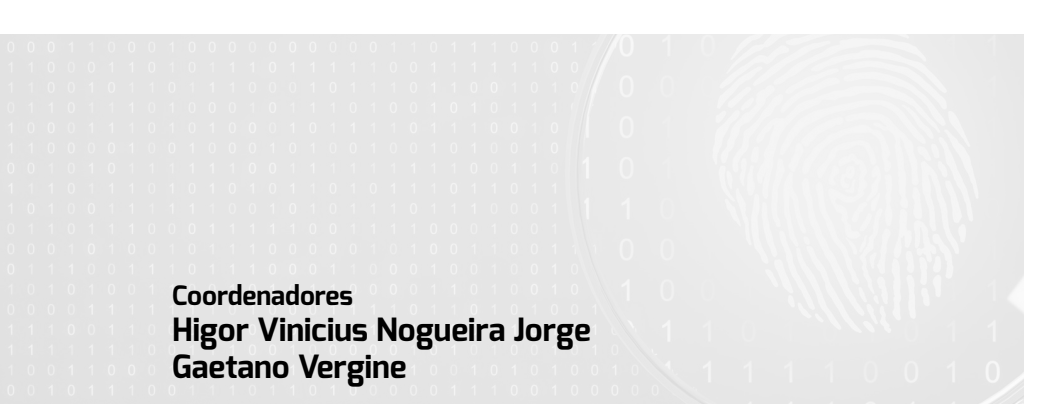




Coordenadores
Higor Vinicius Nogueira Jorge
Gaetano Vergine

RELATOS SOBRE A INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

4ª edição
Revista

2026

 **EDITORA**
*Jus***PODIVM**
www.editorajuspodivm.com.br

AÇÕES PREVENTIVAS NO ENFRENTAMENTO AO CIBERCRIME¹

GAETANO VERGINE E VANDER CRISTIAN RODRIGUES

SUMÁRIO: 2.1. Considerações iniciais; 2.2. O avanço tecnológico dos crimes virtuais; 2.3. O papel da Polícia Civil no enfrentamento ao cibercrime; 2.4. Golpe da falsa identidade; 2.5. Clonagem de WhatsApp; 2.6. Golpe do *Sim Swap*; 2.7. Fraude na entrega do produto; 2.8. Falsa empresa de crédito; 2.9. Falso leilão virtual; 2.10. Extorsão virtual; 2.11. Prevenção das fraudes digitais; 2.11.1. WhatsApp; 2.11.2. *E-commerce* fraudulento; 2.11.3. Falso leilão virtual; 2.11.4. Outras fraudes virtuais; 2.12. Dificuldades enfrentadas na investigação dos crimes virtuais; 2.13. Atuação preventiva especializada da polícia no combate ao cibercrime; 2.14. Considerações finais; 2.15. Referências.

2.1. CONSIDERAÇÕES INICIAIS

Iniciamos este trabalho discorrendo sobre o crescimento dos crimes virtuais no Brasil nos últimos anos, com o apontamento de dados estatísticos obtidos da polícia. Comentamos sobre os vazamentos de dados de grande vulto ocorridos no âmbito global, bem como sobre os seus efeitos na criminalidade.

Citamos a criação da Divisão de Crimes Cibernéticos (DCCIBER), no Departamento Estadual de Investigações Criminais (DEIC), com quatro delegacias especializadas empenhadas no enfrentamento

1. Importante destacar que o DECRETO LEGISLATIVO Nº 37, DE 2021 aprovou o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001.

dos crimes eletrônicos, quando houver envolvimento de organização criminosa ou com emprego de recurso de alta tecnologia.

Na sequência, esclarecemos o papel constitucional exercido pela Polícia Civil e focamos a sua importância na apuração das infrações penais praticadas no âmbito virtual. Explicamos a necessidade da capacitação dos policiais civis para combater essa criminalidade.

Elencamos alguns casos reais relatados por vítimas à polícia, com o desiderato de demonstrar o *modus operandi* dos golpistas digitais. Em contrapartida, apresentamos algumas recomendações de caráter preventivo aos usuários da internet que podem mitigar as fraudes.

Tratamos sobre a legislação vigente dos crimes eletrônicos e destacamos as dificuldades enfrentadas pelas autoridades policiais no curso das investigações criminais. Analisamos as perspectivas e ressaltamos a necessidade da integração das Instituições Financeiras e Empresas de Telefonia com a Polícia Civil para adoção de medidas de caráter preventivo especializado, visando reduzir o prejuízo às vítimas e dificultar a ação dos criminosos.

2.2. O AVANÇO TECNOLÓGICO DOS CRIMES VIRTUAIS

Com a necessidade de isolamento social em decorrência da pandemia gerada pela Covid-19, as pessoas foram obrigadas a passar maior tempo em suas residências em *home office*, fazendo uso de redes sociais para interagir com outras pessoas e realizar estudos, além de contratar serviços e efetuar compras *on-line*.

Aproveitando-se do avanço tecnológico e da engenharia social, os cibercriminosos entraram em cena e intensificaram a prática dos golpes virtuais, causando prejuízos econômicos e morais às vítimas.

Engenharia Social é a arte de enganar pessoas para obtenção de um dado ou informação, explora a curiosidade da pessoa, em vez de invadir ou usar técnicas de *hackers*. Por exemplo, em vez de tentar encontrar ou explorar uma vulnerabilidade de software, um engenheiro social pode chamar um funcionário e se passar por um alguém, para obtenção de uma senha ou acesso ao local premeditado. (PENTTINALI, 2018, Online).

No Brasil, a escalada da criminalidade virtual é alarmante. Comparada a anos anteriores, pesquisas apontam que em 2020 houve um crescimento exponencial dos crimes praticados por meio da rede

mundial de computadores, havendo uma enxurrada de denúncias e ocorrências registradas na polícia.

Dados estatísticos da Polícia Civil do Estado de São Paulo revelam que em 2020 foram registrados no estado de São Paulo cerca de 88 mil crimes ligados à internet, tais como estelionato, extorsão, invasão de dispositivo informático, falsa identidade, dentre outros tipos de fraudes. Em relação ao período de janeiro a maio de 2021, a estimativa é de 56 mil casos computados.

O número é assustador e constata-se uma elevação estimada em torno de 60% de casos registrados nos cinco primeiros meses deste ano, quando comparado com o mesmo período de 2020. A projeção desses números aponta o aumento de casos para os próximos anos. Ressalte-se, ainda, que há inúmeras vítimas que deixam de denunciar fraudes à polícia por diversos motivos ocasionando a subnotificação.

Não bastasse essa situação, em janeiro deste ano a mídia noticiou o impactante megavazamento de 223 milhões de números de CPFs contendo dados básicos dos cidadãos, como nome completo, sexo e data de nascimento, os quais foram expostos em fóruns na Deep e na Dark Web, sendo impossível saber para quantos criminosos foram compartilhadas e comercializadas essas informações (G1, 2021).

No início do mês de abril, também foi divulgado outro vazamento de dados de aproximadamente 553 milhões de usuários do Facebook, os quais tiveram suas informações pessoais disponibilizadas em Fóruns gratuitamente, como números de celular, endereços de e-mail e localização (ÉPOCA, 2021).

Para se ter uma ideia, esses dados obtidos ilicitamente potencializam a prática de outros delitos. O phishing, que é o crime onde o golpista engana a vítima por meio virtual a compartilhar informações confidenciais como senhas ou número de cartões bancários, ou seja, uma verdadeira pescaria, também é utilizado pelos cibercriminosos para complementar as informações obtidas de bancos de dados vazados ou hackeados.

De posse das credenciais obtidas ilicitamente, o estelionatário assume a identidade da vítima e realiza compras com cartões de créditos, promove a abertura de crediário em lojas de médio e/ou de grande porte e falsifica documentos pessoais, além do cometimento de outros crimes (DEFESANET, 2020).

Segundo Santos (2021), o volume e a extensão dos dados vazados trazem uma vasta possibilidade para a prática das mais diversas espécies de fraudes e também o que chamamos de engenharia social, comprometendo a segurança de dados dos brasileiros. Acrescenta que o impacto de vazamento de dados pode gerar consequências durante anos, visto que os dados comprometidos se referem a identificação e documentos pessoais não substituíveis.

2.3. O PAPEL DA POLÍCIA CIVIL NO ENFRENTAMENTO AO CIBERCRIME

A Carta Magna atribuiu às Polícias Cíveis, dirigidas por delegados de polícia de carreira, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, excetuando-se as militares (BRASIL, 1988).

A Lei 12.830/2013, art. 2º, complementando o ditame constitucional, definiu que as funções de polícia judiciária e a apuração de infrações penais exercidas pelo Delegado de Polícia são de natureza jurídica, essenciais e exclusivas de Estado (BRASIL, 2013).

No âmbito estadual, a Lei Orgânica da Polícia atribuiu à Polícia Civil o exercício da Polícia Judiciária, Administrativa e a Preventiva Especializada (SÃO PAULO, 1979).

Conforme o Seminário Integrado de Polícia Judiciária da União e do Estado de São Paulo realizado na ACADEPOL, podemos afirmar que:

A expressão “polícia judiciária” designa o complexo de atividades exercidas pelas Polícias Civil e Federal, tendentes à apuração de autoria, materialidade e demais circunstâncias das infrações penais comuns, à execução do policiamento preventivo especializado e ao desempenho de funções típicas de auxílio amplo à prestação jurisdicional penal, sempre sob direção e responsabilidade do Delegado de Polícia (ACADEPOL, 2013, Online).

Veja-se, então, que no âmbito estadual cabe exclusivamente à Polícia Civil apurar as infrações penais praticadas através do Inquérito Policial e/ou Termo Circunstanciado, sem olvidar da apuração preliminar sumária realizada pela Verificação das Procedências das Informações (VPI), em observância da legislação vigente (BRASIL, 1941).

Daí o importante papel desempenhado pelas Polícias Cíveis no combate aos crimes virtuais, por meio da investigação criminal visando a manutenção da ordem pública.

Para o efetivo enfrentamento dos crimes cibernéticos, no Estado de São Paulo, por meio do Decreto nº 65.241, de 13 de Outubro de 2020, foi criado no Departamento Estadual de Investigações Criminais (DEIC), a Divisão de Crimes Cibernéticos (DCCIBER), com quatro delegacias especializadas, objetivando-se apurar e reprimir fraudes praticadas por meios eletrônicos, com o envolvimento de organizações criminosas ou emprego de recursos de alta tecnologia, contra instituições financeiras, contra instituições de comércio eletrônico, contra violação de dispositivos eletrônicos e redes de dados, bem como ao combate à lavagem ou ocultação de ativos ilícitos.

No mesmo contexto, visando promover o devido apoio técnico às delegacias especializadas, o citado decreto também criou o Centro de Inteligência Cibernética (CIC) e o Laboratório Técnico de Análises Cibernéticas – Lab-Tac, onde atuam policiais qualificados com conhecimento técnico específico e há equipamentos modernos de alta tecnologia. A estrutura da DCCIBER dispõe de um plantão policial para atendimento ao público durante a semana, de segunda a sexta-feira, para a elaboração de registros dos crimes praticados por meio da internet praticados por organizações criminosas ou com emprego de recurso de alta tecnologia.

A DCCIBER iniciou suas atividades no dia 2 de dezembro de 2020, e a Academia da Polícia de São Paulo (ACADEPOL) promoveu cursos específicos a todos policiais designados à divisão cibernética sobre métodos de investigação virtual e combate ao cibercrime, de modo a capacitar os profissionais para atuar na investigação criminal dos crimes digitais.

No que diz respeito a segurança pública relacionada aos crimes virtuais, consigne-se que diferentemente do que ocorre no mundo real onde o policiamento preventivo ostensivo é realizado pela Polícia Militar com a ocupação dos espaços públicos por policiais fardados e viaturas caracterizadas, no ciberespaço esse rigor de fato não acontece.

Indicadores apontam que esse cenário de vulnerabilidade na internet vem se agravando cada vez mais, notadamente em decor-

rência da evolução tecnológica dos golpes digitais e dos ataques de engenharia social com diferentes abordagens.

Destarte, é justamente nessa lacuna existente no ciberespaço que os golpistas virtuais atuam de modo nefasto praticando os mais diversos crimes cibernéticos em detrimento dos usuários da internet.

Estudos apontam que no Brasil o uso de dispositivo móvel com internet é utilizado por golpistas como ferramenta necessária para alcançar o intento criminoso, tal como ocorre nos estelionatos praticados por meio de redes sociais, sites falsos, leilões virtuais, clonagem de cartões de crédito, dentre outras fraudes. Em outros termos, significa dizer que independente do crime praticado, em algum momento o cibercriminoso interage com a vítima por meio de um celular ou tablet.

Nesse sentido, a análise desenvolvida pelo Centro de Inteligência Cibernética (CIC) sobre os crimes cometidos no ciberespaço, indica que por se tratar de um aplicativo muito popular entre os brasileiros utilizado para recebimento e entrega de mensagens criptografadas, o WhatsApp é o serviço de mensageria preferido utilizado por golpistas à prática de inúmeras fraudes, causando prejuízos econômicos e morais às vítimas, parentes e pessoas ligadas.

Frise-se que diuturnamente são reportados à polícia casos de crimes virtuais realizados com o recurso do aplicativo de mensagem, sendo elencados para melhor entendimento alguns casos reais relatados por vítimas demonstrando o modus operandi do agente e o contexto da ação criminosa.

2.4. GOLPE DA FALSA IDENTIDADE

Residente do interior de São Paulo, a vítima relatou ter recebido mensagens via WhatsApp oriundas de uma linha telefônica prefixo 71, Salvador/BA, onde uma interlocutora com voz feminina se fez passar por sua filha, residente naquela cidade.

A golpista disse ter cancelado a linha telefônica que utilizava, alegando que havia perdido o aparelho celular. Com este artifício, a criminosa convenceu a vítima a fazer pagamentos argumentando serem dívidas contraídas com algumas pessoas, acrescentando que em razão da perda do telefone não conseguia fazer os pagamentos via internet.

Acreditando se tratar de sua filha, a vítima realizou as transferências solicitadas para três contas de bancos distintos, totalizando o valor de R\$25.000,00. Somente após confirmar as transações financeiras, a vítima percebeu que havia caído em um golpe.

2.5. CLONAGEM DE WHATSAPP

Noticiou a vítima ter recebido uma ligação telefônica, na qual o interlocutor com voz masculina disse que havia sido realizado um sorteio e a vítima teria ganhado um prêmio da operadora de telefonia no valor de R\$5.000,00. Porém, para receber tal quantia, bastaria apenas responder uma mensagem que receberia via “SMS” com um código.

Ocorre que, ao informar ao interlocutor o código recebido, perdeu o acesso do seu aplicativo de mensagens WhatsApp, constatando que algo de errado havia acontecido.

Em continuidade delitiva, de posse da conta de WhatsApp da vítima, fazendo-se passar por ela, o golpista passou a solicitar ajuda financeira a parentes, amigos e colegas de trabalho, sendo que um primo, uma tia e um amigo realizaram transferências bancárias para cinco contas correntes distintas dos criminosos, totalizando o valor de R\$35.000,00.

2.6. GOLPE DO SIM SWAP

Contou a vítima que numa tarde de quinta-feira tentou fazer ligações telefônicas do seu telefone celular prefixo 11, São Paulo/SP, mas não conseguiu pois sua linha estava inoperante. Em seguida, passou a receber e-mails confirmando o pagamento pela conta mercado pago, razão pela qual entrou em contato com a empresa para bloquear a conta e com a operadora de telefonia para bloquear a linha.

Na ocasião, tomou conhecimento que uma das revendas da operadora havia transferido sua linha telefônica para um novo chip sem a sua autorização, e em circunstâncias não esclarecidas pela atendente, posteriormente tomando conhecimento que havia sido vítima do golpe conhecido como *Sim Swap*.

Alegou ainda que ao conferir o extrato da conta bancária, via aplicativo, identificou a existência de vinte duas movimentações de

débitos de origens desconhecidas, totalizando um prejuízo no valor de R\$8.950,00, vinculados a pagamentos de boletos diversos.

Consigne-se que neste tipo de golpe, o fraudador “oculto” se utiliza de uma terceira pessoa para transferir a linha do chip de uma vítima para um chip em branco a ser utilizado pelo golpista, procedimento este feito junto à operadora de telefonia e sem anuência do contratante do serviço de acesso à internet.

2.7. FRAUDE NA ENTREGA DE PRODUTO

Desejando adquirir um telefone celular, a vítima entrou em contato telefônico com um suposto vendedor com voz masculina que comercializava referido aparelho através de uma página na internet, através de um número telefone celular, prefixo 11, São Paulo/SP.

As tratativas prosseguiram via WhatsApp, e o suposto vendedor identificou-se à vítima. Para dar maior credibilidade à venda, o suposto comerciante indicou seu perfil na rede social Instagram para consulta. Ocorre que, firmado o acordo sobre o valor de venda do aparelho e seguindo as orientações do golpista, a vítima realizou uma transferência bancária no valor de R\$2.750,00, para uma conta corrente indicada pelo suposto vendedor em nome de terceiro.

Porém, após efetuado o pagamento, a vítima foi imediatamente bloqueada no WhatsApp pelo golpista, momento em que percebeu que havia caído numa fraude. A vítima fez contato com a instituição bancária, mas não foi possível realizar o bloqueio da transferência bancária indevida.

2.8. FALSA EMPRESA DE CRÉDITO

Relatou a vítima ter acessado um site de uma suposta instituição de crédito, onde preencheu o cadastro de solicitação de empréstimo disponível na página da internet, no valor de R\$15.000,00. No dia seguinte, foi contatada via WhatsApp e o suposto funcionário confirmou a aprovação do crédito nos termos solicitados.

Para efetivar o empréstimo, a vítima foi orientada a encaminhar cópias do CPF, RG e comprovante de residência, bem como foi solicitada três assinaturas numa folha em branco igual ao seu RG

para confecção do contrato de empréstimo, sem a presença física da contratante na sede da empresa.

Os documentos foram escaneados e remetidos via WhatsApp pela vítima, que em contrapartida recebeu o acordo formal na importância solicitada. Para finalizar as tratativas, solicitou-se à vítima o pagamento via PIX de R\$726,64, referente a taxa de fiador, sendo indicada uma conta bancária para o depósito.

Após o pagamento, a vítima novamente foi contatada onde solicitou-se o pagamento via PIX de R\$1.499,89, para o pagamento de um imposto cobrado pela Receita Federal, sendo providenciada a transferência bancária à conta bancária indicada pelo golpista. Na sequência, a vítima recebeu um comprovante de transferência eletrônica disponível (TED) no valor de R\$18.890,00, mas referido valor não caiu na sua conta.

O interlocutor justificou que se tratava de uma conversão cambial e a vítima deveria devolver o valor depositado a maior de R\$3.890,00, com depósito em outras duas contas correntes. Necessitando do empréstimo, a vítima realizou as transferências solicitadas em contas bancárias indicadas pelo criminoso, momento em que desconfiou que algo estava errado. Então, fez uma ligação à verdadeira empresa, vindo a confirmação que havia caído num golpe.

2.9. FALSO LEILÃO VIRTUAL

Noticiou a vítima que após realizar pesquisas sobre sites de leilões de veículos, acabou localizando uma página na internet onde haviam anúncios de diversos leilões de automóveis, tendo se interessado em adquirir um veículo Honda/HRV anunciado.

Depois de realizar alguns lances, o site contemplou a vítima com a oferta de R\$36.530,00. Em seguida, recebeu uma mensagem pelo aplicativo WhatsApp pelo suposto canal de atendimento da página virtual, onde foi orientada a efetuar o pagamento do lote arrematado através da TED para a conta indicada pelo golpista.

Feita a transferência, a vítima recebeu o termo de arrematação onde constava o endereço para retirada do automóvel, situado no bairro da Mooca/SP. Ao se dirigir ao local indicado, a vítima confirmou que havia caído num golpe, pois se situava uma fábrica de fraldas.

2.10. EXTORSÃO VIRTUAL

Relatou a vítima ter recebido via rede social Facebook um pedido de amizade de um perfil de nome Sabrina Angélica de Azevedo, ostentando uma fotografia de uma pessoa do sexo feminino. Após aceitar tal convite, passou a manter contato com a suposta mulher, sendo que em determinado momento ela passou a enviar à vítima fotografias suas desnudas, bem como solicitou à vítima que lhe enviasse fotos da mesma maneira, o que de fato aconteceu.

Em seguida, as conversas migraram para o aplicativo WhatsApp onde continuaram a falar sobre erotismo e trocaram fotos pornográficas. Ocorre que, no dia seguinte, a vítima recebeu uma ligação de uma linha telefônica desconhecida, onde uma pessoa com voz masculina identificou-se como sendo João Marcos de Azevedo, dizendo-se pai da adolescente, alegando que teria acessado todo conteúdo pornográfico enviado via aplicativo à sua filha.

Alegou que Sabrina era menor de idade e que apresentaria uma “denúncia”. João, o golpista, ainda enviou mensagens com as fotos pornográficas da vítima para provar o que dizia, afirmando que caso não fosse feita a transferência do valor de R\$7.400,00, a “denúncia” seria apresentada à polícia.

João indicou a conta e banco de uma terceira pessoa, sendo que a vítima, sentindo-se pressionada com tal situação, rapidamente realizou a transferência bancária. Após enviar o comprovante de depósito, o suposto pai de Sabrina bloqueou o contato. Neste momento, a vítima percebeu que se tratava de um golpe.

2.11. PREVENÇÃO DAS FRAUDES DIGITAIS

Diante desse panorama, o primeiro passo para reduzir o número de fraudes virtuais é a conscientização dos usuários da internet sobre a necessidade da adoção de medidas de caráter preventivo.

2.11.1. WhatsApp

Tendo em vista o número expressivo de fraudes envolvem o WhatsApp, recomenda-se algumas providências de caráter preventivo ao usuário: a) ativar a confirmação em duas etapas do aplicativo; b) nunca fornecer código verificador que receber via “SMS” em seu

dispositivo móvel; c) não instalar aplicativos de origem desconhecida; d) não compartilhar informações pessoais a pedido de terceiros; e) desconfiar de situações onde alguém solicitar transferências ou pagamentos em caráter urgente; f) realizar contato com a pessoa que solicitou o dinheiro antes de confirmar a transação.

Caso confirmado o golpe, lembramos que o WhatsApp dispõe de um canal de suporte através do e-mail (support@whatsapp.com), com o assunto “Conta Hackeada – Desativação de Conta”, onde a vítima deve reportar o ocorrido seguindo as instruções para bloqueio da conta.

Sugere-se, ainda, o contato junto ao banco visando o bloqueio do dinheiro e o contato com familiares, amigos e grupos, objetivando-se informá-los sobre golpe e evitar o surgimento de outras vítimas.

2.11.2. E-commerce fraudulento

Para evitar o golpe de comércio eletrônico falso, recomenda-se ao usuário as seguintes medidas preventivas: a) utilizar terminais (computador, smartphone, tablet) que sejam seguros; b) ler atentamente as informações dos sites e do produto que deseja comprar, pois normalmente sites fraudulentos podem conter erros de português ou de informações técnicas do produto; c) verificar se há CNPJ cadastrado na página ou canais de comunicação; d) realizar pesquisa de mercado do valor do produto que deseja adquirir, desconfiando de preços muito baixos; e) promover pesquisas na internet para obter informações a respeito da reputação do site em que deseja efetuar compras; f) verificar se o site é seguro, localizando o ícone de um cadeado ao lado do endereço URL, pois ao clicar no ícone será exibido o certificado de segurança da página; g) evitar clicar em links que direcionam a navegação diretamente ao site de compras. Ao invés disso, deve-se digitar o endereço do site (URL) junto à barra de endereço de seu navegador.

Outro aspecto importante é atentar-se no sentido de que os sites fraudulentos geralmente possuem um endereço muito semelhante ao site verdadeiro. Exemplo hipotético: [www.americanas.com.br] (site verdadeiro) e [www.lojasamercanas.com.br] (site falso – exemplo fictício). Note-se que no exemplo do site falso foi incluído o nome “lojas” e a letra “i” do nome “americanas” foi suprimida.

2.11.3. Falso leilão virtual

Nessa espécie de estelionato, aconselha-se ao usuário: a) utilizar dispositivos (computador, *smartphone*, *tablet*) que sejam seguros; b) ler atentamente as informações contidas no site e do veículo que deseja arrematar; c) pesquisar o CNPJ e o endereço informados junto ao site; d) desconfiar de preços muito baixos e fazer uma pesquisa em relação ao veículo que deseja arrematar; e) realizar pesquisas na internet para obter informações a respeito da reputação do site, pois essas informações podem ser obtidas através do Reclame Aqui ou de redes sociais. É possível verificar a lista de sites reprovados, disponibilizada pelo Procon; f) verificar se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço URL; g) conferir o destino do pagamento. No termo de arrematação, a conta bancária informada para a transferência deve estar em nome do Leiloeiro. Não efetue o pagamento, caso haja qualquer divergência; h) Evite clicar em links que direcionam a navegação diretamente ao site de leilão online. Prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador.

Deve-se atentar que os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro, sendo modificado de forma quase imperceptível. Portanto, verifique atentamente o endereço a fim de se certificar se o site em que está se conectando é o site verdadeiro.

2.11.4. Outras fraudes virtuais

Como regra geral para inibir fraudes bancárias ou invasão de dispositivos, orienta-se aos usuários as seguintes cautelas: a) evitar usar computadores públicos e redes abertas de wi-fi para acessar conta bancária ou fazer compras online; b) não abrir e-mails de origem ou de procedência duvidosa; c) não executar programas, abrir arquivos ou clicar em links que estejam anexados ou no corpo desses e-mails; d) deletar esses e-mails e, caso tenha clicado em alguma parte deste e-mail e executado um programa, comunicar imediatamente ao seu banco o ocorrido e alterar todas as suas senhas de acesso à sua conta bancária em outro computador confiável, ou no mesmo após uma verificação completa de infecção de vírus por um técnico confiável; e) não utilizar o cartão bancário para fazer compras em sites desconhecidos.

2.12. DIFICULDADES ENFRENTADAS NA INVESTIGAÇÃO DOS CRIMES VIRTUAIS

A investigação criminal dos crimes digitais normalmente tem início com o registro do boletim de ocorrência eletrônico elaborado pela vítima, por requisição judicial ou ministerial ou ainda mediante requerimento do ofendido. No decorrer das diligências, o delegado de polícia e seus agentes buscam com a devida celeridade coletar a maior quantidade de evidências probatórias para apurar a autoria, materialidade e as circunstâncias do crime.

Sumariamente, podemos dizer que o fluxo das diligências investigatórias do inquérito policial tem início com a identificação do endereço IP do dispositivo eletrônico (de onde partiu o crime) e qualificação do correntista (golpista), passa pela fase da identificação do usuário do IP (qualificação) e pelas pesquisas e análises policiais, quebras dos sigilos telemático, telefônico, bancário e medidas cautelares, e por fim conclui-se com o eventual indiciamento e relatório final.

Segundo Rocha (2003), os crimes cibernéticos devem ser investigados por policiais com conhecimento específico, pois as dificuldades são grandes e esses crimes quase não deixam pistas, devendo a polícia acompanhar e monitorar o espaço cibernético.

Nessa linha, a dificuldade da investigação criminal começa com a morosidade da vítima em reportar o caso à polícia, visto que o crime cibernético é volátil e num curto espaço de tempo as pistas são apagadas.

A Lei 12.830/13, Art. 2º, § 2º, determina que durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos (BRASIL, 2013).

No que diz respeito ao acesso a registros, dados cadastrais, documentos e informações, na mesma linha dispõe a Lei 12.850/13:

Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. (BRASIL, 2013).

Apesar disso, algumas empresas dificultam o atendimento e/ou demoram a responder requisições expedidas pelas autoridades policiais, causando morosidade às investigações e perdimento das provas. Outro impasse é que algumas empresas somente cedem dados de registro de conexão mediante ordem judicial.

Marco Civil da Internet. Lei 12.965/2014, Art. 10, § 2º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput (registros de conexão e de acesso a aplicações de internet), de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. (Brasil, 2014).

Para melhor entendimento, o registro de conexão compreende o conjunto de informações referentes à data e 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. Trata-se de um conjunto de informações imprescindíveis às investigações.

Não se olvide que os integrantes das associações ou organizações criminosas cibernéticas atuam de modo pulverizado no âmbito interestadual e no exterior, o que também dificulta o trabalho da polícia na identificação dos envolvidos.

Nesse contexto, urge a necessidade da implementação de medidas que tornem mais ágil a disponibilização de dados e informações às autoridades policiais durante a investigação criminal, para tornar mais eficaz a repressão aos crimes digitais.

A atual conjuntura motivou o Governo Federal a adotar medidas mais duras para o combate do cibercrime. Sancionada em 28 de maio, a Lei 14.155/2021 alterou o Código Penal com aumento de pena para o crime de violação de dispositivo informático em até quatro anos de reclusão, com endurecimento da punição se houver prejuízo econômico. Para os crimes de furto qualificado mediante fraude e estelionato eletrônico, as penas passaram a ser de reclusão de até oito anos e multa, com punições mais rigorosas se o crime for realizado com uso de servidor localizado em outro país ou se a vítima for idosa ou vulnerável (BRASIL, 2021).

2.13. ATUAÇÃO PREVENTIVA ESPECIALIZADA DA POLÍCIA NO COMBATE AO CIBERCRIME

Segundo o ensinamento de Queiroz (2003, p. 20), a polícia preventiva especializada é atividade policial desenvolvida através do planejamento, técnicas de operações, compilação de dados e processamento das informações criminais, objetivando a prevenção de ilícitos penais.

Objetivando-se adotar ações para mitigar prejuízos econômicos e morais causados às vítimas (pessoas físicas e jurídicas) e dificultar as ações dos cibercriminosos, urge a necessidade da cooperação técnica de instituições financeiras e empresas de telefonia.

Na grande maioria dos golpes virtuais, seja associação ou organização criminosa, a criminalidade se utiliza de um ou mais correntistas para emprestar a conta bancária, visando a movimentação financeira do dinheiro auferido ilicitamente logo após o golpe, o que pode ocorrer através de transferência bancária a outro banco, saque ou até mesmo o pagamento de conta.

Por essas razões, uma medida que poderia reduzir o prejuízo financeiro das vítimas, seria o imediato bloqueio da conta bancária do correntista (golpista), a partir do registro de ocorrência subscrito pela autoridade policial, independentemente de autorização judicial. Essa cautela possibilitaria à vítima restabelecer a sua situação patrimonial e tornaria ineficaz a ação do criminoso.

Análises apontam que em muitos casos examinados a organização criminosa tem muita facilidade em cooptar correntistas, que em contrapartida recebem um percentual do recurso ilícito auferido. Outro aspecto a destacar é que geralmente a vítima não é ressarcida pelo banco.

Entendemos que o bloqueio do IMEI e da linha telefônica do dispositivo eletrônico utilizado pelo golpista a partir do registro de ocorrência subscrito pela autoridade policial, também é uma medida salutar a ser implementada, tal como ocorre nos bloqueios de furtos e roubos de telefones celulares pela polícia.

Para se ter uma ideia, o Centro de Inteligência Cibernética (CIC) identificou um caso onde o golpista utilizou mais de trinta linhas telefônicas em um único IMEI. Em outras palavras, o criminoso atuou

com o mesmo dispositivo móvel sem que houvesse a possibilidade de bloqueio do equipamento pela polícia, fazendo inúmeras vítimas.

Nessa perspectiva, o CIC vem promovendo avanços de caráter preventivo notadamente nos casos de leilões falsos, obtendo-se êxito em “derrubar” sites fraudulentos junto aos provedores de internet de modo a evitar novas vítimas e inibir a ação criminosa.

2.14. CONSIDERAÇÕES FINAIS

Com o impacto da tecnologia digital da informação e comunicação na vida das pessoas, houve um aumento significativo dos crimes praticados por meio virtual. Os vazamentos de dados de grandes proporções que acontecem no âmbito global, tendem a municiar a criminalidade digital a intensificar as suas ações, cujas consequências comprometem a segurança da informação dos usuários da internet.

Surge então a importante missão das Polícias Cíveis no tocante à repressão aos cibercriminosos. No estado de São Paulo, a DCCIBER vem atuando no combate aos crimes eletrônicos envolvendo organizações criminosas ou nas hipóteses onde há emprego de recurso de alta tecnologia.

A capacitação dos policiais cíveis sobre métodos de investigação digital é fundamental para o avanço no enfrentamento dessa criminalidade, em especial porque cabe à Polícia Civil as funções de policiamento preventivo especializado e a repressão criminal no ciberespaço.

Tendo em vista que os crimes digitais são voláteis com rápido desaparecimento das evidências, torna-se premente a implementação de medidas onde no curso do procedimento de Polícia Judiciária a autoridade policial obtenha a resposta da sua requisição solicitada à empresa de internet com maior celeridade, visando a eficácia da investigação criminal e a respectiva punição dos criminosos pela Justiça.

Entendemos que a adoção de medidas como os bloqueios da conta bancária do correntista fraudador, do IMEI e da linha telefônica do dispositivo móvel utilizado pelo golpista, a partir do boletim de ocorrência eletrônico subscrito pela autoridade policial, são medidas de caráter preventivo que irão mitigar prejuízos econômicos e morais às vítimas e também inibir as ações dos cibercriminosos.

Portanto, há muito o que se fazer e por essa razão a Polícia Civil necessita do apoio da sociedade civil e da cooperação das instituições