SECRETARIA DE SEGURANÇA PÚBLICA
UNIVERSIDADE ESTADUAL DE GOIÁS – UEG
COORDENADORIA DE ENSINO
COORDENAÇÃO DE ENSINO PRESENCIAL E DE PÓS-GRADUAÇÃO
ESPECIALIZAÇÃO EM GERENCIAMENTO DE SEGURANÇA PÚBLICA

DANIEL LOPES DA LUZ

ATUAÇÃO DA POLÍCIA MILITAR DO ESTADO DE GOIÁS (PM-GO) NO COMBATE AOS CRIMES DIGITAIS

GOIÂNIA

2024

DANIEL LOPES DA LUZ

ATUAÇÃO DA POLÍCIA MILITAR DO ESTADO DE GOIÁS (PM-GO) NO COMBATE AOS CRIMES DIGITAIS

Artigo apresentado como exigência parcial para aprovação na disciplina Metodologia do Trabalho Científico, do curso de Pós-Graduação em Gerenciamento em Segurança Pública (CEGESP), sob a orientação da Profa. Dra. Tatiane Ferreira Vilarinho.

GOIÂNIA

2024

ATUAÇÃO DA POLÍCIA MILITAR DO ESTADO DE GOIÁS (PM-GO) NO COMBATE AOS CRIMES DIGITAIS

Daniel Lopes da Luz*
Tatiane Ferreira Vilarinho**

Resumo:
O objetivo desse texto é discorrer sobre atuação da Polícia Militar do Estado de Goiás no combate aos crimes digitais. Para tanto, foi desenvolvida uma pesquisa bibliográfica, seguida de busca no sistema de ocorrências do estado RAI seguido de entrevista com responsável pela Delegacia de crimes cibernéticos do estado. Os principais resultados obtidos no estudo apontam que com o surgimento da internet, somado à criação e desenvolvimento das Tecnologias Digitais da Informação e Comunicação (TDICs), a humanidade não alcançou apenas benefícios, pois é perpassada também pelo aparecimento de várias modalidades de delitos ou ilícitos que passaram a ser praticados no ambiente virtual, chamados de crimes cibernéticos, informáticos ou virtuais. Dentre as principais conclusões da pesquisa tem-se que, relação ao serviço de inteligência das polícias militares, mais especificamente da PM-GO, há equipes de policiais tecnicamente especializadas para proceder ao levantamento de informações previstas no sistema jurídico brasileiro, embora muitas de suas ações, contemplando levantamento de informações sobre criminosos ou organizações criminosas, são mantidas sob sigilo, via de regra, posto que são empreendidas para subsidiar os comandantes de operações especiais na tomada de decisões sobre as melhores estratégias e táticas para a identificação e detenção dos infratores.

Palavras-chave: crimes digitais; Polícia Militar; serviço de inteligência.

Abstract: The objective of this text is to disagree about the role of the Military Police of the State of Goiás in combating digital crimes. To this end, a bibliographical research was carried out, followed by a search in the state's RAI occurrence system followed by an interview with the person responsible for the state's cyber crimes department. The main results obtained in the study indicate that with the emergence of the internet, added to the creation and development of Digital Information and Communication Technologies (TDICs), humanity has not only achieved benefits, as it is also permeated by the appearance of various types of delicious or illicit which began to be practiced in the virtual environment, called cyber, computer or virtual crimes. Among the main information of the research is that, in relation to the intelligence service of the military police, more specifically of the PM-GO, there are teams of specialized technical police officers to collect information provided for in the Brazilian legal system, although many of their Actions, including gathering information about criminals or criminal organizations, are kept confidential, as a rule, since they are undertaken to support special operations commanders in making decisions about the best strategies and tactics for identifying and detaining offenders.

Keywords: digital crimes; military police; intelligence service.

* Graduado em Direito pela Faculdade de Anicuns-GO (ANCUNS). Capitão da PM-GO. Especializando em Gerenciamento de Segurança Pública (SSP-GO/UEG). E-mail: daniel.lopes.go@gmail.com.
** Doutora e Mestra em Ciência da Informação pela Universidade de Brasília (UnB). Orientadora do curso de Especialização em Gerenciamento de Segurança Pública (SSP-GO/UEG). E-mail: tatianef.vilarinho@gmail.com.

1 INTRODUÇÃO

São muitos os avanços e benefícios proporcionados pelas Tecnologias Digitais da Informação e Comunicação (TDICs) mundo afora, com destaque para as facilidades de comunicação e acesso à informação, bem como a transformação de bens, produtos e serviços, tornando-os mais eficientes. Entretanto, criminosos se aproveitam desses recursos para praticar diferentes crimes e delitos, criando modalidades de crime a partir da internet e praticados apenas por meio dela, conforme relata Cassanti (2014).

Os primeiros registros de crimes informatizados são da década de 1970, perpetrados por especialistas em informática com a intenção de driblar sistemas de segurança empresariais. Pinheiro (2010) comenta que o foco principal desses delitos eram as instituições financeiras. No entanto, o perfil das pessoas que praticam crimes de informática mudou nos últimos anos, sendo que qualquer usuário com algum conhecimento e acesso à internet pode praticar um crime dessa natureza, pois já tem domínio no uso de aparelhos eletrônicos e das tecnologias digitais.

Há diversos nomes e diferentes tipificações para o que se convencionou chamar de crime cibernético ou informático, o que, conforme Silva (2015), dificulta que se adote uma nomenclatura mais rigorosa em torno de seu conceito. O que importa nesse contexto, contudo, não é a atribuição de um ou outro nome mais adequado para esses crimes, posto que o que deve ser levado em conta, ainda de acordo com a citada autora, é o uso de dispositivos informatizados e a rede de transmissão de dados com a intenção de delinquir e, consequentemente, lesar um bem jurídico de alguma vítima.

As instituições privadas e os órgãos de segurança pública têm grande dificuldade para combater delitos e fraudes no ambiente virtual na maioria dos países, ademais quando se leva em conta que as organizações criminosas despendem de vultosos investimentos nesses tipos de ilícitos, levando o poder público, em contrapartida, a investir em pessoal especializado e material tecnológico de ponta para, desse modo, fazer frente a esses crimes e criminosos, notadamente via inteligência policial (Cepik, 2003).

A inteligência policial tem ligação mais direta com as polícias Civil e Federal, posto que são elas que têm as prerrogativas constitucionais de polícia judiciária. Castro e Rondon Filho (2012) assentam, todavia, a existência e a efetividade da polícia judiciária militar que pode, inclusive, fazer uso da mesma metodologia das polícias Civil e Federal para buscar, coletar e identificar dados e informações e, consequentemente, analisar, integrar, utilizar e

validar esses mesmos dados e informações visando assessorar o planejamento e a decisão estatal via órgãos de segurança pública.

A questão norteadora do estudo que aqui se apresenta tem a ver, frente ao exposto, com a resposta à seguinte pergunta de pesquisa: as ações de inteligência policial da PM-GO têm sido eficazes no combate aos crimes digitais e no desmantelamento de quadrilhas ou organizações criminosas especializadas nesse tipo de crime?

A elaboração deste estudo teve, como foco, a atuação da Polícia Militar e suas ações no combate aos crimes digitais, justificando-se pela possibilidade de demonstrar que a PM-GO é dotada de um sistema presente em seus comandos regionais, apontando, então, em que medida seus recursos são utilizados, com foco na questão do combate aos crimes virtuais no estado de Goiás, indicando-se como o conhecimento produzido pelos seus setores de inteligência é usado, bem como sua eficácia e eficiência.

O objetivo geral do estudo consistiu, por sua vez, é discorrer sobre atuação da polícia militar do estado de goiás (pm-go) no combate aos crimes digitais. Os objetivos específicos elencados foram os seguintes:

a) Dissertar sobre a inteligência policial militar e as atribuições das polícias Civil e Federal;
b) Discorrer acerca dos crimes virtuais;
c) Mapear as ações da PM-GO no combate aos crimes virtuais respaldadas pela sua inteligência policial.

No tocante às hipóteses que direcionam o estudo, tem-se que a inteligência policial da PM-GO tem sido eficaz no combate aos crimes digitais no estado de Goiás, contribuindo para sua atuação operacional e técnica no desmantelamento de quadrilhas ou organizações criminosas, bem como para a identificação e punição dos criminosos especializados nesses tipos de delitos.

A metodologia adotada para a elaboração do trabalho assenta-se no método hipotético-dedutivo, adotando-se como procedimentos metodológicos a pesquisa bibliográfica, pois as informações atinentes às atividades da inteligência policial da PM-GO no combate aos crimes cibernéticos ou virtuais basearam-se no levantamento de referências que já foram analisadas e publicadas em formato digital ou impresso e estão disponibilizadas como artigos científicos, dissertações de mestrado e teses de doutorado.

O artigo está organizado em quatro seções ou tópicos, sendo a introdução o primeiro deles, vindo em seguida o tópico que disserta sobre os crimes virtuais contra a ordem pública e o serviço de inteligência da PM-GO na identificação desses ilícitos, bem como suas ações no enfrentamento dessa modalidade criminosa e das pessoas ou organizações criminosas que perpetram esses ilícitos. Também se disserta sobre as atribuições das polícias Civil e Federal.

Encerrando o trabalho tem-se as considerações finais do estudo enfatizando os principais achados teóricos do estudo, bem como o alcance ou não dos objetivos propostos em sua parte introdutória, vindo, a seguir, a indicação das referências que embasam sua elaboração.

2 CRIMES VIRTUAIS E A PM-GO

Os chamados crimes cibernéticos ou virtuais começaram a ganhar expressão no Brasil a partir da segunda metade dos anos 1990, especificamente no momento em que, conforme Cassanti (2014), descobriu-se uma "invasão" a vários sites ligados à administração federal, como o do Supremo Tribunal Federal (STF), mais precisamente em 18 de junho de 1996. Deste então, reforça o autor, a sociedade brasileira passou a ter conhecimento do que é um crime dessa natureza, de modo que os vários setores da administração pública passaram a ter um problema que só se agravaria ao longo dos anos.

Ao tratar dos crimes cibernéticos, Cardozo (2019) argumentam que crime, em seu sentido mais amplo, pode ser entendido como quaisquer atos ilícitos que são praticados por diferentes indivíduos, de forma descuidada ou proposital, expondo ou lesando bens jurídicos. Os autores consideram que, quanto aos crimes virtuais, estes correspondem a atos ilícitos, posto que são praticados por pessoas atingindo a sociedade, coletiva ou individualmente.

Frente aos avanços com a descoberta dos crimes cibernéticos, Malaquias (2012) assevera que se desenvolveu também uma preocupação por parte das autoridades públicas e dos usuários em geral, bem como de profissionais de diversas áreas. Para o autor, com as facilidades para o acesso a internet e, consequentemente, das redes sociais para as diferentes esferas da população mundo afora, tornou-se inevitável a modernização de diversas campos do conhecimento, impondo-se, inclusive, a reformulação de produtos e serviços.

Os crimes virtuais correspondem a uma nova espécie de delito ou ilícito criminal que, segundo Pinheiro (2010), não se encaixam nas definições já existentes, sendo-lhes imprescindível um meio próprio de realização. Tratando-se, então, de um crime de meio, pois

se utiliza do ambiente virtual e é cometido por *hackers*, cujo enquadramento jurídico em termos de tipificação remete às definições de estelionato, extorsão, falsidade ideológica, fraude e outros.

Ao tratar desses tipos de crimes, Bortot (2017) explica que eles são classificados em diferentes categorias, como a invasão cibernética ou o acesso não autorizado a um sistema virtual; a fraude cibernética, em que se dá o roubo da identidade de outra pessoa; a fraude *on-line* e a pirataria, dentre outras. Compõem ainda essa lista, segundo a autora, a pornografia cibernética e obscenidade, exemplificadas com os materiais de exploração infantil, e, a ciberviolência, cujos exemplos mais frequentes são o *cyberstalking* e o cyberterrorismo.

Ao tratar da classificação dos crimes digitais, Cardozo (2019) enfatizam que eles podem ser indiretos, mediados ou mistos; ou ainda impróprios e próprios. Em relação aos crimes digitais próprios, são aqueles em que a inviolabilidade dos dados ou informações sob automatização e proteção, enquanto bem jurídico na norma penal, são acessados indevidamente. Os impróprios são aqueles em que o aparato principal para seu cometimento é o próprio aparelho da vítima. Quanto aos mistos, o autor esclarece que se referem aos que decorrem da invasão de aparelhos eletrônicos. Já os mediatos ou indiretos não têm a ver com os delitos-fim informáticos, mas possuem algumas características comuns com eles.

Quanto à quantidade de crimes cibernéticos praticados tanto no Brasil como em outros países, Bortot (2017) comenta que é praticamente impossível apurar esses números por diversos fatores, com destaque para a falta de definições legais mais padronizadas para a investigação desses crimes, bem como para as poucas estatísticas oficiais que sejam, simultaneamente, confiáveis e válidas.

Não há dúvidas de que um tratamento mais rigoroso por parte da iniciativa privada e dos governos é indispensável para que se inicie a superação de abordagens e concepções políticas equivocadas. Diniz, Muggah e Glenny (2014) lembram que, em razão da natureza técnica da questão, cidadãos e governos encontram-se relativamente carentes de informações acerca das respostas que devem dar, sendo que empresas e instituições consideram que o entendimento dos pontos relacionados com essas práticas criminosas ultrapassa suas capacidades ou, ainda, que essas ameaças não têm muita relevância.

2.1 Crimes cibernéticos e as atribuições das polícias Civil e Federal

O art. 144 da Constituição Federal da República diz que a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I – polícia federal; II – polícia rodoviária federal; III – polícia ferroviária federal; IV – policias civis; V – policiais militares e corpos de bombeiros militares (Brasil, 1988).

A Polícia Civil é a instituição responsável pela investigação de práticas criminosas, bem como pela apuração das infrações penais. Entre suas principais atribuições está a investigação criminal, por meio da reunião de provas e da oitiva de testemunhas, coletando informações que esclareçam os fatos e identifique os responsáveis por ele. Cabe, à Polícia Civil, a instauração e condução de inquéritos policiais nos crimes de ação pública, a emissão de relatórios e laudos técnicos sobre os casos em curso, o cumprimento de mandados de busca e apreensão, bem como a efetiva prisão; dentre outros determinados pela autoridade judicial, auxiliando-a com o fornecimento de informações e provas para a instrução processual.

À Polícia Federal, por sua vez, cabe, dentre outras atribuições, em nível federal, o combate ao crime organizado, a investigação de crimes contra o sistema financeiro, assim como de crimes cibernéticos, o combate ao tráfico de drogas e armas, dentre outros.

2.2 Principais crimes cibernéticos ou informáticos

São várias as condutas que criminosos ou organizações criminosas praticam e podem ser entendidas ou reputadas como crimes cibernéticos ou informáticos, valendo-se de técnicas que são utilizadas para ter sucesso em suas atividades delituosas. Dentre as mais conhecidas, Soares (2019) aponta e discute o acesso ilegítimo, o dano informático, a fraude bancária e crimes contra a ordem econômico-financeira, o furto de dados, a interceptação ilegítima, a pedofilia e a pornografia infantil.

2.2.1 Acesso ilegítimo

Ao tratar do acesso ilegítimo, Jesus e Milagre (2016) comentam que se trata do ilícito do crime cibernético em que o criminoso acessa, sem autorização, violando ou não medidas de segurança, um dado no sistema informático, que pode ser apenas um aparelho ou dispositivo, bem como um grupo de dispositivos ou máquinas informatizadas que estejam interligados. Esse acesso acontece, segundo os autores, por meio ardiloso ou violento, sendo

frequente também a utilização de subterfúgios visando induzir a vítima a algum erro, o que favorece o acesso do criminoso.

Uma das técnicas mais utilizadas pelos criminosos virtuais para perpetrar o acesso ilegítimo é conhecido *backdoor* que, segundo FGV (2012) é um programa ou *software* que facilita o retorno do invasor ao dispositivo de informática invadido, dispensando a necessidade de se recorrer novamente aos métodos utilizados na primeira invasão. Em outros termos, o agente tem a garantia de acesso no futuro e de forma remota ao aparelho ou dispositivo da vítima.

A atividade delituosa de acesso ilegítimo em dispositivos informáticos tem previsão de punição no ordenamento jurídico brasileiro. Conforme a atualização dada pela Lei nº. 14.155/2021, de 27 de maio de 2021, ao Código Penal de 1940, em seu art. 154-A, a pena é de um a quatro anos de reclusão para ou autor do delito que "[...] adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita" (Brasil, 2021).

2.2.2 Dano informático

O delito conhecido como "dano informático" corresponde, de acordo com Milagres e Jesus (2016), ao ato ilegítimo e intencional de alterar, apagar, danificar, deteriorar ou eliminar dados informáticos ou informatizados valendo-se, por exemplo, de "vírus". Ou seja, de um programa malicioso com capacidade de se propagar a partir da geração de cópias de si mesmo, inserindo-se em outros arquivos e programas. Para que se dê a ativação de um "vírus" é preciso executar um arquivo ou programa infectado que é disponibilizado em e-mails e páginas de internet, bem como por mensagens de celular.

A probabilidade de um usuário de serviços de internet de ter seus dispositivos conectados à *web* ser "infectado" é alta, pois é corriqueiro o recebimento de "vírus" via mensagens não solicitadas, principalmente por e-mail, conhecidas como *spams*. Mensagens quie, mesmo sendo meramente publicitárias, são utilizadas, com frequência, para aplicar golpes cibernéticos ou virtuais, grande parte deles por meio da instalação de programas maliciosos (Brasil, 2012a).

Há também previsão legal de punição para o crime de "dano informático", conforme a atualização dada para o Código Penal, cujo tratamento é disposto no art. 163. Jesus e Milagre (2016) comentam que há algum tempo tentou-se um tratamento específico para o "dano

informático", mas, com a atualização do Código Penal pela Lei nº. 12.735/2012 (Brasil, 2012b), a proposta da inclusão desse dispositivo foi suprimida.

2.2.3 Furto de dados e interceptação ilegítima

A ação delituosa conhecida como "furto de dados" consiste na cópia ou movimentação ilegítima ou ilícita de informações confidenciais. Jesus e Milagre (2016) chamam a atenção para a inexistência, no ordenamento jurídico brasileiro, de algum dispositivo legal com previsão de punição para esse tipo de conduta delituosa. O que se tem é que, com o "vazamento" de informações da vítima, aplica-se o art. 153 do Código Penal, que trata do crime de divulgação de segredo.

O tratamento do "furto de dados" como uma qualificadora do crime de invasão de dispositivo informático é dado pelo § 3º do art. 154-A. Ocorre quando a invasão perpetrada pelo invasor tiver, como resultado, a posse conteúdo de comunicações eletrônicas tidas como privadas, segredos comerciais ou industriais e informações sigilosas definidas em lei por exemplo, bem como o controle, à distância ou remoto, não autorizado do dispositivo que foi invadido (Brasil, 2021).

Várias técnicas usadas nos ambientes virtuais não têm a função precípua de "furtar dados", mas os criminosos cibernéticos utilizam-nas para acessar informações sobre suas vítimas, como por exemplo o *spyware*, que é um programa criado para monitoramento de atividades de um dado sistema e enviar os registros para um terceiro. Dentre as várias espécies ou tipos de *spyware* tem-se o *keylogger*, que é utilizado na captura e armazenamento do que é digitado pelo usuário em seu teclado do computador ou celular. Há ainda o *screenlogger*, que tem a capacidade de guardar imagens de telas de dispositivos informáticos dos usuários, informações sigilosas inclusive.

Quanto à "interceptação ilegítima", Jesus e Milagre (2016) explicam que se trata do uso de meios técnicos visando a captura de informações que são transmitidas privadamente, podendo acontecer de duas formas: a) impedindo o recebimento de mensagens pelo destinatário ou b) permitindo o recebimento, mas com o interceptador tendo acesso ao conteúdo. Para este delito há previsão no ordenamento jurídico brasileiro, art. 10 da Lei nº. 9.296/1996, que regulamenta a parte final do inciso XII do art. 5º da Constituição da República Federativa do Brasil (Brasil, 1988).

2.2.4 Fraude bancária e crimes contra a ordem econômico-financeira

Dentre os crimes cibernéticos, informáticos ou virtuais conhecidos como “fraude bancária” e crimes contra a ordem econômico-financeira, Pinheiro (2010) destaca o estelionato digital, a extorsão e o furto mediante fraude. Sobre o estelionato digital o autor esclarece que já há previsão no Código Penal, em seu art. 171, consistindo na ação do criminoso em obter vantagem ilícita, para ele mesmo ou outra pessoa, causando prejuízo à vítima após induzi-la ou mantê-la em erro por meio de ardil, artifício ou quaisquer outros meios ou recursos fraudulentos. Também há a previsão da fraude eletrônica no art. 171, §2ª-A e § 2º-B, consistindo na fraude com utilização de informações fornecidas pela vítima ou por terceiro, induzindo a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou ainda por qualquer outro meio fraudulento análogo.

Esse tipo de crime pressupõe, de acordo com Santos e Fraga (2010), uma vítima cuja vontade está viciada e, desse modo, não oferece resistência para o cometimento do delito. Ele é cometido fartamente via internet, sendo comum a existência de pessoas que são vitimadas pelos criminosos nessa modalidade criminosa. Já existe, inclusive, pacificação jurisprudencial sobre a definição desse ilícito como estelionato digital que, segundo os citados autores, é diferenciado do furto mediante fraude no ambiente virtual, isso porque são fáceis de serem confundidos.

Em relação à extorsão enquanto crime informático, Magalhães, Parra Filho e Marcheri (2022) explicam que é mais comumente praticado com o uso de *ransomware*, um *software* do tipo *malware* criado com o escopo de infiltrar sistemas sem a percepção de seus proprietários ou titulares. Essa prática criminosa se efetiva quando dados com senhas de uma pessoa são compactados ou criptografados e o acesso dos titulares é bloqueado, inutilizando-se o dispositivo infectado; sendo que para acessá-lo de novo os criminosos exigem pagamento das vítimas.

2.2.5 Pedofilia e pornografia infantil

De acordo com a explicação trazida em seu site oficial, o Ministério Público de Santa Catarina explica que a pedofilia se refere “[à] atividade de aliciar crianças, pela internet ou qualquer outro meio, com o objetivo de praticar atos sexuais com elas, ou para fazê-las se exibirem de forma pornográfica [...]” (Santa Catarina, [2024]).

Dentre as principais condutas que são associadas à utilização da internet e outras tecnologias, o art. 241 do ECA tipifica a oferta e venda de materiais pornográficos infantojuvenis. O art. 241-A alude às condutas de oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar, por qualquer meio, materiais pornográficos, bem como assegurar o armazenamento e o acesso desses materiais por meio da rede de computadores. O art. 241-B, por sua vez, alude às condutas de aquisição, posse ou armazenamento, por qualquer meio, de materiais pornográficos (Brasil, 1990, 2008).

No que tange a violência sexual contra crianças e adolescentes, Basílio (2020) explica que o fundamental é “abrir os olhos” em relação a esse tipo crime. A autora aponta também o considerável despreparo do próprio sistema judiciário em lidar com casos como esses, apesar de ser nada mais que ações criminosas que atentam contra a dignidade da criança e do adolescente. Tais crimes

> Englobam [...] conjunção carnal, prática de ato libidinoso, presença, participação ou indução de menor de 14 (catorze) anos a satisfazer a lascívia própria ou de outrem, além de atos que submetam, induzam ou atraiam à prostituição ou outra forma de exploração sexual alguém menor de 18 (dezoito) anos (Tortoriello, 2019).

O que se precisa para o enfrentamento mais eficiente dos crimes sexuais, inclusive os virtuais, que atentam conta a dignidade de crianças e adolescentes, é a criação de uma ampla rede de tutela que consiga, sobretudo, diferenciar as vítimas infanto-juvenis.

A proteção à criança e ao adolescente nada mais é que uma obrigação de todos, pois não há dúvidas de que necessitam de todo cuidado e dedicação da sociedade. O ECA dispõe de diretrizes para esses cuidados e mudanças no que tange as regras com os menores, o que se chama de rede de proteção infanto-juvenil, a qual

> [...] trouxe inúmeras mudanças nas redes de proteção e fez avançar incontáveis pautas no que diz respeito aos Direitos Humanos de Crianças e Adolescentes no Brasil, ao, por exemplo, estabelecer os Conselhos e fundos de Direitos das crianças e adolescentes, assim como os conselhos tutelares. Tanta fora a primazia da referida legislação que o ECA chegou a ser condecorado pela Organização das Nações Unidas (ONU), em razão de seu conteúdo extremamente avançado (Basílio, 2020).

É visível que, mesmo com todo o amparo dado pelo texto legislativo, a ocorrência de casos em que se configuram abusos sexuais infanto-juvenis é frequente, ou seja,

> [...] casos de afronta aos direitos desse público infanto-juvenil são cada vez mais comuns, principalmente, quanto aos casos de violência sexual infantil, sendo a de dentro do convívio familiar mais difícil de ser detectada e combatida, pois o crime

> costuma ser camuflado e imperceptível, em razão do lugar onde é praticado, na maioria das vezes dentro de sua própria casa, e, cujos os agressores costumam ser de fácil identificação da vítima, como seus parentes, pessoas próximas ou de confiança dessas e/ou de seus pais (Lobato, 2019).

A maior preocupação em relação a esses indivíduos que têm desejo sexual em crianças e adolescentes é que, conforme Greco (2017), trata-se de pessoas que podem cometer abusos, assim como criar a própria pornografia, o que exige um trabalho especializado das forças de segurança, inclusive a infiltração policial.

2.3 Inteligência policial no combate aos crimes cibernéticos ou virtuais

Foi em 2001, quando uma facção criminosa demonstrou a capacidade de se comunicar com membros presos e promover rebeliões no estado de São Paulo e, posteriormente, em 2006, quando outras facções promoveram ataques, que se viu a necessidade de a inteligência policial intervir nesse universo de cometimento de crimes virtuais.

> Nas últimas décadas, a sociedade brasileira passou a sofrer com maior intensidade a ação das organizações criminosas devido ao recrutamento da violência e dos corriqueiros atentados a vida e ao patrimônio. Dessa forma, o medo, a instabilidade emocional e a insegurança se tornaram rotina para as pessoas principalmente nas grandes cidades (Jorge, 2018, p. 3).

A grande dificuldade que se tem nesse contexto tem a ver com a preservação da identidade dos comunicantes, o que atrapalha nas investigações, principalmente quando se trata de pessoas que estão se comunicando a partir de outros países, notadamente via rede mundial de computadores, em ambientes virtuais de acesso mais restrito, tais como a *darknet* e a *deep web*.

> Os crimes praticados no âmbito da *deep web* e *darknet* representam um grande desafio para a atuação dos órgãos de investigação criminal e inteligência, principalmente quando se levam em conta as dificuldades de investigar crimes praticados por intermédio desses ambientes virtuais, bem como os percalços que dificultam a antecipação de cenários e tornam inviáveis quaisquer tentativas de evitar práticas terroristas (Jorge, 2018, p. 4).

Na apuração da autoria e materialidade de crimes praticados na internet tem-se o recurso dos “dados negados”, o que é benéfico para aqueles que praticam crimes cibernéticos. De acordo com Jorge (2018), “dado negado, no âmbito da inteligência policial, é todo aquele

conhecimento de interesse do aparato estatal de investigação que não esteja disponível e que se exija a sua busca pelo elemento operacional".

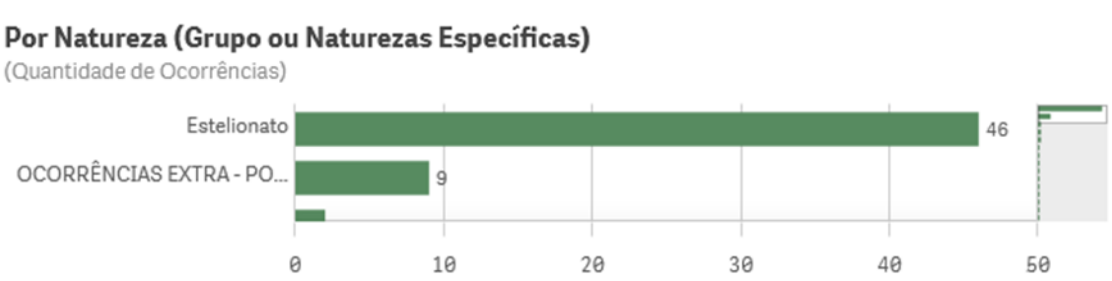
No caso brasileiro são muitas as entidades públicas envolvidas no que se pode chamar de gestão da segurança cibernética. Muitas delas, de acordo com Diniz, Muggah e Glenny (2014), estão focadas no desenvolvimento de ferramentas e técnicas de atualização, como o CSIRT brasileiro (CERT.br); o *Network Information Center* (NIC.br), que é responsável pelo gerenciamento do nome de domínio de primeiro nível do país. Há também, segundo os autores, o Centro de Segurança da Informação Renato Archer, do Ministério da Ciência e Tecnologia, o SERPRO e o INI, dentre muitos outros.

Quantos aos registros pela PM-GO de crimes cibernéticos, pesquisa realizada via ferramenta de visualização de informações e registros de ocorrências nominada "Qlik Sense", mostram que no ano de 2020 não houve ocorrências registradas na modalidade "crime cibernético". No ano de 2021 houve 48 registros pela PM-GO, sendo que, destas, 46 eram relacionadas a estelionato (Figuras 1 e 2).

Figura 1 - Registros de crimes cibernéticos em 2021 pela PM-GO

Fonte: Disponível em: https://paineis.ssp.go.gov.br/sense/app/7e16731c-d969-43b1-9426-29585e07ff23/sheet/2a01f478-bdf8-4a8f-8417-c1e26a44a3a8/state/analysis . Acesso em: 17 abr. 2024.

Figura 2 - Registros de crimes cibernéticos, em 2021, pela PM-GO, por natureza



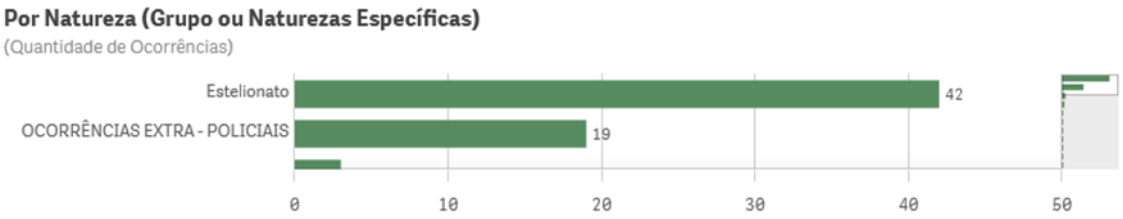
Fonte: dados da pesquisa (2024).

No Ano de 2022 houve 46 registros, com 42 ocorrências relacionadas a estelionato, resultando em uma diminuição de 6% em relação ao ano anterior (Figuras 3 e 4).

Figura 3 - Registros de crimes cibernéticos em 2022 pela PM-GO

Fonte: Fonte: dados da pesquisa (2024).

Figura 4 - Registros de crimes cibernéticos, em 2022, pela PM-GO, por natureza



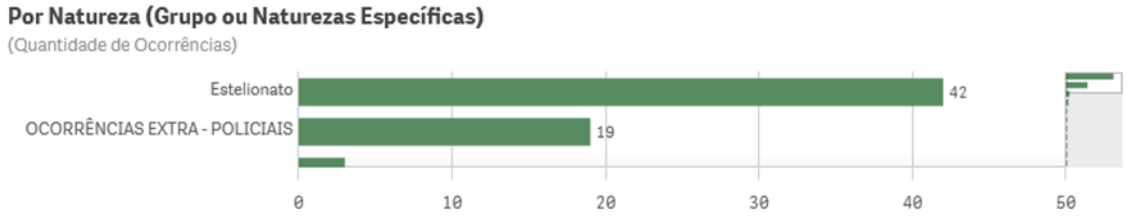
Fonte: Fonte: dados da pesquisa (2024).

No ano de 2023 houve 59 registros, destas, 57 relacionadas a estelionato e 18 relacionadas a outras ocorrências extrapoliciais. Verifica-se um aumento de 31% no registro de crimes cibernéticos pela PM-GO em relação a 2022 (Figuras 5 e 6).

Figura 5 - Registros de crimes cibernéticos em 2023 pela PM-GO

Fonte: Fonte: dados da pesquisa (2024).

Figura 6 - Registros de crimes cibernéticos, em 2023, pela PM-GO, por natureza



Fonte: Fonte: dados da pesquisa (2024).

Em contrapartida, segundo Valeriano (2023), o estado de Goiás registrou aumento de 1.022,2% nas ocorrências relacionadas a fraudes por meio eletrônico de 2021 para 2022, havendo um salto de 128 para 1.461 registros. De modo que o Estado alcançou o segundo lugar, no país, na quantidade de registros deste tipo de ocorrência, que vão além do estelionato, abrangendo cada vez mais casos de pedofilia, subtração de dados e assédio sexual por meio digital, que também configuram crimes cibernéticos.

Em entrevista para a pesquisa, com o titular da Delegacia Estadual de Repressão a Crimes Cibernéticos (DERCC) de Goiás, o titular informou que a atuação da Polícia Civil nestes crimes, onde há um trabalho integrado com outras polícias, principalmente nos crimes interestaduais, e uso de técnicas investigativas típicas da polícia judiciária. Sobre a instituição afeta de registro, relata que, normalmente, por não ser situação de flagrante ou pelo fato de exigir providências/técnicas exclusivas de polícia judiciária – como investigação e representações judiciais, as vítimas procuram diretamente a Polícia Civil. Mas há também as que procuram a Polícia Militar, sendo que estas são devidamente encaminhadas para o distrito policial ou para a DERCC.

Há ainda os registros realizados na Delegacia Virtual, de forma *on-line*, onde a vítima escolhe, no sistema, as opções desejadas e preenche os campos com as informações indispensáveis para o registro da ocorrência, a qual será submetida a avaliação para aprovação e validação.

Assim, o número de ocorrências registradas pela Polícia Militar, dentro de sua esfera de competência originária, não condiz com a quantidade de crimes que ocorrem, em decorrência de boa parte serem registrados na delegacia de Polícia Civil. O que, somado às barreiras legais da atribuição constitucional, dificultam o mapeamento, o levantamento de dados e a atuação incisiva da inteligência policial militar.

Há uma hierarquia entre as instituições governamentais que trabalham com gestão da segurança das redes brasileiras. Diniz, Muggah e Glenny (2014) pontuam que no topo está o Gabinete Presidencial de Segurança Institucional (GSI) que, em contato direto com o presidente da República, encarrega-se de lidar com todos os aspectos civis da segurança cibernética. É de sua responsabilidade também outras áreas, que incluem assuntos de ciberdefesa e militares.

A ação da Polícia Militar tem, como uma das principais características, o policiamento ostensivo, com o patrulhamento em áreas urbanas e rurais e atuação em situações de

emergência. Por outro lado, os crimes cibernéticos ocorrem majoritariamente no meio virtual, sendo que, conforme demonstrado, a maioria das vítimas procura e registra as ocorrências diretamente nas delegacias de Polícia Civil. No entanto, embora a competência de Polícia Judiciária esteja intrinsecamente ligada à das polícias Civil e Federal, nada obsta a Polícia Militar de Goiás de desenvolver ações para a redução das ocorrências de crimes cibernéticos.

Para aprimorar e possibilitar a atuação da Polícia Militar neste tipo de ocorrência a instituição necessita oferecer treinamento contínuo e especializado para os militares que atuam na área de inteligência para que possam estar atualizados a respeito das técnicas e tendências neste campo. E, desta forma, trabalhem em parceria com órgãos especializados em segurança cibernética, quais sejam, as Polícias Civil e Federal, para troca de informações, expertises e recursos. Isto tendo em vista que a colaboração, tanto em nível local quanto interestadual, pode ser crucial nas respostas a esses crimes, que transcendem fronteiras, alcançando múltiplas jurisdições e competências.

Primordial ainda é a aquisição e implementação de ferramentas tecnológicas avançadas para a repressão e prevenção de crimes cibernéticos, incluindo *softwares* e sistemas de monitoramento, visando o acompanhamento das redes sociais de perto e as atividades em outros espaços virtuais onde os criminosos cibernéticos possam atuar, identificando e rastreando potenciais ameaças. Além de também realizar campanhas e programas de conscientização junto à população para orientar sobre os perigos do mundo digital e como se proteger de crimes cibernéticos.

Assim, a divulgação de operações da Polícia Militar, isoladamente ou em conjunto com outras instituições, em jornais, redes sociais e outros canais de comunicação, também tem caráter preventivo. O que se deve buscar é cada vez mais maximizar o alcance dessas publicações, de forma categórica, sem que se exponha os meios e ferramentas utilizadas pelos agentes para que não perca a sua eficácia.

3 CONSIDERAÇÕES FINAIS

Buscou-se, neste artigo, evidenciar que o surgimento da internet, somado à criação e desenvolvimento das TDICs, a humanidade vem experimentando diversos avanços culturais, econômicos, políticos e sociais. Realidade que é perpassada também pelo surgimento de várias modalidades de delitos ou ilícitos que passaram a ser praticados no ambiente virtual, chamados de crimes cibernéticos, informáticos ou virtuais.

No estudo aponta-se que, quanto aos diversos crimes cibernéticos ou informáticos praticados nos ambientes virtuais, os mais conhecidos são: o acesso ilegítimo, o dano informático, a fraude bancária e crimes contra a ordem econômico-financeira, o furto de dados, a interceptação ilegítima, o estelionato na modalidade fraude eletrônica, a pedofilia e a pornografia infantil. Sendo que muitos deles já têm previsão legal de punição no ordenamento jurídico brasileiro, outros ainda aguardar a regulamentação legal por parte do legislativo federal.

Em relação ao serviço de inteligência das polícias militares, mais especificamente da PM-GO, há equipes de policiais tecnicamente especializadas para proceder o levantamento de informações previstas no sistema jurídico brasileiro. Muitas de suas ações contemplando o levantamento de informações de criminosos ou organizações criminosas são mantidas sob sigilo, via de regra, posto que são empreendidas para subsidiar os comandantes de operações especiais na tomada de decisão sobre as melhores estratégias e táticas para a identificação e detenção dos infratores.

Para que a Polícia Militar possa desempenhar seu mister de manutenção da ordem pública, que implica garantia dos direitos fundamentais, dentre os quais, direto à vida, à liberdade, à igualdade, à segurança e à propriedade, deve-se buscar perenemente treinamento contínuo e especializado para os militares que atuam na área de inteligência. Neste sentido, é preciso buscar parceria com as polícias Civil e Federal, particularmente as equipes especializadas em segurança cibernética. E, somado a isso, proceder a aquisição e implementação de ferramentas tecnológicas avançadas para o levantamento de informações e a prevenção de crimes cibernéticos. Bem como para o desenvolvimento de ações de conscientização ao cidadão para que não se torne um alvo “fácil”, além da maximização da divulgação de ocorrências com resultados positivos de forma a inibir a ação de pretensos criminosos.

REFERÊNCIAS

BASÍLIO, Jessyka. A eficácia do ECA na proteção da dignidade sexual na infância e adolescência. **Justificando**, [*s. l.*], 14 jul. 2020. Disponível em: https://www.justificando.com/2020/07/14/a-eficacia-do-eca-na-protecao-da-dignidade-sexual-na-infancia-e-adolescencia/. Acesso em: 17 abr. 2024.

BORTOT, Jéssica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **VirtuaJus**, Belo Horizonte, v. 2, n. 2, p. 338-362, 2017. Disponível em:

https://periodicos.pucminas.br/index.php/virtuajus/article/view/15745/15745-56007-1. Acesso em: 17 abr. 2024.

FUNDAÇÃO GETÚLIO VARGAS-FGV. Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro. **Relatório políticas de internet**: Brasil, 2011. São Paulo-SP: Comitê gestor da Internet do Brasil. Acesso em: 17 abr. 2024.

BRASIL. **Constituição Federal de 1988**. Brasília: Presidência da República, 1988. Disponível em https://www.jusbrasil.com.br/topicos/10644726/artigo-227-da-constituicao-federal-de-1988. Acesso em: 15 fev. 2021.

BRASIL. **Decreto n°. 5.007, de 8 de março de 2004**. Promulga o Protocolo Facultativo à Convenção sobre os Direitos da Criança referente à venda de crianças, à prostituição infantil e à pornografia infantil. Brasília: Presidência da República, 2004. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5007.htm. Acesso em: 17 abr. 2024.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília: Presidência da República, 1990. Disponível em http://www.planalto.gov.br/ccivil_03/ leis/l8069.htm. Acesso em abr./2024.

BRASIL. **Lei nº. 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969, Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989 [...]. Brasília: Presidência da República, 2012b. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 17 abr. 2024.

BRASIL. **Lei nº. 14.155/2021, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília: Presidência da República, 2021. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm#art1. Acesso em: 17 abr. 2024.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CASTRO, Clarindo Alves de.; RONDON FILHO, Edson Benedito (coord.). **Inteligência de segurança pública**. Curitiba-PR: Juruá, 2012.

CEPIK, Marco. Sistemas nacionais de inteligência: origens, lógica de expansão e configuração atual. **Dados**: Revista de Ciências Sociais, Rio de Janeiro, v. 46, n. 1, p. 75-127, 2003. DOI 10.1590/S0011-52582003000100003. Disponível em https://www.scielo.br/j/dados/a/6CLtBMghPGZrhsFFH5LhHrQ/?format=pdf&lang=pt. Acesso em: 17 abr./2024.

COUTO, Cleber. Pedofilia no Estatuto da Criança e Adolescente: art. 241-E e sua interpretação constitucional. **Jus Navigandi**, Teresina, v. 20, n. 4421, 9 ago. 2015. Disponível

em: https://jus.com.br/artigos/41178/ pedofilia-no-estatuto-da-crianca-e-adolescente-art-241-e-e-sua-interpretacao-constitucional. Acesso em: 17 abr. 2024.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. Deconstructing cyber security in brazil: threats and responses. **Igarapé Publications**, [Rio de Janeiro], paper estratégico n. 11. 2014. Disponível em: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf. Acesso em: 17 abr. 2024.

CASTRO, Clarindo Alves de., & RONDON FILHO, Edson Benedito (Coords.). **Inteligência de segurança pública**. Curitiba-PR: Ed. Juruá, 2012.

FERNANDES, Simone dos Santos Lemos; CALDI, Valéria. Do reflexo do desenvolvimento das novas tecnologias de informação na prática de crimes contra crianças e adolescentes. *In*: SILVA, Ângelo Roberto Ilha da (coord.). **Crimes cibernéticos**. Porto Alegre: Livraria do Advogado, 2017.

GRECO, Rogério. **Código penal comentado**. 11. ed. Niterói-RJ: Impetus, 2017.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

JORGE, Higor Vinícius Nogueira. **Investigação criminal tecnológica**: contém informações sobre inteligência policial, drones e recursos tecnológicos aplicados na investigação. 2. ed. Rio de Janeiro: Brasport, 2018. v. 2.

LOBATO, Camila Daniella Seabra. A violência sexual contra crianças e adolescentes: (in)eficácia da pena aplicada ao agressor sexual infantil. **Âmbito Jurídico**, São Paulo, v. 22, n. 181, fev. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/a-violencia-sexual-contra-criancas-e-adolescentes-ineficacia-da-pena-aplicada-ao-agressor-sexual-infantil/. Acesso em: 17 abr. 2024.

MAGALHÃES, Gabriela Alves Aires; PARRA FILHO, Raphael Hernandes; MARCHERI, Pedro Lima. **O enfrentamento jurídico dos ataques de ransomware no Brasil e no mundo**. Brazilian Journal of Developmet, v.8, n.9, p.61971-61984, 2022.
MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova**: a investigação criminal em busca da verdade. Curitiba: Juruá, 2012. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/51922/38896

NUCCI, Guilherme de Souza. **Manual de direito penal**. 10. ed. rev. e ampl. Rio de Janeiro: Forense, 2014. Disponível em: https://direitouniversitarioblog.files.wordpress.com/2017/02/manual-do-direito-penal-guilherme-nucci.pdf. Acesso em: 17 abr. 2024.

PINHEIRO, Juliano Lima. **Mercado de capitais**: fundamentos e técnicas. 5. ed. São Paulo: Atlas, 2009.

PINHEIRO, Patrícia Peck. **Direito digital**. 4. ed. São Paulo: Saraiva, 2010.

SANTA CATARINA. Ministério Público de Santa Catarina. **Sobre a pedofilia**. Florianópolis: MPSC, [2024]. Disponível em: https://www.mpsc.mp.br/navegacao-segura-na-

internet-e-combate-a-pedofilia/sobre-a-pedofilia#:~:text=Al%C3%A9m%20disso%2C%20a%20atividade%20de,a%203%20anos%2C%20e%20multa. Acesso em: 20 abr. 2024.

SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. **As múltiplas faces dos crimes eletrônicos e dos fenômenos tecnológicos e seus reflexos no universo jurídico**. São Paulo-SP: OAB SP, 2010.

SILVA, Camila Cortellete Pereira da; PINTO, Daniela Devico Martins; MILANI, Rute Grossi. Pedofilia, quem a comete? Um estudo bibliográfico do perfil do agressor. *In*: ENCONTRO INTERNACIONAL DE PRODUÇÃO CIENTÍFICA CESUMAR, 8., 2013, Maringá. **Anais eletrônicos** [...]. Maringá: Cesumar, 2013. Disponível em: cesumar.br/prppge/pesquisa/epcc2013/oit_mostra/Camila_Cortellete_Pereira_da_Silva.pdf. Acesso em: 17 abr. 2024.

SILVA, Patrícia Santos da. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

SOARES, Victor Augusto Gonçalves. **Crimes informáticos**: os desafios enfrentados pelo direito penal na era digital. 2019. Monografia (Graduação em Direito) - Centro de Ciências Sociais Aplicadas, Departamento de Direito, Universidade Federal do Rio Grande do Norte, Natal, 2019. Disponível em: https://repositorio.ufrn.br/handle/123456789/51725. Acesso em: 17 abr. 2024.

TORTORIELLO, Melissa. Combate a crimes contra a dignidade sexual de crianças e adolescentes na internet. **DireitoNet**, [*s. l.*], 26 jul. 2019. Direito Penal. Disponível em: https://www.direitonet.com.br/artigos/exibir/ 11039/Combate-a-crimes-contra-a-dignidade-sexual-de-criancas-e-adolescentes-na-internet. Acesso em: 17 abr. 2024.

VALERIANO, Maria Luiza. Crimes saem das ruas e vão para os meios eletrônicos em Goiás. **Portal 6**, Goiânia, 8 dez. 2023. Disponível em: https://portal6.com.br/2023/12/08/crimes-saem-das-ruas-e-vao-para-os-meios-eletronicos-em-goias/. Acesso em: 17 abr. 2024.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.