de guarda e disponibilização, dentro dos interstícios legais, da porta lógica em acessos via CGNAT.

Ademais, Santana (2023) destaca a necessidade de imposição de sanções cíveis, criminais e administrativas às plataformas que não colaborarem com as investigações ou recalcitrarem no cumprimento de medidas demandadas, conferindo-se efetividade ao art. 12 da Lei nº 12.965, de 2014. Também é imprescindível a capacitação de policiais civis para atuação nesse campo investigativo, acompanhada da necessária valorização profissional, do ponto de vista salarial e material/estrutural. A instituição policial deve ofertar, de forma periódica, cursos de atualização quanto aos métodos e às ferramentas de investigação de crimes cibernéticos, buscando-se os profissionais com mais expertise em cada temática, como no caso das apurações inerentes ao cometimento do crime de estupro virtual.

Santana (2023) afirma ser salutar uma maior integração de sistemas e bases de dados cadastrais, uma vez que a maioria dos alvos em investigações de crimes cibernéticos (até mesmo no caso de estupro virtual) reside em localidades distantes de onde está sediada a unidade investigativa, tornando-se essencial a pesquisa de suas qualificações em fontes oficiais atualizadas e integradas com diversas bases de dados, mesmo locais (concessionárias de energia, água, secretarias de saúde, de educação etc.)

Sob a perspectiva da perícia criminal, conforme exposto pela chefa do Núcleo de Computação Forense da Polícia Civil do Estado do Tocantins, há um conjunto de circunstâncias que contribuem para o rápido crescimento e disseminação dos crimes sexuais virtuais. Inicialmente, é relevante destacar a elevada complexidade dos exames periciais a serem realizados, demandando conhecimento altamente especializado.

No que se refere à referida complexidade investigativa relacionada ao trabalho da perícia técnica, os métodos de extração de dados em dispositivos eletrônicos são um exemplo do quão é necessário um profissional com avançados conhecimentos. Em relação aos métodos de extração, podemos relacionar os seguintes: a) manual (superficial); b) lógico em sentido amplo: nível lógico em sentido estrito e nível de sistema de arquivos; e) físico; f) *hex dump*; g) *chip-off*; h) *Join Teste Action Group* (JTAG); i) microleitura.

Na extração manual (superficial), não há a necessidade de utilização de nenhum *software* específico; os dados são acessados diretamente pelo manuseio do dispositivo, sendo necessário apenas que o dispositivo esteja desbloqueado. Neste método, é impossível a recuperação de dados excluídos.

A extração lógica em sentido amplo exige a utilização de *softwares* específicos, subdividindo-se em dois tipos de extrações: a) nível lógico em sentido estrito; b) nível de sistema de arquivos. Na primeira, o *software* faz interação com o sistema operacional do aparelho, podendo extrair vários dados importantes, como: SMS, contatos, registros de chamadas, mídias e áudios. Na segunda, o *software* coleta dados de *backup* do dispositivo, além de recuperar arquivos ocultos, podendo extrair imagens, vídeos e conteúdo de aplicativos (Facebook, WhatsApp, Instagram etc.).

A extração física é de maior profundidade, pois atinge a memória física do aparelho, sendo, em regra, o único método que recupera dados que foram excluídos, sendo também utilizado um *software*. O *hex dump é um método de extração física em que se utiliza um software* que acessa diretamente o conteúdo da memória *flash* do dispositivo e recupera dados apagados. A memória *flash* é um *chip* de memória de computador que mantém informações armazenadas sem a necessidade de uma fonte de energia.

Na mesma toada, no método *chip-off*, de extração física, o extrator retira o *chip* de memória da placa do aparelho e usa um leitor de *chip* para realizar a extração dos dados, podendo causar danos físicos no dispositivo, tratando-se de método altamente complexo, tendo em vista que especialmente os *smartphones* vêm apresentando codificação na memória física.

Outro método de extração física é o JTAG, em que ocorre a intervenção direta no aparelho utilizando o uso de solda na placa de circuitos do dispositivo, proporcionando o acesso a informações brutas armazenadas na memória *flash*. Ainda, tem-se o método de microleitura, também de extração física, que consiste na leitura em microscópio eletrônico de cada porta lógica do circuito da memória.

Analisando os métodos de extração de dados de dispositivos eletrônicos explicados acima, percebe-se que é de suma importância que os órgãos de investigação cibernética tenham à sua disposição ferramentas e *softwares* específicos para proceder ao trabalho investigativo de delitos sexuais cometidos no ambiente virtual. Nesse ponto, a perita criminal Leila (2023), afirma: *"É necessária a disponi-*

bilização de ferramentas e softwares especializados e recursos de armazenamento de dados digitais, o que demanda elevado investimento".

Além disso, a chefa do Núcleo de Computação Forense da Polícia Civil do Tocantins, ressaltou a circunstância da volatilidade da informação digital, sendo necessário o emprego de meios tecnológicos para a preservação de conteúdos extraídos e analisados, especialmente com vista à preservação da cadeia de custódia da prova digital.

Por fim, ao ser questionada sobre as melhorias que poderiam ser implementadas para fortalecer a investigação e combate a crimes virtuais sexuais, especialmente o estupro virtual, sob a ótica da perícia técnica, Leila (2023) ressaltou a importância da capacitação frequente dos peritos que atuam na área, a aquisição de ferramentas e de *softwares* especializados, recursos para armazenamento digital para facilitar o acesso aos relatórios pelos atores envolvidos na investigação, a filtragem prévia das evidências encaminhadas para análise pericial e o compartilhamento de informações entre atores da investigação e equipe pericial.

6 CONSIDERAÇÕES FINAIS

O estudo desenvolvido no presente artigo demonstrou que a prática do estupro virtual se adapta aos tipos penais dos crimes de estupro e estupro de vulnerável, tendo em vista consistirem em delitos de forma livre e pela circunstância da prescindibilidade do contato físico entre autor e vítima.

Na doutrina e na jurisprudência, conforme aventado, a prática do crime de estupro no ciberespaço é plenamente possível, já havendo casos julgados em que fora reconhecida a ocorrência do estupro virtual, existindo algumas ponderações no que se refere à virtualidade do delito sexual, pois tratar-se-ia de conduta real praticada em ambiente cibernético.

Outrossim, no que que tange à tipificação do estupro virtual, podemos concluir que a legislação atual comporta a prática do crime por meio do ambiente cibernético, tanto do art. 213 quanto do art. 217-A do Código Penal, não havendo que se falar em violação ao postulado principiológico da legalidade estrita.

Entretanto, conforme explicitado, seria de bom alvitre o aprimoramento da legislação, com vista a prever de forma expressa o cometimento da conduta no ambiente cibernético, o que traria mais estabilidade jurídica, além de dar uma redação moderna aos dispositivos legais supracitados.

A extorsão sexual praticada no ambiente cibernético, mesmo que haja uma finalidade lucrativa (patrimonial), não atrai a incidência do crime de extorsão de natureza patrimonial, tendo em vista que no primeiro o elemento subjetivo específico (especial fim de agir) é a satisfação da lascívia do autor do crime e praticada mediante grave ameaça adapta-se de forma imediata ao tipo penal do crime de estupro. No entanto, seria de bom alvitre que a legislação fosse aperfeiçoada, com

vista a afastar qualquer dúvida a respeito do enquadramento da extorsão sexual nos tipos penais dos crimes de estupro e de estupro de vulnerável.

De mais a mais, a investigação de crimes sexuais cometidos no meio virtual, especialmente o estupro virtual, demonstrou ser um grande desafio para a Polícia Judiciária Civil, não sendo diferente no estado do Tocantins, onde problemas são enfrentados tanto no campo investigativo quanto no espectro da atuação da perícia técnica, conforme explicitado no presente estudo científico.

Entretanto, conforme tratado, a Polícia Civil tocantinense desenvolveu importantes investigações exitosas na seara dos crimes sexuais cometidos no ciberespaço, no caso o estupro virtual, demonstrando expertise na área de investigação cibernética.

Outrossim, problemas em relação à operacionalização da coleta de vestígios digitais e armazenamento representam grandes barreiras à eficiência da tutela da higidez e integridade da cadeia de custódia da evidência digital, sendo necessários investimentos para a melhoria da atuação pericial.

No que diz respeito ao campo investigativo na polícia tocantinense, há a necessidade de proceder à capacitação dos policiais para que possam adquirir conhecimentos técnicos e operacionais para atuarem no âmbito da investigação de crimes cibernéticos, neles incluído o estupro virtual, o que já vem sendo realizado por meio das capacitações capitaneadas pela Escola Superior de Polícia do Tocantins (ESPOL/TO).

Ademais, a ampliação do poder requisitório do delegado de polícia somado à maior celeridade e presteza no atendimento dos pedidos de informações por parte dos provedores de conexão e de aplicações da Internet seria de grande relevância para as investigações de cibercrimes sexuais, especialmente em relação ao estupro virtual.

Portanto, a incidência de crimes sexuais no ambiente cibernético, incluindo nesta alçada o estupro virtual, é uma realidade contemporânea da criminalidade moderna, o que demanda um maior aprimoramento procedimental e operacional por parte dos órgãos de investigação, demanda esta que se faz presente no âmbito da Polícia Civil tocantinense, que tem buscado aprimorar as técnicas investigativas, seja por meio de cursos de capacitação ou por meio do uso de ferramentas e de *softwares* destinados ao desvendamento de delitos cometidos em detrimento da dignidade sexual dos usuários da grande rede.

REFERÊNCIAS

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus 70976-MS.** Rel.: Min. Joel Ilan Paciornik. Julgado em: 2/8/2016. DJe 10/8/2016.

CASELLI, Guilherme. **Manual de Investigação Digital.** 3. ed. São Paulo: JusPodivm, 2023.

CAVALCANTE, Márcio André Lopes. **Contato físico entre autor e vítima não é indispensável para configurar o delito**. Buscador Dizer o Direito, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/1f3202d820180a39f736f20fce790de8>. Acesso em: 2/6/2023.

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial.** 8. ed. Salvador: JusPodivm, 2016.

CRUZ, Shirley. **Ação conjunta das polícias civis do Tocantins e da Bahia resulta na prisão de homem investigado por estupro virtual de crianças e adolescentes.** Disponível em: https://www.to.gov.br/ssp/noticias/acao-conjunta-das-policias-civis-do-tocantins-e-da-bahia-resulta-na-prisao-de-homem-investigado-por-estupro-virtual-de-criancas-e-adolescentes/3y2lejo1fjom Acesso em: 13 ago. 2023.

GONÇALVES, Victor Eduardo Rios. **Direito Penal Esquematizado:** Parte Especial. 8. ed. São Paulo: Saraiva, 2018.

GOMES, Matheus Arruda. **Juiz do Piauí decreta primeira prisão por estupro virtual no Brasil.** Jusbrasil. Disponível em: https://www.jusbrasil.com.br/noticias/juiz-do-piaui-decreta-primeira-prisao-por-estupro-virtual-no-brasil/493303189 Acesso em: 25 jun. 2023.

LOPES. Mariângela Tomé. A infiltração de agentes no Brasil e na Espanha. Possibilidade de reformulação do sistema brasileiro com base no direito espanhol. **Revista Brasileira de Ciências Criminais.** São Paulo, v. 19, n. 89, p. 495-532, mar./abr. 2011.

MARTINS, José Renato. Não é correto se falar em estupro virtual, o crime de estupro só pode ser real. **Revista Consultor Jurídico**, 2017. Disponível em: https://www.conjur.com.br/2017-ago-18/opiniao-crime-estupro-real-nunca-virtual. Acesso em: 4/6/2023.

MASSON, Cleber. **Direito Penal:** parte especial arts. 213 a 359-h. 8. ed. São Paulo: Forense, 2018.

MACHADO, Nealla Valentim; PEREIRA, Silvio da Costa. Sexting, mídia e as novas representações da sexualidade. *In:* **Congresso Brasileiro de Ciência da Comunicação**, 36., 2013, Manaus, Papers. Manaus: Intercom, 2013, p. 1 – 12. Disponível em: https://www.intercom.org.br/papers/nacionais/2013/resumos/R8-1134-1.pdf. Acesso em: 23 abr. 2023.

MEIRELES, Luciano Miranda. A realidade do Estupro Virtual. *In.* **Revista Parquet em foco**. n. 1. Escola Superior do Ministério Público do Estado de Goiás. Goiânia: ESMP-GO (set./dez. 2017).

PEREIRA, M.T.M.A. **Investigação Policial de Crimes Eletrônicos.** São Paulo: Acadepol – Academia de Polícia "Dr. Coriolano Nogueira Cobra", 2019.

PORTO, Márcio Rogério. Experiências positivas em investigações envolvendo compartilhamento NAT e CGNAT sem a porta de origem. *In.* **Tratado de investigação criminal tecnológica.** 3. ed. São Paulo: JusPodivm, 2023.

SATO, Gustavo Worcki. A infiltração virtual de agentes e o combate à pedopornografia digital. *In.* **Direito Penal sob a perspectiva da investigação criminal tecnológica.** 2. ed. São Paulo: JusPodivm, 2023.

SILVA NETO, Luís Gonzaga da. Investigação Criminal Tecnológica do Estupro Virtual. *In.* **Direito Penal soba a Perspectiva da Investigação Criminal Tecnológica**. Jorge, Higor Vinicius Nogueira (Coord.). 2. ed. São Paulo: JusPodivm, 2023.

SILVA, Andressa Benevides da. **Estupro Virtual:** análise doutrinária e jurisprudencial, 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/estupro-virtual-analise-doutrinaria-e-jurisprudencial/. Acesso em: 23 abr. 2023.

TOCANTINS, Conexão. **Polícia Civil indicia homem suspeito de praticar o crime de "estupro virtual" contra mulher em Porto Nacional.** Disponível em: https://conexaoto.com.br/2021/10/08/policia-civil-indicia-homem-suspeito-de-praticar-o-crime-de-estupro-virtual-contra-mulher-em-porto-nacional Acesso em: 13 ago. 2023.

TOLEDO, Cleber. **Suspeito de "estupro virtual" em Miracema é preso em Palmas.** Disponível em: https://clebertoledo.com.br/tocantins/suspeito-de-estupro-virtual-em-miracema-e-preso-em-palmas/ Acesso em: 12 ago. 2023.

VALE, João Henrique do. **Minas Gerais registra primeiro caso de prisão por estupro virtual.** Jornal Estado de Minas, 21/09/2017. Disponível em: https://www.em.com.br/app/noticia/gerais/2017/09/21/interna_gerais,902256/minas-gerais-registra-primeiro-caso-de-prisao-por-estupro-virtual.shtml Acesso em: 25 jun. 2023.

Recebido em: 15/10/2023
Aprovado em: 24/10/2023