ACADEMIA MILITAR

As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos

Autor: Aspirante-Aluna Cavalaria da GNR Ana Marta de Sousa e Silva

Orientadora: Professora Doutora Sofia de Vasconcelos Casimiro

Coorientador: Tenente-coronel Infantaria da GNR Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, setembro de 2022

ACADEMIA MILITAR

As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos

Autor: Aspirante-Aluna Cavalaria da GNR Ana Marta de Sousa e Silva

Orientadora: Professora Doutora Sofia de Vasconcelos Casimiro

Coorientador: Tenente-coronel Infantaria da GNR Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, setembro de 2022

EPÍGRAFE

“O instinto de ganância está a tal ponto desenvolvido que estorva a ação do senso moral ou social, ou concomitantemente, o instinto moral ou social é a tal ponto atrofiado que não inibe o senso de ganância, há uma rutura de equilíbrio.”

Fernando Pessoa

DEDICATÓRIA

À minha família e, em particular aos meus pais.

AGRADECIMENTOS

O presente Relatório Científico Final do Trabalho de Investigação Aplicada simboliza o fim do Curso de Formação de Oficiais da Guarda Nacional Republicana, realizado na Academia Militar. Por esse motivo, representa o culminar de uma etapa, onde foram ultrapassadas diversas adversidades, em que o apoio de quem nos está mais próximo é fundamental.

À minha orientadora, Professora Doutora Sofia Casimiro, pelo apoio prestado, por todos os conhecimentos transmitidos e pelo tempo disponibilizado para me auxiliar na realização da presente investigação.

Ao Tenente-Coronel Tiago Lopes, o meu coorientador, por todos os conhecimentos transmitidos, pela presença permanente ao longo de toda a investigação, pelos conselhos e por me ter desafiado a fazer sempre melhor ao longo de todo o trabalho.

A todos os militares que transmitiram o seu conhecimento, demonstrando sempre espírito de camaradagem e disponibilidade para me auxiliar durante todo o processo de elaboração da investigação**.**

Aos meus pais, por todos o apoio, durante esta longa caminhada que foi a Academia Militar.

À minha tia, por todo o apoio ao longo destes cinco anos e a permanente disponibilidade em me auxiliar.

A todos os meus camaradas de curso: sem vocês nada teria sido igual e tão especial.

A todos vós, o meu mais sincero agradecimento!

RESUMO

As denúncias por práticas fraudulentas relacionadas com plataformas eletrónicas de pagamento, geralmente enquadráveis no crime de burla, têm vindo a aumentar, segundo as ocorrências participadas pelas forças de segurança ao Ministério Público, dotando de particular pertinência e atualidade a presente investigação.

A investigação foi dividida numa parte teórica e numa parte prática. Na parte teórica foi efetuada uma revisão de literatura, onde é explanada a tipologia dos crime resultante do uso indevido de plataformas eletrónicas de pagamento, a evolução dos crimes de burla, os tipos de métodos de pagamento *online* mais utilizados e o trabalho desenvolvido pela GNR tanto na área da prevenção como na repressão deste tipo de ilícitos. Na parte prática foi adotado um método dedutivo com uma abordagem quantitativa e qualitativa, sendo feita a análise de inquéritos por questionário e inquéritos por entrevistas.

Da análise efetuada, incluindo nesta também a documental, foi possível verificar que os crime relacionados com a utilização fraudulenta de plataformas eletrónicas de pagamento têm vindo a aumentar de forma significativa, sendo o número de denúncias cada vez maior. Esta nova realidade exige uma constante adaptação das forças de segurança, nomeadamente da GNR, na criação de ações de sensibilização e programas de prevenção criminal com desenvolvimento de capacidades e competências para combater este tipo de ilícitos.

A investigação desenvolvida permitiu perceber que a GNR já desenvolve trabalho na área da investigação criminal e prevenção dos ilícitos em causa, muito embora se verifique que existe ainda muito trabalho a desenvolver de forma a atenuar o fenómeno criminal com que nos deparamos. Assim, a continua investigação na área, o desenvolvimento de ações de esclarecimento e a constante formação dos militares serão ferramentas valiosas para atingir o objetivo último, o da segurança da população.

Palavras-chave: MB Way; Burla; Plataforma eletrónica de pagamento; Guarda Nacional Republicana; Investigação Criminal; Prevenção.

ABSTRACT

The number of reports of fraudulent practices related to electronic payment platforms, which generally fall under the crime of fraud, has been increasing, according to the occurrences reported by the security forces to the Public Prosecutor's Office, thus providing the present investigation with particular pertinence and timeliness.

The research was divided into a theoretical and a practical part. In the theoretical part a literature review was conducted, where the typology of the crimes resulting from the misuse of electronic payment platforms is explained, as well as the evolution of fraud crimes, the types of *online* payment methods that exist and the work developed by the GNR both in the area of prevention and in the fight against this type of crime. In the practical part a deductive method with a qualitative and quantitative approach was adopted, with the analysis of questionnaires by interview and questionnaires by survey.

After document analysis and consequent analysis of statistical data, it was possible to verify that crimes related to the fraudulent use of electronic payment platforms have been increasing significantly, and the number of complaints is growing. This new reality requires a constant adaptation of the security forces, namely the GNR, in the creation of awareness-raising actions and special programs and development of capabilities and skills to combat this type of illicit activity.

The research developed allowed us to realize that the GNR already develops work in criminal investigation and prevention of these crimes, but there is work to be done to mitigate the criminal phenomenon we face. Thus, the continued investigation in the area, the development of clarification actions, and the constant training of the military will be valuable tools to achieve the goal, the safety of the population.

Keywords: MB Way; Fraud; Electronic payment platform; Guarda Nacional Republicana; Criminal Investigation; Prevention.

ÍNDICE GERAL

ÍNDICIE DE FIGURAS

ÍNDICE DE QUADROS

ÍNDICE DE TABELAS

LISTA DE APÊNDICES

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

ATM- *Automated Teller Machine*

CTT- Correios de Portugal

CVC- *Card Verification Code*

DIC- Direção de Investigação Criminal

E- Entrevistado

GNR- Guarda Nacional Republicana

IMEI- *International Mobile Equipment Identify*

LOIC- Lei de Organização da Investigação Criminal

NIC- Núcleo de Investigação Criminal

OE- Objetivo Específico

OG- Objetivo Geral

OPC- Órgão de Polícia Criminal

PJ- Polícia Judiciária

PSP- Polícia de Segurança Pública

QC- Questão Central

QD- Questão Derivada

QI- Questão Inquérito

NUIPC- Número Único de Identificação de Processo Crime

RASI- Relatório Anual de Segurança Interna

SIBS- Sociedade Interbancária de Serviços, SA

SIIC- Secção de Informações e Investigação Criminal

TIA- Trabalho de Investigação Aplicada

INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada, é enquadrado na estrutura curricular do mestrado integrado em Ciências Militares na Especialidade de Segurança da Guarda Nacional Republicana (GNR) da Academia Militar. A presente investigação tem como intuito a aplicação dos conhecimentos adquiridos ao longo de toda a formação na Academia Militar, a fim de adquirir o grau académico mestre.

O tema da presente investigação é: "As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos".

O objetivo geral (OG) da investigação é perceber de que forma a GNR se encontra capacitada para investigar e prevenir os ilícitos relacionados com as burlas com recurso a plataformas eletrónicas de pagamento. Assim defino seis objetivos específicos (OE): (OE1) perceber se a sensibilização e prevenção dos crimes em estudo é do conhecimento dos militares e suficiente para a população estar alerta para este tema; (OE2) estudar os *modus operandi* que os agentes criminosos utilizam para a concretização do crime; (OE3) entender os novos métodos utilizados para a realização dos ilícitos; (OE4) explanar os procedimentos realizados pelos militares da GNR, quando se deparam com um inquérito relacionado com os ilícitos de burla com recurso a plataformas eletrónicas de pagamento; (OE5) entender as controvérsias que o enquadramento legal do crime origina no processo de investigação e (OE6) entender de que forma é feita a cooperação entre todas as entidades participantes no processo de investigação deste tipo de ilícitos.

A realização desta investigação insere-se na fase de conclusão do Curso de Formação de Oficiais e tem como objetivo contribuir para o estudo de matérias de interesse para a GNR. A investigação incide sobre o novo *modus operandi* na prática do crime de burla, associado ao uso de plataformas eletrónicas de pagamento, nomeadamente da plataforma MB Way, a mais usada em Portugal (SIBS, 2020), pretendendo perceber as capacidades e as competências da GNR na investigação e prevenção deste tipo de ilícitos.

Para o enquadramento da investigação é necessário perceber o seu âmbito jurídico, através do enquadramento legal dos atos ilícitos[1] em causa (Nota Prática nº 20/2020), bem como pela apresentação dos diplomas e conceitos que tratam de assuntos sobre a cibercriminalidade em Portugal. O diploma em destaque no enquadramento do tema à luz do Direito Internacional é a Convenção sobre o Cibercrime, também referida como Convenção de Budapeste, negociada no seio do Conselho da Europa em 2001. A Convenção sobre o Cibercrime "é o documento mais completo sobre o assunto e reconhecida como um importante instrumento na luta contra o cibercrime" (Vidigal, 2012, p. 30). No plano nacional, destaca-se o Código Penal e a Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro.

Os atos ilícitos em estudo, apesar de poderem revestir especificidades que os permitem enquadrar em tipos legais de crime diversos, têm sempre como principal modo de realização o engano do lesado. "A olhar a mentira dos salões, esquecemos a verdade das celas" (Torga, 2011). O agente criminoso utiliza o "conto do vigário" para se apropriar de algo que não é seu. É, por isso, importante estudar a evolução destes acontecimentos ao longo da história, o que permitirá perceber as técnicas utilizadas pelos agentes criminosos, assim permitindo retirar conclusões sobre o que será ainda possível fazer por parte dos órgãos de polícia criminal (OPC) na prevenção e combate a este tipo de ilícitos.

A análise dos Relatórios Anuais de Segurança Interna tem uma importância fundamental na análise de dados. Estes relatórios são lançados anualmente e servem para explanar o trabalho desenvolvido pelas entidades de segurança interna competentes em Portugal, quer no número de ilícitos participados, quer nas ações de combate e prevenção criminal (RASI 2020). A comparação dos dados expostos nestes relatórios ao longo dos anos permite a análise deste tipo de criminalidade em Portugal e as tendências observadas nas matérias em estudo.

Após esta análise, a investigação é complementada com o estudo da evolução da legislação em Portugal relevante para o tema. Os meios tecnológicos tiveram um papel revolucionador na forma como os consumidores fazem as suas compras (SIBS, 2020). Apesar de as plataformas eletrónicas de compra e venda de produtos e serviços (componentes essenciais do comércio eletrónico ou, na expressão mais habitual, embora

[1] Crime de Burla, artigo 217º Código Penal; Crime de Burla Qualificada, artigo 218º Código Penal; Crime de Burla Informática e nas Comunicações, artigo 221º Código Penal; Crime de Falsidade Informática, artigo 3º Lei do Cibercrime; Crime de Acesso Ilegítimo, artigo 6º Lei do Cibercrime.

anglo-saxónica, *e-commerce*) já existirem desde 1994 (Abdalla, 2017), a sua expressividade aumentou devido à pandemia Covid 19, que fez ampliar este tipo de comércio (Oliveira, 2020). Como consequência do aparecimento do e-commerce, surgiram também as plataformas eletrónicas que permitem a realização dos pagamentos pelo mesmo meio, que consistem nas plataformas eletrónicas de pagamento (Abdalla, 2017), sendo que atualmente em Portugal a que merece mais destaque é a plataforma da SIBS designada MB Way, que é a mais utilizada e através da qual é também realizado o maior número de ilícitos (GNR, 2022).

Após uma análise estruturada da vertente teórica do tema, importa perceber como estes ilícitos são encarados na prática e a forma como é feita a prevenção e o combate a este tipo de crimes. De início, é feito o estudo das quatro formas típicas de atuação, identificadas pelo Ministério Público, no SIATID (2021): cedência dos dados do cartão da vítima; a cedência dos dados do cartão da vítima e dos respetivos códigos de levantamento; método de *smishing* e método de *phishing* sendo que estes últimos métodos poderão reconduzir a vítima para um sítio eletrónico falso (por exemplo, para uma falsa plataforma OLX, sendo esta plataforma a mais utilizada na prática destes atos).

Após identificadas as formas de atuação dos agentes criminosos é importante perceber a forma de atuação da GNR no combate e prevenção a este tipo de fenómenos. Na área do combate, o trabalho da GNR inicia-se pelo recebimento da participação por parte do lesado, bem como pelo respeito de todos os prossupostos necessários para adquirir os dados relevantes para a realização da investigação. Neste âmbito, foi feita uma uniformização de procedimentos (DIC, 2020), para que todo o dispositivo dê resposta ao ilícito da forma mais correta e completa possível. Seguidamente, o prosseguimento do trabalho realizado pela GNR depende diretamente do Ministério Público, pois só após a atribuição do inquérito a este OPC é que a GNR poderá realizar e concluir o seu trabalho de investigação.

No momento da investigação, os militares da GNR deparam-se com a problemática da prova digital. Como previsto no Código de Processo Penal, todos os princípios existentes para a obtenção de prova física, têm também de ser cumpridos para a obtenção da prova digital. No entanto as suas características tornam o trabalho com este tipo de prova mais desafiante. Segundo Pires (2013), a prova digital tem um caráter volátil, forjável e frágil. Todas estas características implicam um trabalho célere especializado por parte dos militares, para que a investigação tenha sucesso.

Na área da prevenção são realizadas ações de sensibilização ao tema nas redes sociais, nos órgãos de comunicação social e através dos programas especiais de policiamento de proximidade, onde a informação é levada a todos os cidadãos que se encontram mais isolados ou que tenham sido identificados como um alvo mais frágil e por isso mais provável para ser abordado pelos agentes criminosos (GNR, 2022).

O Ministério Público tem um papel fundamental no decorrer dos inquéritos, sendo a entidade responsável pela investigação e aquela que decide a respetiva atribuição aos Órgãos de Polícia Criminal. Para isso, desenvolveu um conjunto de recomendações e instruções que permitem a todos os profissionais trabalharem em concordância, proporcionando assim vantagens para a concretização do objetivo último: a aplicação da justiça.

As informações recolhidas através de uma análise documental, de diplomas legais, artigos científicos, conferências, trabalhos de investigação, notícias, notas práticas, instruções e recomendações de órgãos especializados e diplomas internos da GNR serão complementadas por inquéritos por entrevista e inquéritos por questionário realizados a militares da GNR com experiência na matéria. De todas as informações recolhidas, será feita a análise dos inquéritos por entrevista e por questionário e serão analisados e discutidos os dados obtidos na presente investigação.

No fim, serão realizadas as conclusões sobre a investigação realizada, bem como a análise das dificuldades e limitações encontradas ao longo da mesma. Durante este processo, serão mencionadas recomendações, bem como a sugestões para investigações futuras.

PARTE I- ENQUADRAMENTO TEÓRICO E CONCEPTUAL

CAPÍTULO 1
ENQUADRAMENTO JURÍDICO

1.1 Evolução da Convenção de Budapeste

A necessidade de harmonização internacional, referente à cibercriminalidade e à prova eletrónica, originou a Convenção da Budapeste, sobre o Cibercrime. A Convenção foi celebrada em 2001, consistente num instrumento jurídico completo e abrangente, com toda a informação necessária para a criação de legislação nacional e internacional sobre a temática da cibercriminalidade e cooperação internacional entre os Estados membros da Convenção (Vidigal, 2012).

A cerimónia de abertura da assinatura da Convenção foi realizada a 23 de novembro de 2001 em Budapeste, tendo conduzido à sua assinatura por 30 países, 4 deles não membros do Conselho da Europa, embora tenham feito parte das suas negociações (Canadá, Estados Unidos da América, Japão e África do Sul). Nos oito anos seguintes, a Convenção foi assinada por 46 países e ratificada por 25. Houve também países que procederam à elaboração de legislação nacional consentânea com esta Convenção, mesmo não a tendo assinado, sendo isto sinal de "harmonização e uma estandardização do processo" (Vidigal, 2012, p. 30). Em 2019 já existiam 71 Estados a participarem como membros da Convenção, sendo que 64 faziam parte da mesma, 3 novos Estados assinaram a mesma em 2019 e 5 outros Estados foram convidados a aderir.

A integridade e a confidencialidade da rede e dados informáticos estão sujeitos a constantes ataques, sendo necessário estabelecer objetivos para a prevenção deste fenómeno. É necessário incutir comportamentos de prevenção para a utilização fraudulenta dos sistemas, redes e dados informáticos, possibilitando assim o desenvolvimento de técnicas de investigação criminal nacionais e internacionais, promovendo a cooperação entre diversos órgãos de polícia criminal (OPC) nacionais e estrangeiros. Todos estes princípios foram abordados em 2001 na elaboração da Convenção Sobre o Cibercrime.

O diploma da Convenção é composto por 48 artigos, divididos em 4 capítulos. O primeiro capítulo é composto por um só artigo, onde se encontram as definições de vários conceitos, nomeadamente: sistema informático, dados informáticos, prestador de serviços e dados de tráfego. No segundo capítulo são estabelecidas as medidas a adotar a nível nacional. Nos artigos segundo ao décimo primeiro são enumeradas as infrações que deverão ser punidas pela lei criminal nacional. As infrações têm em comum a falta de especificação da sanção que deverá ser aplicada. Na Convenção apenas é referido que cada Estado adotará a nível interno as medidas que considerar necessárias para estabelecer a infração penal deste tipo de crime (Vidigal, 2012). Ao longo do segundo e terceiro capítulos, são explicadas as competências das partes e os cenários de atuação, sendo nestes capítulos explicada a cooperação internacional a implementar, salientado o auxílio mútuo em diversos aspetos, entre o Estados membros da Convenção. No último artigo do capítulo III da Convenção do Cibercrime é abordada a Rede 24/7, sendo estabelecido que cada parte deverá ter disponibilidade permanente, para que seja possível prestar auxílio de forma imediata, "nas investigações e nos procedimentos relativos a infrações penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma eletrónica, da prática de infrações penais" (Convenção sobre o Cibercrime, 2009). O último capítulo aborda as disposições finais sobre a convenção, estabelecendo princípios de adesão à Convenção, a aplicação territorial, os efeitos da Convenção e a consulta entres as partes, entre outros aspetos. Para complementar esta Convenção foi criado um protocolo adicional, onde são implementadas medidas contra atos de natureza racista e xenófoba com recurso a meios informáticos.

Aderir à Convenção traduz-se em vantagens evidentes para os Estados membros da mesma, uma vez que esta pode ser usada como padrão no que ao tema da cibercriminalidade diz respeito, harmonizando assim as legislações nacionais, poderá ser utilizada como guia para legislar internamente. A adesão à Convenção em si traduz-se em mais-valias para os países que o fazem. A cooperação internacional desenvolvida através de um quadro jurídico comum na área da cibercriminalidade e prova digital são uma grande vantagem, permitindo que todos os membros se encontrem em permanente cooperação e consonância de forma a dar uma mais rápida e eficaz resposta aos desafios com que se deparam, assegurando uma cooperação fiável e eficiente (Conselho Europeu [CE], 2019). Através da adesão à Convenção, os países também passam a ser membros do Comité da Convenção sobre o Cibercrime, que é atualmente o órgão intergovernamental responsável por toda a matéria relacionada com a cibercriminalidade.

São desenvolvidas Notas de Orientação nesta matéria, tendo em conta a partilha de experiências e informações que fazem a avaliação da aplicabilidade das normas já instauradas, permitindo desta forma uma constante atualização das políticas em vigor.

Apesar de as vantagens que a Convenção proporcionou no combate à cibercriminalidade serem evidentes, esta também é alvo de algumas críticas. A classificação dos tipos de crimes feita ao longo da Convenção é bastante ampla. No entanto, ainda apresenta algumas lacunas, não fazendo menção a crimes como a lavagem de dinheiro e roubo de identidade. Este facto é defendido por Alkaabi, Mohay, McCullagh e Chantler (2010). A abrangência internacional da Convenção acaba por gerar algumas dúvidas quanto aos critérios de determinação da lei aplicável, sendo dada maior relevância ao critério do território e menor ao da nacionalidade do infrator (Brenner, 2006). Isto é, o local onde foi praticado o crime é o que tem mais relevância para determinar a lei aplicável. No entanto, levantam-se questões nesta temática, uma vez que o que é punido em determinado país pode não ser punido no país de origem do infrator, fazendo assim com que seja necessário o diálogo entre as partes envolvidas nesta situação, de forma que um acordo seja estabelecido. A cooperação internacional em permanência também é necessária nesta situação. São também tecidas várias críticas neste campo, uma vez que o trabalho desenvolvido nesta matéria pelos Estados depende em muito de terceiros.

1.2 Enquadramento dos ilícitos penais cometidos através de plataformas eletrónicas de pagamento

A Convenção de Budapeste fez a introdução na legislação de vários tipos penais no que diz respeito ao tema da cibercriminalidade. Fazendo uma análise mais específica de acordo com o tema abordado na presente investigação, o foco recai sobre as burlas relacionadas com o uso de plataformas eletrónicas de pagamento. As práticas criminosas são diferenciadas de acordo com o *modus operandi* utilizado pelos agentes autores dos crimes. Apesar de a intenção de quem pratica este tipo de ilícito ser sempre a mesma - obter proveito próprio de forma ilegal - a forma de atuação leva a que o enquadramento jurídico aplicado aos factos seja variável.

Desta forma, e nunca podendo excluir qualquer outro tipo de enquadramento legal, por se relacionar com práticas tão abrangentes, devem ser considerados o crime de burla, previsto no artigo 217.º do Código Penal; o crime de burla qualificada, previsto no artigo 218.º do Código Penal; o crime de burla informática, previsto no artigo 221.º do Código

Penal; o crime de falsidade informática, previsto no artigo 3.º da Lei do Cibercrime; e o crime de acesso ilegítimo, previsto no artigo 6.º da Lei do Cibercrime.

A relevância de outras burlas não pode ser descurada, uma vez que, o processo em causa faz com que a vítima seja levada ao engano, desta forma, o burlão obtém proveito próprio através de dinheiro ou outro qualquer benefício ou vantagem patrimonial.

1.2.1 Crime de Burla- Artigo 217.º Código Penal

O procedimento utilizado para a realização de burlas com recurso a plataformas eletrónicas de pagamento é um processo enganador que origina um injusto ganho económico do agente criminoso. Este leva o lesado a dar acesso pleno à sua conta bancário ou que seja iludido, de forma a ser o mesmo a pagar por um serviço que por si será prestado. É necessária a análise do caso concreto em investigação, para que a tipificação do crime seja feita da forma mais correta. No entanto, este tipo de procedimento pode vir a traduzir-se no crime de burla, previsto no artigo 217.º do Código Penal. Contudo, muitas vezes as vítimas destes ilícitos apercebem-se a tempo do sucedido, o que impede que o crime seja consumado, verificando-se apenas uma tentativa. A tentativa também é punível nos termos do Código Penal, artigo 22.º e artigo 217.º, n.º 1 e 2. Todavia, o procedimento penal depende de queixa, por se tratar de um crime semipúblico, de acordo com o artigo 217.º, n.º 3, também do Código Penal.

Apesar de o procedimento criminal não ser iniciado no caso de não ser apresentada uma queixa-crime, a informação apurada através da notícia do ocorrido não deverá ser descurada, servindo para que a investigação seja encaminhada de forma a apurar se o agente criminoso daquele ilícito terá praticado outros. Assim, a atuação será enquadrada no crime de burla qualificada, para o qual o procedimento criminal não depende de queixa.

1.2.2 Crime de Burla Qualificada- Artigo 218.º Código Penal

Os critérios para a qualificação da burla são diversos. Um dos critérios respeita à adoção da burla como modo de vida, nos casos em que uma mesma pessoa ou grupo de pessoas pratica várias vezes os atos suscetíveis de qualificação como crime de burla. Muitas vezes, em situações em que as vítimas nem sequer têm conhecimento umas das outras, é verificado pelas autoridades policiais que indivíduos ou grupos de indivíduos se organizam de forma a concretizar estes crimes sistematicamente. Assim, os indivíduos

que cometem as irregularidades auferem rendimentos que lhes permitem fazer desta atividade um modo de vida, possibilitando o enquadramento na burla qualificada, de acordo com o artigo 218.º, n.º 2, b) do Código Penal.

De acordo com outro critério, os danos causados por este crime podem ser considerados de valor elevado ou consideravelmente elevado. Muitas das vezes estes valores não são obtidos através de uma só ação criminosa, sendo necessário observar vários atos que levam a que os proveitos obtidos cheguem a uma quantia tão elevada. No entanto, através do processo de investigação e o correlacionar de factos, é possível chegar a valores de tal forma significativos que o crime é qualificado como burla qualificada, através do artigo 218.º, n.º 1 ("valor elevado") e n.º 2, a) ("valor consideravelmente elevado") do Código Penal.

Como outros critérios para o enquadramento do ilícito como burla qualificada, é importante ressalvar não só o aproveitamento de especial vulnerabilidade da vítima, tendo em conta a idade, condição de doença ou deficiência, como também a especial dificuldade económica originada pelo prejuízo causado pela burla. Nestes casos o crime tem a forma qualificada, de acordo com o artigo 218.º, n.º 2, alíneas c) e d) do Código Penal.

1.2.3 Crime de Burla Informática e nas comunicações- Artigo 221.º Código Penal

No estudo do crime de burla com recurso a plataformas eletrónicas de pagamento, também deve ser considerada a burla informática e nas comunicações. Neste ilícito, cada caso é um caso, bem como a sua tipificação, estando por isso dependente de uma análise isolada, de forma concreta. Nesta situação, está em causa a violação da estrutura de programa informático, a utilização incorreta ou incompleta de dados e a utilização ou processamento sem autorização de dados, como previsto no artigo 221.º, n.º 1 do Código Penal.

A utilização da plataforma MB Way, de forma indevida, recorre à manipulação de dados informáticos, podendo assim o ilícito ser tipificado, de acordo com o explanado.

1.2.4 Crime de Falsidade informática- Artigo 3.º Lei do Cibercrime

Para a presente investigação é relevante o estudo do crime de falsidade informática. Este consiste na introdução, modificação, eliminação ou supressão de dados ou qualquer outra forma que interfira com o seu tratamento, do qual é exemplo, o intuito de enganar, conforme se encontra previsto no artigo 3.º, n.º 1 da Lei do Cibercrime. De

todos os crimes em estudo, este pode ser considerado como o que tem a pena punitiva mais gravosa a ser aplicada. No início do processo de investigação, o local da sua prática poderá ser considerado determinante para que seja estabelecido o lugar onde será feita a atribuição de investigação do processo. A prática de vários crimes poderá ser feita em várias comarcas, pelo que a atribuição do processo deverá ser feita à comarca onde se verifique o ilícito com a pena mais gravosa, tal como está previsto no artigo 28.º, a) do Código de Processo Penal.

No processo de burla com recurso a plataformas eletrónica de pagamento, mais concretamente a plataforma MbWay, este tipo de ilícito é consumado através da emissão de ordens bancárias, com recurso às credenciais dos lesados, obtido através da criação de um *site* falso, onde os dados da vítima são extraídos e utilizados posteriormente. Após ter sito feito o acesso ao sistema bancário das vítimas, estes processos podem ser traduzidos em levantamentos, pagamentos ou transferências.

1.2.5 Crime de Acesso Ilegítimo- Artigo 6.º Lei do Cibercrime

O crime de acesso ilegítimo encontra-se explanado no artigo 6.º da Lei do Cibercrime, e traduz-se no acesso sem autorização ou conhecimento do lesado para tal, num sistema informático que não lhe pertence. As ações relacionadas com a produção, venda, distribuição ou disseminação em um ou mais dispositivos informáticos de programas, códigos ou dados informáticos que produzam ações que não foram previamente autorizados pelos titulares dos sistemas informáticos.

No caso específico do crime de burla com recurso a plataformas eletrónicas de pagamento, o agente criminoso pode, através da plataforma MB Way, aceder a informações, como o saldo bancários ou os movimentos realizados pelo titular da conta. Um sistema multibando é intitulado como um sistema informático, segundo o artigo 2.º, a) da Lei do Cibercrime, consequência disto, o acesso a uma conta bancária através do multibando, feito de forma ilegítima, pode ser tipificado como crime de acesso ilegítimo, tendo em conta todas as circunstâncias do ato, que não poderão ser descuradas durante todo o processo de investigação. Durante toda a ação do uso indevido da plataforma MB Way, é utilizado, de forma imprópria, o código de acesso à mesma, ferramenta de segurança usada pela aplicação em causa, ação que mais uma vez se enquadra na descrição do crime de acesso ilegítimo.

1.3 Evolução da Burla (Conto do vigário por via digital)

Os crimes de burla têm como base, o levar ao engano outro, para que seja obtido um proveito próprio, pelo que, ao longo dos tempos estes fenómenos têm vindo a adaptar-se à realidade em que são praticados, sempre guiados por princípios desonestos assentes na ganância e no desejo de poder. O primeiro relato relacionado com este tipo de ilícitos, foi descrito 300 anos antes de Cristo, um comerciante grego realizou uma apólice de seguros que seria paga, com juros, após a venda da mercadoria que iria transportar na sua embarcação. O plano do comerciante consistiu em vender a mercadoria à revelia da seguradora e afundar a embarcação posteriormente, desta forma, este iria reclamar à seguradora tanto a carga, supostamente destruída, como o barco afundado, ficando com lucro inteiramente para ele. Este é o primeiro grande evento relatado na história que pode ser tipificado, de acordo com os crimes em estudo na presente investigação (Beattie, 2021).

Estima-se que no ano de 1617 tenha sido escrito e publicado um livro de contos sobre fraudes financeiras, pelo autor chinês Zhang Yingyu, intitulado "*A New Book for Foilinf Swindles, Based on Wordly Expirience*". O livro faz a compilação de vários contos, que relatam vários crimes de fraudes e burlas, demonstrando vários exemplos destes tipo de ilícitos, no final de cada conto é feito um pensamento crítico, em maior parte destes pensamentos são elogiadas as capacidades intelectuais e engenhosas dos vigaristas, que praticam os ilícitos e criticada a falta de capacidade das vítimas para a perceção do que lhes está a acontecer, sendo culpabilizadas por tal facto, nos outros casos o autor faz uma reflexão moral sobre os factos relatados, demonstrando a ilicitude dos atos praticados. Este livro foi escrito durante o período da Dinastia *Ming*, no qual a China se envolve num comércio mundial de bens, todo este processo originou grande movimento económico no país e proporcionou o aparecimento de esquemas fraudulentos, a obra na sua primeira edição, tem como objetivo ser um guia para evitar ser alvo destes acontecimentos, no entanto acaba em alguns casos, por ser usada como guia para o desenvolvimento dos ilícitos.

O século XIX ficou marcado por vários esquemas de grande dimensão, e apesar de nos dias que correm ser usual o aviso para este tipo de fenómenos, durante os anos de 1800 os esquemas eram tão elaborados e tão pouco publicitados, que nos Estados Unidos a Ponte de Brooklyn chegou a ser vendida várias vezes. Os meios de comunicação não

tinham a abrangência que têm hoje, no entanto os meios de transporte já podiam ser usados com uma facilidade relativa devido ao desenvolvimento das linha ferroviárias, o que proporcionava a prática de burlas e fraudes em grande número, em sítios não muito distantes. Os indivíduos que praticavam as atividades ilícitas, faziam-no como modo de vida e apenas eram descobertos através dos testemunhos valiosos das suas vítimas, que acabavam por descrever o individuo e os métodos utilizados com exatidão.

É já no século XX que os "*Ponzi Schemes*" se tornam famosos, recebem este nome devido a um dos seus autores, Charles Ponzi, consistiam em levar indivíduos a efetuar investimentos, com a promessa de um retorno elevado, no entanto este nunca era obtido na realidade, funcionando como um esquema em cadeia em que apenas era possível dar lucro a uns, após novas pessoas serem levadas ao engano. Apesar dos autores e dos métodos irem variando, o erro que as vítimas cometem acaba por ser sempre o mesmo, confiar dinheiro próprio num investimento em que não existem garantias de ser seguro.

A evolução deste tipo de ilícitos é evidente, as estratégias utilizadas pelos agentes criminosos vão variando e adaptando-se à realidade da sociedade em que se encontram, sinal disso é a tendência crescente dos crimes de burlas informática, falsidade informática e acesso ilegítimo como é possível observar nos RASI dos últimos anos. É possível perceber que o trabalho desenvolvido na área da prevenção, ainda não é suficiente, encontrando-se os crimes de burla entre os que são mais participados em Portugal.

1.4 Evolução dos crimes de burla em Portugal de acordo com os RASI (2014-2021)

Os Relatórios Anuais de Segurança Interna (RASI), nomeadamente os realizados desde o ano de 2010, através da análise dos seus dados, permitindo compreender, os crimes de burla praticados em Portugal. É no ano de 2010 que o uso de plataformas eletrónicas para a concretização de burlas começa a ser considerada uma ameaça relevante, devido à imaterialidade associada a este fenómeno, ou seja, algo que só é observável após ser consumado crime. Nesta altura, já tinha um potencial de crescimento que merecia ser tido em conta, tendo este fenómeno sido considerado como uma das principais ameaças à segurança interna em 2010. O programa especial "Apoio 65- Idosos em Segurança" em 2011 inicia a prevenção para os diversos crimes de burla, sensibilizando os idosos para esta temática, para que os mesmo não sejam levados ao engano.

A evolução dos crimes de burla é tão evidente, que o seu estudo nos RASI é feita de uma forma cada vez mais elaborada, São diversos os fatores que o justificam, e é a

partir do ano de 2012 que os crimes de burlas são os mais participados no Sistema de Queixa Eletrónico. Também nesse ano, é realizado em paralelo com o programa especial anteriormente abordado, o programa especial "Gerações de Mãos Dadas", com o intuito de mais uma vez alertar os idosos para as práticas fraudulentas associadas a este tipo de crimes. No ano de 2013 é observada a tendência do ano anterior, mas é no ano de 2014, que surgem dados mais relevantes para a presente investigação, sendo associados aos ilícitos praticados os crimes de falsidade informática e de acesso ilegítimo, passando estes agora a terem também um papel de destaque nos estudos realizados nos RASI.

Deste então, que a presença dos ilícitos apresentados anteriormente são uma constante, ganhando cada vez mais um papel de destaque. São ainda sistematicamente considerados como ameaças para a segurança interna, para a qual a intervenção é necessária, de modo a controlar a tendência de crescimento. Fazendo uma análise dos dados, através de gráficos realizados com dados fornecidos pelos RASI, é possível perceber que o número de ilícitos participados do crime de burla informática e nas comunicações, atingiu o seu pico no ano de 2019, com um aumento de 66,7%, os crimes de "outras burlas" atingiram o seu máximo no ano de 2017, com um aumento de 47,9%, já os crimes de acesso ilegítimo e falsidade informática, registaram máximos no ano de 2019, com aumentos de 56,2 e 57,3% respetivamente. No que respeita ao número de arguidos, referente ao crime de burla informática e burla nas comunicações, registou-se o seu número máximo em 2014, com 372 arguidos constituídos, o crime de acesso ilegítimo, registou o maior número de arguidos em 2015, com 54 arguidos, o crime de falsidade informática registou o maior número de arguidos constituídos no ano de 2019, com 29 arguidos, todos os dados referidos anteriormente estão ilustrados nos gráficos presentes nos Apêndices N e O.

1.5 Acompanhamento legislativo da evolução da sociedade tecnológica

Figueiredo Dias, fez uma reflexão sobre a evolução do Código de Processo Penal, dizendo, "quem presidiu à Comissão elaboradora do novo Código, é levado a ver neste uma unidade coerente e concludente; enquanto, com o rosto crítico do universitário comprometido com as coisas do processo penal, não pode deixar de problematizar, e às vezes mesmo pôr em dúvida as soluções do novo direito" (1999, p.4).

O uso da informática é a realidade cada vez mais observável na sociedade atual, seja qual for a área que estiver a ser abordada ou trabalhada. A implementação desta realizada virtual proporcionou o aparecimento de práticas ilícitas com recurso a meios

informáticos, abrangendo vários tipos criminais e diversas áreas onde os agentes criminosos atuam. A evolução destas práticas criminosas, originou a necessidade de as mesmas serem tipificadas e as suas características serem explanadas, para que estas venham a ser punidas por lei (Ribeiro 2015).

Passados 23 anos da afirmação feita por Figueiredo Dias, ainda hoje se verifica que a tipificação dos crimes se encontra em permanente evolução assim como a legislação existente em Portugal. Para fazer face à evolução da criminalidade informática, foram criadas normas que complementam a Lei do Cibercrime. Faria Costa (1998), considera que se todo o serviço que internet fosse suspenso a nível mundial, mesmo que apenas por horas, a confusão que se iria instalar seria caótica. Esta realidade tem tanta importância, que as áreas Penal e Processual Penal não poderão ficar atrás no acompanhamento da evolução da mesma.

O legislador desenvolveu instrumentos jurídicos que acompanham a evolução da sociedade informatizada. Segundo Sieber (1992), este processo de evolução é dividido em quatro fases sendo elas: proteção da vida privada (sendo a manutenção da proteção dos dados pessoais o principal foco); a preocupação com os ilícitos de caracter económicos realizados com recurso à internet; elaboração de diplomas legislativos que regulem a justiça na área da criminalidade informática; e reformas legislativas que acompanhem a contante evolução da criminalidade informática.

A criminalidade informática tem uma abrangência mundial e não conhece fronteiras (Pires, 2013), por este mesmo motivo a legislação criada a nível europeu foi adotada também em Portugal, exemplo disso é a Convenção sobre o Cibercrime e a Lei do Cibercrime que se mantém atualizadas segundo as normas europeias e que servem como doutrina legislativa para a aplicação da lei no nosso país.

CAPÍTULO 2
MÉTODOS DE PAGAMENTO *ONLINE*

2.1 Evolução dos métodos de pagamento

A existência de uma nova realidade leva à criação de novas ferramentas na área bancária e no comércio tendo como objetivo facilitar qualquer tipo de questão relacionada com transações monetárias (Abdalla, 2017). O aparecimento do comércio *online* proporcionou também uma necessidade de adaptação eletrónica no que aos pagamentos diz respeito, foi então necessário criar formas de pagamento *online*, de maneira a proporcionar uma experiência rápida e vantajosa para quem usava este tipo de serviços, realidade que ainda hoje se verifica e que se encontra em constante adaptação à evolução da sociedade (Ureche & Plamondom, 2000).

Apesar da realidade dos métodos de pagamento *online* não ser estranha nos dias que correm, nem sempre os métodos de pagamento conhecidos faziam o recurso à internet, existiu uma evolução e adaptação ao longo dos tempos, principalmente na temática das transações entre partes, onde é necessário a troca de quantias por vezes de elevado valor. Até meados da década de 40, as trocas monetárias e os pagamentos eram feitos em dinheiro vivo, o que implicava uma grande logística, por vezes bastante insegura, pois o transporte destas quantias tinha de ser feita ponto a ponto (Abdalla, 2017).

Mais tarde, surgiram os cheques, medida implementada pela primeira vez nos Estados Unidos pela empresa Mastercard, o que proporcionou uma vantagem na segurança e na rapidez, as quantias eram transferidas ou levantadas em instituições bancárias, este método também poderia ser utilizado em retalhistas como forma de pagamento (Mastercard,2022). Em 1953, surgem os primeiros cartões bancários, também oriundos da plataforma Mastarcard, e mais tarde surge a empresa americana VISA, que faz a implementação dos cartões de débito no mundo bancário (Visa, 2022). Em Portugal, esta realidade foi introduzida nos anos 50, todo o processo foi possível devido à associação de um banco nacional, Banco Pinto & Sotto Mayor, a um banco americano, Bank of American, que já trabalhava que estas funcionalidades. Apesar de todo o sistema de cartão bancário estar introduzido na realidade nacional, apenas em 1974 é que o mesmo foi legislado, tendo sido estabelecido que todos os processos relacionados com estas matérias ficariam obrigadas a supervisão do Estado (Nepri, 2014). No entanto, a grande evolução no nosso país surge com o aparecimento do Multibanco, em 1985, apesar de

termos sido dos últimos países da Europa Ocidental a implementar um serviço deste género, foi através da observação e aprendizagem do que já tinha sido feito noutros países, que conseguimos desenvolver o sistema Multibanco mais eficaz e com mais funcionalidades em comparação aos existentes. A implementação deste serviço permitiu agilizar a vida de quem o utiliza, sendo possível fazer qualquer tipo de pagamento ou transação através do mesmo (SIBS, 2019).

Para Abdalla (2017), a evolução de uma sociedade digital, originou o aparecimento dos métodos de pagamento com recurso à internet, em 1994 são efetuadas as primeiras compras *online* e o grande passo nesta matéria é dado em 1995 com o lançamento da Amazon, o primeiro grande *site* de compra de produtos *online*. A evolução destes métodos de pagamento foi uma realidade expectável e em 1998 é criada uma plataforma de pagamentos *online*, PayPal. É a partir do ano 2000 que os bancos começam também a desenvolver os seus serviços *online*, permitindo aos seus clientes a realização de tarefas administrativas e transações monetárias desde que tivessem acesso à internet. A informatização da sociedade é cada vez mais uma realidade, em 2007 a Apple lança em nome próprio uma plataforma de pagamentos *online* a Apple Pay, em resposta a Google lança plataformas semelhantes, tornando a oferta deste tipo de serviços variada e abrangente (SIBS, 2019).

Portugal não foi exceção à regra mundial e também se adaptou a uma sociedade digital, criando plataformas eletrónicas de pagamento, com destaque para a plataforma MB Way, a mais utilizada a nível nacional e a que origina mais preocupações, devido ao número crescente de ilícitos praticados com recurso a esta (SIBS, 2020). A SIBS, em 2014 criou esta plataforma que tinha como objetivo agilizar compras *online*, sendo possível realizar as transações associando apenas um número de telemóvel a uma conta bancária, todo o processo de adesão poderia ser realizado numa caixa multibanco. A plataforma MB Way foi evoluindo cada vez mais, disponibilizando serviços para além daqueles que permitiam o pagamento de algo *online*, tendo como destaque a introdução na plataforma do serviço MB Net que permite a criação de cartões virtuais e os pedidos diretos de dinheiro entre usuários fazendo o uso exclusivo da plataforma para realizar todas as ações. A mais recente evolução é o uso do MB Way como se de o cartão associado à plataforma se tratasse, sendo possível realizar o pagamento através de terminais multibanco recorrendo apenas a um dispositivo móvel que tenha a aplicação instalada (MB Way 2020).

Segundo a Nota prática nº 20/2020 (2020), a evolução dos métodos de pagamento é uma realidade observável que produz vantagens e desvantagens evidentes. Por um lado, é possível uma universalização do comércio sendo que através do recurso à internet é possível realizar qualquer tipo de compra, em qualquer parte do mundo. Por outro lado, os métodos ilícitos praticados com o recurso a estas plataformas são difíceis de prever e combater por parte das autoridades competentes, todo o processo requer uma constante adaptação a uma sociedade digital em permanente evolução.

2.2 Banca eletrónica e comércio eletrónico, enquadramento legal

O aparecimento da banca eletrónica é relativamente recente, sendo a que as suas primeiras menções em artigos ocorrem apenas no início do século XXI, este fenómeno acontece através do aparecimento de uma sociedade de informação, que gera desafios e tumores diariamente. A banca eletrónica traduz-se num fenómeno mundial que consiste na utilização de serviços bancários fazendo o recurso à internet, telemóvel e *Automated Teller Machine* (ATM), existindo assim uma redução dos custos de utilização para quem faz o uso destas plataformas. O emprego de tecnologias da banca eletrónica proporciona uma autonomia aos utilizadores na gestão das suas contas bancárias, havendo a necessidade deste serviço estar em contante evolução para que nunca deixe de ser eficiente (The supervisor of banks, 2021).

O conceito de comércio eletrónico aparece diretamente relacionado com o de banca eletrónica, é uma evolução natural dos recursos proporcionados e um facilitismo criado para ou seus utilizadores. O comércio eletrónico surge como se fosse um retalhista de elevada qualidade que oferece os seus serviços *online*, em vez de ser o tradicional modo presencial. Foi inicialmente definido como meio de divulgação de serviços de certas marcas para os seus consumidores, sendo que nos dias que correm assenta em plataformas de compra e venda de produtos e serviços (Alves, 2017).

As vulnerabilidades dos sistemas e redes desta sociedade é espelhada em assuntos como transferência bancárias pela Internet, à revelia dos titulares das contas. O conceito de banca eletrónica já foi explicitado por diversos autores, mas em comum a todos, está a referência a um uso das funcionalidades do banco à distância e o perigo de subtração dos dados de acesso feito por piratas informáticos. O aparecimento destes novos acontecimentos motivam as investigações sobre o tema e consequente abordagem jurídica do mesmo, levantando questões relativas ao enquadramento feito e se esse

enquadramento é o mais correto a adotar devido à evolução da prática deste tipo de crimes (Correia & Jesus, 2016).

É devido ao aparecimento das ferramentas anteriormente mencionadas, que a maior parte dos crimes tipificados como burla informática e nas comunicações surgiram nas últimas décadas, a prática criminosa é associada à introdução ilegal no sistema informático do lesado, fazendo uma manipulação e usurpação de dados do mesmo aproveitando-os a seu favor (Santos, 2005, p. 259-260). O enquadramento jurídico destes fenómenos é dúbio e nem sempre consensual, tendo em conta as explanações feitas no capítulo 1 relativamente à tipologia e forma dos crimes existentes no sistema jurídico português. Apesar da tipificação mais comum nos ilícitos deste género ser a burla, o que está em causa não é uma violação do património mas sim uma manipulação de dados, não sendo assim o enquadramento jurídico mais correto a adotar (Correia & Jesus, 2016). Para Correia & Jesus, após uma análise de diplomas legais referentes à criminalidade informática, como a Lei da Cibercriminalidade Informática e a Lei do Cibercrime, o enquadramento legal dos ilícitos relacionados com a banca eletrónica, deveria ser feito nos diplomas da matéria da cibercriminalidade e não no Código Penal. Ao ser adotada a linha de pensamento destes autores, a discórdia perante o atual enquadramento legal dos ilícitos é permanente, sendo que os mesmos consideram um incorreto enquadramento jurídico dos crimes em estudo.

Os crimes praticados com recurso à plataforma MB Way são possíveis de ser realizados devido à integração desta plataforma num sistema de banca eletrónica. Através do uso do MB Way são possíveis realizar transferências e pagamentos sendo apenas necessário associar um número de telemóvel a uma conta bancária e ligação à internet. Os níveis de criminalidade com recurso a este meio sofreram um grande aumento em 2020, facto motivado pelo crescimento do número de compras realizadas *online* (comércio eletrónico) e consequente uso dos sistemas de banca eletrónica, todos estes fatores foram originados pela pandemia Covid-19 vivida na época (RASI 2020).

2.3 MB Way em Portugal, soluções e problemas da plataforma

O aumento do número de compra e venda de produtos e serviços *online* motiva um crescimento do uso de plataformas de pagamento que façam o recurso à internet. Em todas as transações comerciais que se realizem, o conceito de pagamento tem de estar implícito, numa realidade virtual, como é a do mundo *online*, são simulados mecanismos

de pagamento eletrónicos que se traduzem nas transações realizadas através plataformas de pagamento *online* (Ureche & Plamondon, 2000).

As plataformas eletrónicas de pagamento, podem ser consideradas como "um tipo de sistema de informação interorganizacional para transações monetárias, com o propósito de conectar simultaneamente entidades coletivas e individuais" (Lapa, 2021, p.40). Os métodos de pagamento servem de auxílio às organizações de forma a satisfazerem as preferências de pagamento dos seus clientes (Comissão Europeia, 2021). Para que sejam fiáveis as transações eletrónicas realizadas, deverão obedecer a alguns requisitos, entre eles autenticação, integridade e confidencialidade, desta forma as quantias em causa são autorizadas pelo cliente e a segurança das operações consegue ser assegurada (Amor, 2000).

A evolução dos tempos, e todos os fatores observados nos últimos anos, levam a que a implementação de plataformas eletrónicas de pagamento na sociedade seja usual. As operações realizadas são diversas e abrangem todos os espetros das transações efetuadas, desde o uso comum em estabelecimentos comerciais e as transações físicas, ao pagamento que é efetuado através do uso da internet, em dispositivos eletrónicos, o comércio eletrónico, a realização de pagamentos e transferências através de plataformas bancárias *online* e a mais recente novidade nesta matéria, a introdução das criptomoedas que são consideradas como meios de transações monetárias eletrónicas (World Bank, 2016).

Portugal, não foi exceção à evolução dos sistemas de pagamento, acabando por adotar plataformas eletrónicas de pagamento como forma de realizar as transações monetárias na realização das suas compras. A plataforma de mais destaque no nosso país é o MB Way, criada pela SIBS, sendo "o método de pagamento preferido nas compras *online* dos utilizadores" (SIBS, 2020). A plataforma MB Way pode ser definida como "solução multibanco que permite fazer compras *online* em lojas físicas, gerar cartões virtuais, enviar e pedir dinheiro e levantar dinheiro através do smartphone" (MB Way, 2022, p.14).

A aplicação MB Way é considerada segura, pois a sua utilização apenas implica a associação de uma conta de débito a um número de telemóvel, não sendo feita a partilha de quaisquer dados confidenciais com o comerciante. No entanto, e apesar da segurança durante o uso da aplicação, feita pelo próprio titular da conta, ser uma realidade, a sujeição a práticas ilícitas está presente e tem uma evolução cada vez mais evidente. O número de ilícitos praticados com o recurso a plataformas eletrónicas de pagamento, e mais

especificamente o MB Way, é uma realidade cada vez mais observada no nosso país. (Deco Proteste, 2019).

Como disse, Oliveira (2020) as denúncias recebidas nos últimos tempos, relacionadas com o fenómeno das Burlas MB Way, têm vindo a aumentar consideravelmente. Este fenómeno observa-se normalmente em plataformas de compra e venda de produtos como o OLX, ocustojunto.pt entre outras. O engano fraudulento tem vindo a ser desenvolvido através do uso da plataforma MB Way, e tem originado diversas vítimas, que são levadas a disponibilizar valores monetários, por vezes de montante bastante elevado. Nesta temática tanto a caracterização da vítima, como a caracterização do lesado, são importantes. A complexidade do crime é de tal ordem, que não se cinge apenas há grande abrangência registada na população, mas também à sua tipificação.

Nos órgãos de comunicação social e mais precisamente no Alerta da GNR para diferentes burlas através do MB Way, feito na revista sábado, percebemos que todos poderemos estar sujeitos a este tipo de abordagem, e a falta de conhecimento sobre a temática leva a que qualquer tipo de pessoa se possa tornar vítima deste tipo de burla, como os métodos utilizados recorrem ao uso de plataformas *online*, o crime acontece em todo o país, sem qualquer relação entre as vítimas. A idade das vítimas é variável, sendo que os principais utilizadores das plataformas mais afetados, são geralmente vendedores ou compradores de diversos produtos, sendo que normalmente a oferta tem como objetivo a rápida venda/ compra, assim como uma boa relação qualidade/preço. Se no caso das vítimas não existe qualquer relação aparente entre os lesados, no caso dos burlões/ criminosos é possível identificar um padrão de atuação, são diversos os agentes que atuam nesta área, fazendo o uso de cartões pré-pagos e verifica-se que já burlaram diversas vítimas, o que por vezes leva a uma conexão processual penal, devido a esta abrangência nacional poderá ocorrer a relação entre processos, em diversos pontos do país (Instrução nº 1/2020). Assim a junção dos processos e consequente atribuição da investigação é feita de acordo com o local onde os levantamentos em caixas multibanco foram feitos, pois a probabilidade do autor do crime se encontrar na zona referida é maior (Nota Prática 22/2021), todos estes acontecimentos serão explanados detalhadamente no próximo capítulo.

A novidade que este crime originou, levantou controvérsia quanto à sua classificação e também competência de investigação. O Ministério Público, a GNR e a Polícia de Segurança Pública (PSP) têm classificado este crime de diversas formas, desde

Burla, prevista no artigo 217.º do Código Penal, Burla Qualificada, prevista no artigo 218.º o Código Penal, Burla informática e nas comunicações, prevista no artigo 221.º da Código Penal, entre outros. São estas diferentes classificações que levam à delegação da investigação aos diversos órgãos de polícia criminal. Nos crimes de Burlas, excetuando aquelas que têm um valor consideravelmente elevado ou outras circunstâncias que estejam previstas no Código Penal ou na Lei de Organização da Investigação Criminal (LOIC), a competência da investigação cabe à GNR e PSP. As diversas interpretações referentes à tipificação deste crime, levam a que a atribuição dos inquéritos referentes a esta temática sejam deferidos por parte da GNR e PSP para a Polícia Judiciária (PJ), isto é motivado por estar previsto na LOIC que é da competência reservada já à PJ, a "Burla" punível com pena de prisão superior a 5 anos, artigo 7.º, nº3, c) e l) da LOIC, através da interpretação desta lei pode concluir-se que a Burla informática é da competência da PJ.

A prática de crimes MB Way recorre aos métodos variados, constituem Burlas recorrendo à falta de conhecimento dos lesados, o burlão/ criminoso não tem uma ação direta na plataforma informática, dessa forma o crime não poderá ser considerado como "burla informática e nas comunicações", previsto no Código Penal, poderá então ser enquadrado como "burla" ou "burla qualificada", consoante as circunstâncias. De acordo com o artigo 8º da LOIC a competência de investigação pode ser deferida, ocorrendo durante a fase de inquérito, artigo 7º da LOIC. Assim, mesmo que o crime de "burla" seja da competência da GNR ou PSP poderá ser submetido para a PJ, este ato constituí uma competência deferida para a investigação criminal previsto no artigo 8ºda LOIC. Em caso de reserva do inquérito para a PJ, todos os prossuposto devem ser cumpridos de acordo com o artigo 10º, nº3 da LOIC.

De acordo com a opinião mais recente do Ministério Público sobre o tema, este é tipificado como potencialmente crime de falsidade informática e acesso ilegítimo, sendo assim feita a atribuição do inquérito para investigação à PJ, a nível nacional. Desta forma, foi feita uma coordenação e articulação da investigação, por se encontrar apenas um OPC a investigar este crime.

CAPÍTULO 3
A GNR NA PREVENÇÃO E INVESTIGAÇÃO DOS CRIMES DE BURLA RELACIONADOS COM O USO DE PLATAFORMAS ELETRÓNICAS DE PAGAMENTO

3.1 Os tipos de ilícitos praticados com recurso a plataformas eletrónicas de pagamento

O Ministério Público desde 2019, que recebe de forma cada vez mais recorrente, denúncias relacionas com ilícitos de burlas com recurso à plataforma MB Way. Estes dados decorrem dos RASI de 2019, 2020 e 2021. Este fator é motivo de preocupação para todas as entidades e autoridades competentes, pelo que é necessário começar a estudar o fenómeno e estabelecer procedimentos de atuação, de forma a dar respostas corretas a este tipo de ilícitos.

Primeiramente, é necessário estudar a forma como são praticados os ilícitos, tendo em conta os métodos utilizados, as plataformas que são utilizadas para a realização do crime, os tipos mais prováveis de vítimas e os tipos de burlões que comentem os ilícitos. O Ministério Público elabora diversas notas práticas e relatórios de situação sobre o tema, ferramenta muito útil para as forças de segurança, que dessa forma se vão mantendo atualizadas e conseguem atuar de forma mais eficaz. As burlas MB Way têm sempre como princípio de atuação a utilização de uma forma de comércio não presencial, seja através de redes eletrónicas ou não.

Segundo o Relatório da SIATID, do Ministério Público (2021), existem atualmente quatro grandes métodos para a prática dos ilícitos utilizando a plataforma eletrónica de pagamento MB Way. Em todos os métodos é comum a vontade de venda de um produto ou serviço por parte da vítima, sendo feito uma escolha nas redes sociais e plataformas de compra e vende de produtos, como o OLX e o Custo Justo, por parte dos burlões de quem serão os seus "alvos". A procura dos praticantes do crime, recaí em pessoas que não tenham conhecimento das funcionalidades da plataforma MB Way ou que o seu conhecimento seja bastante reduzido, é então feita a proposta de pagamento fazendo o recurso a esta plataforma por ser a forma mais rápida e segura de realizar a transação, e após esta aceitação, o burlão oferece-se para ajudar o futuro burlado a usar o MB Way, para que assim seja possível levar a pessoa em causa ao engano. Após todo este

procedimento, é solicitado que a vítima se desloque até uma caixa multibanco, onde o restante processo de associação da conta do lesado ao número de telemóvel do burlão é consumado, através da disponibilização dos códigos de acesso (Nota Prática nº 20/2020).

As forças segurança sentiram a necessidade de se adaptarem aos novos ilícitos praticados na sociedade, fazendo assim uma formação e consequente evolução técnica, o que originou uma adaptação dos criminosos a este nova realidade, que agora recorrem a formas de burla mais sofisticadas (GNR, 2022). Assim, segundo o Relatório da SIATID, do Ministério Público (2021), são enumerados e explicados os quatro principais métodos utilizados, sendo os mesmos: cedência dos dados do cartão da vítima; cedência dos dados do cartão da vítima através do envio de códigos de levantamento; método de *smishing* e método de *phishing*- falso serviço OLX.

O primeiro método, cedência dos dados do cartão da vítima, é utilizado quando existe desconforto ou negação por parte da vítima em usar a aplicação ou deslocar-se até uma caixa multibanco, assim o burlão sente necessidade de ser o próprio a associar os dados do cartão ao seu número de telemóvel, sendo então essencial obter os mesmos. Através do contacto mantido com a vítima, são solicitados os números do cartão de débito/ crédito, de que a mesma é titular, e os três dígitos de segurança (código cvc), após a obtenção destes dados, o burlão tem total capacidade de fazer a associação da conta bancária do lesado ao seu número de telemóvel, através da aplicação MB Way, ficando assim com total acesso à mesma.

Num segundo método, cedência dos dados do cartão da vítima e dos respetivos códigos de levantamento, o burlão não solicita qualquer dado bancário ao lesado, ou seja, não são pedidas informações sobre o cartão do lesado ou o código de segurança do mesmo (como no primeiro método). O agente criminoso pede que a aplicação MB Way seja utilizada na opção "levantar dinheiro", desta forma são produzidos códigos de levantamento pelo lesado, que são posteriormente enviados para o burlão sem que o mesmo se aperceba que está a ser lesado, sendo feitos levantamentos até ao valor máximo de 400 euros, levantamento máximo que pode ser efetuado num dia em Portugal (Multibanco, 2022).

Num terceiro método, método de *smishing,* a cibercriminalidade já é observada de forma mais aprofundada e deve ser analisada de maneira mais especializada. O *smishing* consiste na tentativa de obtenção de dados, pessoais, financeiros ou de segurança, através do serviço de mensagens (APB, 2017). Neste método todos os tipos de comércio poderão utilizados, desde o e-commerce até ao comércio tradicional, no entanto é no mercado

online que a sua prática foi verificada. O burlão para a realização deste método, não realiza chamadas telefónicas, ao contrário do que se verifica nos métodos explicados anteriormente, por sua vez, usa plataformas de mensagens desde o comum SMS, Whatsapp e email. Depois das negociações serem realizadas, sempre recorrendo às plataformas referidas, o burlão envia um link ao lesado, onde é enviado um formulário para que seja realizado o preenchimento de dados que serão utilizados para, supostamente, efetuar o pagamento ou para ser feito o envio de algo. O *link* enviado corresponde a um *site* simulado, que aos olhos do comprador parece que uma plataforma para si familiar, como por exemplo o *site* dos CTT. O lesado acaba por preencher todos os dados solicitados, dando assim acesso ao burlão aos dados necessários para que este faça a burla e fique com total acesso às contas bancárias dos lesados.

O último método alvo de estudo, é o método de *phishing*- falso serviço OLX, mais uma vez o tema da cibercriminalidade está implícito e necessita de uma análise mais elaborada. O *phishing* pode ser enquadrado em várias formas, mas interessa perceber que *phishing* é uma fraude realizada através de métodos eletrónicos, que tem como principal objetivo a obtenção de dados dos lesados, de forma ilícita (Ribeiro, 2015). No caso específico das burlas efetuadas com recurso a plataformas eletrónicas de pagamento, o método utilizado é semelhante ao descrito anteriormente, o *smishing*, pois a concretização do ato da burla é feita através do envio de uma mensagem da parte do burlão para o lesado. Ao longo de todo o processo, a fase de negociação é feita da forma regular, a principal diferente na burla que é realizada através de phishing é a apresentação de uma "nova funcionalidade" da plataforma de compra e venda de produtos (a mais utilizada para realizar este ilícito é a plataforma OLX). Esta funcionalidade consiste num serviço de entregas feito pela própria plataforma, serviço oferecido graças a uma suposta parceria entre a mesma e os CTT. O burlão envia um link ao lesado, onde após o mesmo fazer o preenchimento de dados, ficará com acesso ao serviço disponibilizado, é desta forma que que é feita um falso pagamento e a apresentação de um falso transporte para a mercadoria. No entanto, o resultado final é apropriação de dados pessoais e bancários do lesado, por parte do burlão, ficando o mesmo com capacidade, através do uso da plataforma MB Way, de ter acesso às contas bancárias do lesado.

Os ilícitos praticas estão em contante evolução, o que torna a tarefa das autoridades dificultada, sendo necessária uma contante avaliação e consequente formação na matéria para dar resposta aos problemas encontrados.

3.2 Capacidades da GNR para investigação de crimes de burlas com recurso a plataformas eletrónicas de pagamento

As forças de segurança, com particular interesse para a presente investigação, a GNR, necessitam de se adaptar às novas práticas ilícitas que vão surgindo na sociedade e estabelecer procedimentos de abordagem e resolução para problemáticas com que se deparam.

Primeiramente, é necessário identificar o OPC competente para a realização da investigação no âmbito criminal, este processo é realizado de acordo com o previsto no artigo 8º da LOIC, competência deferida para a investigação criminal, e segundo o entendimento do procurador do Ministério Público responsável pelo inquérito. As circunstâncias observadas em cada caso, podem definir diferentes tipificações criminais do ilícito, como já foi explicado no primeiro capítulo da presente investigação, de acordo com a tipificação feita a atribuição do processo poderá ser delegada na GNR, PSP ou PJ, seguindo sempre os princípios estabelecidos na LOIC (Nota Prática nº 20/2020).

Na Nota Prática nº 22/2021, é feita a análise do tipo de crime em causa é crucial no que à competência territorial diz respeito, os fenómenos observados, que dizem respeito a ilícitos com recurso a plataformas eletrónicas de pagamento, são bastante abrangentes e dispersos a nível nacional, fazendo com que o elemento que faz a conexão do processo seja variável. Esta dispersão poderá ser explicada pois numa primeira abordagem o contacto entre as parte é efetuado a partir de um local desconhecido, após ser realizada a negociação, dá-se então o processo de burla em si, em que são feitas transferências bancárias ou levantamentos de numerário fazendo o recurso a meios eletrónicos ou caixas ATM, sendo aqui a dispersão nacional uma realidade incontrolável por parte dos OPC. Caso tenha sido a vítima e realizar a operação, quando levado ao engano, é fácil identificar o loca onde as mesmas foram realizadas, uma vez que o lesado transmite essa informação no momento da queixa, caso tenha sido o burlão a efetuar a operação é necessária uma investigação mais aprofundada para averiguar todos os prossupostos.

A competência territorial é também afetada pelas diversas investigações existentes espalhadas pelo país, que em muitos casos se tornam num processo único. Este tema é abordado e explicado na Instrução nº 1/2020 do Ministério Público, é relatado que apesar das vítimas dos processos existentes serem desconhecidas umas das outras, verifica-se que o agente ou grupo que praticou o ilícito poderá ser o mesmo, as queixas são

apresentadas por todo o país, sem ligação entre elas e de forma dispersa, no entanto o agente criminoso, vem muitas vezes a verificar-se o mesmo, pois os contactos telefónicos são efetuado através de consultas de anúncios *online*. A observação de todos estes fatores, leva à conexão de vários inquéritos num só processo, contudo tal só se verifica quando a atribuição da investigação tenha sido feita no mesmo OPC, quando os processos se encontram todos distribuídos no mesmo magistrado ou quando os processos são da responsabilidade do mesmo departamento ou serviço do Ministério Público. A atribuição de competência de investigação num mesmo processo poderá ser feita em OPC diferentes, este facto é observado devido à imensidão de processos espalhados em diferentes comarcas e ao tratamento não abrangente que existe nos dados que são tratados em âmbito processual.

O contacto efetuado entre o agente que pratica o crime e a vítima é realizado de forma virtual, não existindo contacto físico entre eles, desta forma os meios de prova que existem são digitais. Os elementos de prova existentes são muitas vezes armazenados por um curto espaço de tempo, sendo posteriormente eliminados, desta forma, a rápida recolha de prova e informação é essencial para o sucesso do processo de investigação (Nota Prática nº 20/2020).

O processo de investigação tem início com a receção da queixa e é aí que são necessários recolher certos elementos que ajudaram na futura investigação. Desta forma, a GNR emitiu um conjunto de instruções e informações para que o processo fosse uniformizado e os mais completo possível (Nota Prática nº 20/2020). No momento de receção da queixa é importante recolher o máximo de informação com todos os detalhes considerados pertinentes. Inicialmente é importante que a vítima dê a descrição de todos os factos referentes ao ilícito de que foi alvo, nesta parte importa perceber os dias e horas que os contactos foram estabelecidos, todos as características possíveis de averiguar sobre o suspeito da prática ilícita, todos os aspetos referentes ao anúncio colocado *online*, devem ser identificados todos os métodos de contacto utilizados pelo agente do crime (mensagens, chamadas, email…), identificação do o número de telemóvel do suspeito e do número de telemóvel associado à plataforma MB Way, indicar a conta ou os cartões bancários que foram associados no ato da burla e obter um extrato dos movimentos bancários (DIC, 2020).

Na instrução realizada pela Direção de Investigação Criminal- DIC (2020), também são referidos os procedimentos internos a adotar por parte dos profissionais que recebem a queixa. É importante a recolha e tratamento de elementos como, a cópia ou

impressão do anúncio que foi utilizado para a realização do esquema fraudulento, aconselhamento da vítima para não eliminar os dados telefónicos referentes ao contacto com o burlão, poderão servir como meio de prova relevante para a investigação, fazendo assim a recolha e registo de todas as mensagens, referentes ao ilícito, que a vítima tiver em sua posse, fazer a identificação da caixa multibanco, caso tenha sido realizado algum levantamento por parte do agente criminoso (importante recolher o local e entidade), realizar as diligências necessárias para fazer a recolha das imagens da caixa multibanco, anexar ao processo, em caso de existência, da queixa da vítima à entidade bancária e verificar em plataformas internas se os dados recolhidos coincidem com algum inquérito já existente.

Após a realização de todos os pressupostos referentes ao procedimento de queixa, dá-se início ao processo de investigação, é necessário então, analisar todos os dados recolhidos e completar as informações registadas até ao momento, assim, importa solicitar a entrega de imagens em locais onde tenham sido realizados levantamentos ou pagamentos com os dados do lesado, que anteriormente apresentou queixa, bem como todos os registos presentes nesses locais, como são exemplos faturas de compras de produtos. Dentro da estrutura de investigação criminal também é importante a atribuição de tarefas para que a recolha de dados seja o mais rápido e eficaz possível (GNR 2022).

No contacto inicial com o Ministério Público é importante fazer o pedido de algumas diligências para assegurar que os meios de prova são utilizados na sua plenitude e que a recolha de informação é feita da forma mais célere possível (GNR, 2022). Desta forma, é importante que seja feito o pedido à operadora responsável para a identificação do titular do cartão SIM utilizado para a realização da burla, assim como, de todos os IMEI[2] onde o cartão SIM este ativo e identificar se mais algum cartão está associado ao mesmo proprietário. Nos casos em que o cartão SIM é um pré-pago é importante identificar o local da venda do cartão utilizado, solicitando essa informação à operadora. Desta forma, poderá ser posteriormente solicitada a visualização das imagens de segurança do estabelecimento onde o cartão foi adquirido DIC (2020).

No contacto com entidades externas, como as instituições bancárias e a própria SIBS é necessária a recolha de informações que ajudaram no apuramento dos factos. Junto da entidade bancária, é necessário pedir o congelamento da conta para onde foram

[2] IMEI- *International Mobile Equipment Identify*- Número de identificação global, único para cada telemóvel.

feitas as transferências fraudulentas, o levantamento do sigilo bancário para que desta forma sejam obtidos os estratos dessa/as contas e o levantamento de todos os números telefónicos associados a esse cliente e respetivas contas bancárias. No que diz respeito à SIBS, é importante que esta forneça a informação de todas as contas bancárias associadas aos números de telemóvel identificados para a realização da burla na plataforma MB Way, assim como todos os movimentos realizados com o recurso à aplicação móvel da plataforma eletrónica de pagamento (GNR 2022).

Quando todas as informações estiverem disponíveis e capazes de serem analisadas, a estrutura de investigação criminal da GNR dá início ao processo de análise de informação que irá ser uma ferramenta útil para a investigação com consequente apuramento de factos.

3.3 A problemática da Prova Digital

Araújo & Faria (2007), constataram que a tecnologia é uma realidade ao alcance de qualquer pessoa, sendo a capacidade de manusear e conhecer as ferramentas digitais uma realidade observada na sociedade em geral. A evolução de uma sociedade virtual promove o uso das tecnologias como ferramentas de realização criminal, surgem como forma de engano tanto para as forças de segurança, no combate a todo o tipo de ilícitos, como para as próprias vítimas dos crimes que são iludidas através dos meios eletrónicos (Rocha, 2019).

Na evolução dos fenómenos criminais, a evolução das tecnologias tem um papel preponderante. A existência de um mundo virtual é aproveitada pelos criminosos como uma janela de oportunidade para a realização e inovação de ilícitos. “Os deslocamentos das tecnologias de informação e comunicação para a criminalidade (…) trouxe consequências nunca antes vistas. Estas tecnologias permitem não só um rápido crescimento da criminalidade de efeitos globais, como, as mudanças das práticas dos tradicionais tipos de crime e o surgimento de uma nova criminalidade- o Cibercrime” (Santos, 2020, p.2).

É importante definir cibercrime para perceber melhor a dimensão da problemática em estudo. Assim, de acordo com o estabelecido na Convenção sobre o Cibercrime (2009), esta prática criminosa é definida como um ato ilícito praticado com recurso ou contra uma rede de comunicação eletrónica ou um sistema de informação. Nos atos praticados na área do cibercrime são utilizados dispositivos eletrónicos como objeto de crime, sendo utilizada a informática como meio malicioso (Santos, 2020, p.2).

Os meios utilizados para as práticas criminosas a nível informático, têm um caracter digital, em consequência as provas recolhidas para a realização das investigações são, provas digitais, condição que impões a implementação de novas práticas e o aparecimento de novos desafios para a investigação criminal (Santos, 2020, p.3). A prova digital é uma prova volátil, de natureza complexa, que consegue ser eliminada rapidamente e a existência do ilícito torna-se difícil de apurar (Rocha 2019).

Na obtenção da prova digital, todos os princípios que são acatados na obtenção de prova física têm também de aqui ser cumpridos, tendo de ser respeitados os direitos humanos, conforme previsto na Constituição da República Portuguesa, e nos artigos 124.º a 190.º do Código de Processo Penal. No artigo 341º do Código Civil está explanada a principal função da prova, que se traduz na demonstração da realidade dos factos. O ritmo de evolução tecnológica é tão elevado que se torna difícil para o legislador acompanhar, dessa forma durante o processo de investigação são encontrados entraves processuais, no que diz respeito à necessidade de salvaguardar os direitos fundamentais de todos os agentes do crime (Ribeiro, 2015). Pires (2013), definiu as principais características da prova digital, que demonstram em muito as dificuldades encontradas pelo investigador na sua recolha e tratamento. A prova digital é de carácter temporário e volátil, uma vez que, apenas se encontra disponível num determinado período de tempo que em muitos casos é reduzido; é facilmente forjável, podendo ser alterada através de manipulação informática por qualquer outro tipo de dados, por último o autor destacou a fragilidade deste tipo de prova, a mesma deve ser tratada de forma especializada e cuidada.

Uma realização correta da recolha de prova digital, é fundamental para que a mesma seja legal e consequentemente validada como meio de prova na investigação. As estruturas de investigação criminal devem ter os meios técnicos e humanos para a correta recolha e consequente análise de dados das provas recolhidas nos mais diversos crimes em que este tipo de prova seja uma realidade (Pires, 2013). Na GNR é a DIC que faz a coordenação de todo o processo de investigação criminal, desde o momento operativo até ao momento técnico, sendo assim o responsável por informar os militares de todos os procedimento a realizar (como já foi explicado anteriormente) e todo o tipo de informação relevante para este temática.

Os meios de prova e a própria prova poderão ter um caracter proibido, artigo 126.º do CPP e artigo 32.º, nº8 da CRP. Os meios de prova, são considerados meios processuais que fazem a imposição da tutela dos direitos materiais, sendo assim uma barreira, que para descobrir a verdade, é necessário ultrapassar (Costa, 2017), ou seja, para que sejam

cumpridos todos os direitos fundamentais existem limites que têm de estar sempre presentes na realidade da investigação (Ribeiro, 2015), as provas de caráter digital estão também vinculadas a este facto. O regime de proibição de prova existente, serve para disciplinar a investigação criminal realizada pelos órgãos competentes, são estabelecidas regras que necessitam de ser cumpridas, caso contrário o não cumprimento do respeito dos direitos individuais é uma realidade e a prova poderá ter um caráter nulo (Costa, 2017).

O respeito pelos direitos fundamentais, e consequências disso, traduzem-se numa dificuldade para a realização da investigação criminal, num processo em que os meios de prova sejam digitais. No entanto, estes não são os únicos entraves encontrados ao longo da investigação, sendo necessário respeitar todos os protocolos existentes entre a Procuradoria-Geral da República e as operadoras de telecomunicações e pesquisa em plataformas de cooperação internacional e a nível da União Europeia, atividades que despendem de algum tempo que no trabalho com prava digital é fundamental, tendo em conta o seu caráter volátil (Almeida, 2014). Já no que diz respeito aos profissionais que fazem a recolha e o tratamento deste tipo de prova, os mesmos, têm de ter capacidades técnicas em investigação criminal complementadas por um conhecimento informático avançado, sendo para isto necessário o investimento em formação dos profissionais da área (Santos, 2020).

3.4 Programas de prevenção criminal de policiamento comunitário na prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento

O trabalho desenvolvido pelos militares da GNR na prevenção de ilícitos praticados com recurso a plataformas eletrónica de pagamento é essencial, para que a população esteja informada e se possa precaver de ser vítima destes fenómenos criminosos (GNR 2022).

Através das redes sociais, meios de comunicação em geral, ações de sensibilização em juntas de freguesias e escolas e fazendo policiamento de proximidade, deslocando-se os militares junto das populações mais vulneráveis, uma vez que estes poderão não ter acesso fácil às outras formas de divulgação, é possível dar a conhecer os novos ilícitos praticados com recurso a plataformas eletrónicas de pagamento e transmitir conhecimentos à população que permitam que não sejam levados ao engano. A constante divulgação das operações de combate a este tipo de ilícito, realizadas pela GNR, também

é uma fonte de informação bastante útil para manter a população alerta para este tipo de ilícito.

Os militares da GNR, devem estar constantemente atualizados no que diz respeito aos métodos de atuação utilizados pelos agentes criminosos e as plataformas mais utilizadas para realizar o ilícito, desta forma conseguirão esclarecer e alertar a população sobre a temática e dar resposta aos incidentes relacionados com a mesma.

A desinformação é uma temática cada vez mais usual, muito devido ao crescimento das redes sociais e consequente partilha de informação falsa (DIC, 2020). Por este mesmo motivo, a GNR está presente nas plataformas de redes sociais e em contacto permanente com os órgãos de comunicação social, para que a informação transmitida à população seja verídica.

O trabalho desenvolvido diariamente pelos militares, tem como objetivo principal a manutenção da segurança em todo o território nacional, sendo crucial o trabalho realizado para alertar a população para os fenómenos criminal, sendo assim feita uma prevenção da criminalidade em Portugal.

3.5 A posição do Ministério Público na temática das Burlas com recurso a plataformas eletrónicas de pagamento

Os ilícitos praticados com recurso a plataformas eletrónicas de pagamento, são uma realidade desde que existem plataformas *online* de compra e venda de produtos, sendo que na pandemia Covid 19, esta realidade de comércio sofreu um grande aumento devido ao fecho do comércio presencial e ao isolamento social, os ilícitos associados a isto, mais precisamente as Burlas MB Way, também, e segundo o RASI 2020, registaram um aumento considerável.

O Ministério Público, ao deparar-se com a complexidade criminal existente, criou e publicou a Instrução nº 1/2020, devido à necessidade de articulação e coordenação nos assuntos desta matéria. É definido que a coordenação deverá ser feita através de uma partilha de informação interna, no seio do Ministério Público, levando assim a que exista uma articulação entre processo e possível agregação dos mesmos num só. A nível regional também a necessidade de estabelecer princípios foi sentida, tendo sido criadas recomendações e a introdução desta matéria em manuais de procedimentos de forma a recolher as informações corretas no momento da investigação e a coordenar a concentração de processos dentro do Ministério Público e no próprio OPC responsável pela investigação (Nota Prática nº 22/2021).

A dispersão territorial dos processos referentes a ilícitos fraudulentos relacionados com as burlas MB Way é de abrangência nacional. Sendo possível identificar este fenómeno como um dos mais expressivos no país, conclusão retirada através dos dados partilhados pelos magistrados das diferentes comarcas (Instrução nº 1/2020).

O número de participações feitas, junto das autoridades competentes, é bastante expressivo, no entanto o número de agentes criminosos identificados é reduzido, o que implica que os processos relacionados com este fenómeno criminal tenham uma "abordagem concentrada e coordenada" (Nota Prática nº 22/2021, p. 2).

Após vários esclarecimentos e o desenvolver de diversos processos, o Ministério Público chegou à conclusão de que o importante para a atribuição do inquérito é o local onde atos ilícitos tenham sido praticados, ou seja, onde o ato criminoso tenha sido realmente consumado, não sendo importante para a atribuição do inquérito o local onde a conta que recebe os fundos de forma ilícita se encontra sedeada ou o local onde foi detetado a atividade do cartão SIM utilizado para a associação à plataforma MB Way. Em caso de desconhecimento, do local da concretização do ilícito, a atribuição do inquérito é feita no primeiro local em que tenha existido notícia do crime (Recomendação 1/2021).

Numa tentativa de especialização do Ministério Público na matéria das Burlas MB Way, foi feito um esforço para fazer a atribuição dos inquéritos, referentes a estes ilícitos, a um conjunto de magistrados especializados, no entanto tal não foi possível devido à escassez de meios humanos para o fazer. A solução encontrada foi centralização de informação no Departamento Central de Investigação e Ação Penal, sendo assim possível a consulta de todos os inquéritos e a constante partilha e atualização de informação sobre estas matérias (Instrução nº 1/2020).

Em caso de conflito de competências o Ministério Público estabeleceu que, "os inquéritos que sejam remetidos por Procuradorias da República diferentes, em que esteja em causa a investigação de Burlas MB Way (...) devem ser devolvidos por se afigurar desnecessário e prejudicial aos interesses das investigações suscitar o respetivo conflito negativo de competências sobre matérias já anteriormente decididas, podendo sempre a quem sejam devolvidos os autos, caso não mereça concordância, suscitar tal conflito" (Recomendação 1/2021, p.7).

Por todos os motivos explanado supra, é necessário continuar a aprofundar os conhecimentos na área da presente investigação, sendo esse um dos principais intuitos da presente investigação.

PARTE II- ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO

CAPÍTULO 4
METODOLOGIA DE INVESTIGAÇÃO

4.1. Natureza da Investigação

O presente estudo é realizado no âmbito de um Trabalho de Investigação Aplicada, que conclui a formação académica solicitada para a obtenção do grau mestre. De acordo com a recolha bibliográfica efetuada é possível compreender a perceção de alguns autores sobre a temática, a abordagem mais adequada para investigar a problemática e as questões que já tinham surgido aquando da investigação desses autores.

Uma investigação tem como objetivo "captar a importância do processo de aprendizagem, de forma a obter informação para atingir os objetivos pretendidos com método e rigor" (Biblioteca do Instituto Superior Técnico, 2015, p.13). A presente investigação é aplicada sendo pouco abstrata e tem uma aplicação prática, um carater exploratório com o objetivo de aumentar conhecimento sobre o tema, descritiva de forma a explanar o tema e por fim explicativa, pois tem como objetivo perceber melhor a problemática e dar resposta à questão central e às questões derivadas propostas para a investigação. Para que todos estes aspetos sejam observados ao longo da investigação é necessário "compor etapas dispostas de forma sistemática, obedecendo a uma forma sequencial" ou seja "um conjunto de etapas que quando executadas de forma sistemática facilitam a obtenção de conhecimentos", (Jung, 2009, p.37) isto é, um método científico.

Ao longo do seguinte capítulo, será apresentada a metodologia utilizada para a realização da presente investigação. Desta forma, é necessário identificar o modelo de análise, o procedimentos científico e metodológico, a amostragem e os dados recolhidos e consequente tratamento dos mesmos.

4.2 Modelo de análise

Tendo em conta que uma investigação científica é realizada na tentativa de dar resposta a uma problemática ou solucionar um problema, isto é, uma investigação científica é "um sistema de produção de conhecimentos, com base em meios de trabalho

determinados" (Romão, 2021, p.6), as questões que surgem para a investigação têm como objetivo dar respostas aos problemas existentes e solucionar os mesmos. Assim, a questão central (QC) e consequentes questões derivadas (QD), são:

QC: Qual a capacidade da GNR para prevenir e investigar o crime de burla cometido através de plataformas eletrónicas de pagamento (MB Way)?

QD.1- De que modo é feita a sensibilização / educação da população com vista à prevenção dos crimes de burla?

QD.2- De que forma as burlas são cometidas pelos autores (métodos, tipos)?

QD.3- Qual a evolução que se tem observado nas burlas com recurso a plataformas eletrónicas de pagamento (MB Way)?

QD.4- De que modo a estrutura de investigação criminal da GNR, investiga / combate o crime de burla cometido através da aplicação MB WAY e que métodos mobiliza na sua prática?

QD.5- De que forma o enquadramento legal dos crimes de burla realizados através da aplicação MB WAY implica a investigação?

Com vista ao explanado nas perguntas para a presente investigação, importa perceber qual o papel que a GNR desempenha, junto da população, na prevenção da problemática que são as burlas MB Way, a forma como estas burlas são cometidas, por quem são praticadas e quais as suas principais vítimas. Também é importante perceber quais as capacidades da GNR na prevenção e combate a este tipo de ilícitos e de que forma, estas capacidades, poderiam ser melhoradas. Por fim, o trabalho de cooperação no combate a este tipo de ilícito também é alvo de estudo, com o objetivo de perceber de que forma esta cooperação é feita.

4.3 Procedimento científico e metodológico

"A ciência utiliza-se de um método que lhe é próprio, o método científico, elemento fundamental do processo de conhecimento realizado pela ciência para diferenciá-la do senso comum" (Severino,2013, p.89), ou seja, a ciência usa o método científico para produzir conhecimento científico. Este conhecimento científico poderá ser definido como, o conhecimento diferente do conhecimento do senso comum, no entanto não é um conhecimento superior, é adquirido através do método científico e está em constante desenvolvimento (Silva, M., Costa, E., Costa, A. (2013).

A presente investigação utiliza abordagem qualitativa e quantitativa, pois faz o recurso a entrevistas semiestruturadas e inquérito por questionário a militares com

experiência na matéria em estudo, que servem para produzir dados sobre o objeto de estudo e uma análise documental que servirá também como fonte de conteúdo para a produção de conhecimento. Uma investigação qualitativa "é pautada por diferentes metodologias, técnicas e ferramentas. Quando se estudam estas diferenças quer reforçar-se a especificidade, e eficiência e a eficácia do desenho metodológico em relação aos objetivos e questões de investigação a que se quer dar resposta" (Souza, 2016). Por sua vez, uma abordagem quantitativa "caracteriza-se por ser nomotética pois enfatiza o desenvolvimento da investigação dentro de protocolos estabelecidos e técnicas específicas." (Neves, 2006).

A presente investigação assenta numa abordagem qualitativa e quantitativa. O método utilizado para a investigação, é o método dedutivo, "um método que parte do geral e, a seguir, desce para o particular" (Prodanov & Freitas, 2013, p.27), ou seja, "parte de princípios reconhecidos como verdadeiros e indiscutíveis e possibilita chegar a conclusões de maneira puramente formal, isto é, em virtude unicamente da sua lógica" (Gil, 2008, p.9).

O trabalho de investigação tem como finalidade identificar os contornos exatos deste tipo de ilícito, sob a perspetiva de Direito português, nomeadamente os métodos utilizados e o enquadramento legal do tema. Adicionalmente, este trabalho tem como finalidade abordar a vertente operacional da Guarda Nacional Republicana (GNR) sob dois prismas: (i) sob o prisma da investigação criminal, analisando as respetivas competências e capacidades da GNR neste tipo de ilícito criminal, nomeadamente os seus constrangimentos e oportunidades; (ii) sob o prisma da prevenção criminal, analisando as competências e capacidades da GNR para sensibilizar a população nesta matéria, em especial os mais vulneráveis, como as crianças, jovens e idosos, nomeadamente através do programa de prevenção criminal e policiamento comunitário. Adotou-se a matriz de investigação, constante no Apêndice B.

4.4 Amostragem: Composição e caracterização

O tempo de investigação é limitado, pelo que é necessário fazer uma seleção dentro de uma polução de uma amostra representativa, ou seja, "é necessário fazer a coleta da amostra uma vez que se pretende recolher informação da população em estudo" (Mello, 2018). Por ter sido escolhido um grupo restrito dentro do público-alvo alargado, para a realização da investigação é necessário realizar uma amostragem, de forma a perceber o pensamento e modo de atuação de toda a população (Jeová, 2016).

A escolha da amostra teve em consideração as funções desempenhadas pelos militares e especialistas entrevistados, em matéria de processos de burlas MB Way, especificamente no âmbito da investigação e prevenção e em matéria relacionada com as competências do Ministério Público. Tendo em conta os objetivos definidos, optou-se por uma amostra não probabilística por conveniência incluindo os participantes que o investigador tem maior acesso. De referir que se considerou ainda o recurso a testemunhos privilegiados, pelo conhecimento aprofundado que tinham sobre o objeto de estudo (Silva & Pinto, 2014).

4.5 Inquérito por entrevista

O público-alvo das entrevistas (Apêndice A) são militares da GNR com experiência na prevenção e combate aos ilícitos relacionados com a prática fraudulenta no uso da aplicação MB Way. Os militares da GNR entrevistados consistem, num militar da Secção de Informações e Investigação Criminal (SIIC) de um Comando Territorial, militares do Núcleo de Investigação Criminal (NIC) de diferentes destacamentos territoriais e militares de secções de inquéritos dos Postos Territoriais.

Nº Entrevistado	E	Função	Posto
Entrevistado 1	E1	Militar da SIIC	Sargento-Ajudante
Entrevistado 2	E2	Militar do NIC	1º Sargento
Entrevistado 3	E3	Militar do NIC	Cabo
Entrevistado 4	E4	Militar do NIC	Cabo
Entrevistado 5	E5	Militar NIC	Cabo
Entrevistado 6	E6	Militar da Secção de Inquéritos	Cabo
Entrevistado 7	E7	Militar da Secção de Inquéritos	Cabo
Entrevistado 8	E8	Militar da Secção de Inquéritos	Guarda Principal

Tabela 1: Identificação dos entrevistados da GNR
Fonte: Elaboração Própria

4.6 Inquérito por questionário

O público-alvo dos inquéritos por questionário (Apêndice M) é constituído por militares que pertencem à estrutura de investigação criminal da GNR, nomeadamente,

militares das SIIC dos Comandos Territoriais, militares dos NIC dos Destacamentos Territoriais e militares das secções de inquéritos dos Postos Territoriais. Dentro do dispositivo da GNR, estes militares são os que trabalham diretamente com processos relacionados com burlas realizadas com recurso a plataformas eletrónicas de pagamento e, mais especificamente com recurso à plataforma MB Way. Sendo assim, o seu conhecimento é importante para a realização da presente investigação.

Os dados recolhidos através dos inquéritos por questionário, não permitem a identificação pessoal dos inquiridos, tendo um caráter totalmente anónimo.

4.7 Métodos de recolha de dados

O processo de recolha de dados deve ser organizado e planeado rigorosamente. Uma correta aplicação deste processo aumenta a qualidade da investigação que está a ser realizada. Para Sousa & Baptista (2011, p.53) o processo de recolha de dados "é caracterizado como um procedimento operatório, rigoroso e bem definido" estes processos têm como objetivo fundamental viabilizar a investigação (Sá, Costa, & Moreira, 2021, p.17), através de uma verificação empírica (Pardal & Lopes, 2011, p.70). Todo o processo de recolha de dados é influenciado de acordo com a natureza e objetivos principais da investigação (Carvalho, 2015).

Para a presente investigação, a recolha de dados realizada recai em análise documental, inquérito por entrevista e inquérito por questionário e, todos estes dados servem para fazer um enriquecimento da investigação a ser realizada e surgem como complemento uns dos outros com o objetivo final de dar respostas as todas as questões que surjam ao longo a investigação (Alves, 2017).

A análise documental faz o complemento de informações obtidas por outras técnicas. Quando se faz uma investigação, a recolha de informação leva a que sejam construídas ideias que estruturam o trabalho realizado, todo este processo é conseguido através da análise de documentos (Matos, 2015).

O inquérito por entrevista assenta num contacto direto entre o investigador e os interlocutores (Quivy & Campenhoudt, 1992). Este tipo de recolha de dados tem como grande vantagem a adaptabilidade o que permite obter o máximo de informação e compreensão possível (Borg e Gall, 2002).

O inquérito por questionário foi mobilizado por ser um dos mais utilizados por investigadores de diversas áreas tendo como objetivo a recolha de informação factual sobre acontecimentos ou situação (Quivy & Campenhoudt, 1992).

A opção por este desenho mobilizando metodologias quantitativas e qualitativas é efetuada no sentido do complemento, isto é, esta conceção tem por objetivo compensar as fraquezas e os pontos cegos de caga um dos métodos (Brayman, 2012).

4.7.1 Data e local de recolha dos dados

A presente investigação iniciou-se em outubro de 2020, com a elaboração do projeto de TIA, no âmbito da disciplina de Metodologia do TIA, que consequentemente orientou e deu bases de estudo para a realização da mesma.

A recolha de dados, análise de documentos e toda a elaboração da investigação foi efetuada entre a Escola da Guarda, em Queluz, a Academia Militar, na Amadora, o Comando Territorial de Portalegre e repositórios científicos *online*, nos períodos entre outubro de 2021 e junho de 2022. No que diz respeito aos questionários por entrevista, foram realizados durante os períodos de janeiro e abril de 2022, fazendo o recurso a plataformas eletrónicas e ao modo presencial para a realização das mesmas.

4.7.2 Tratamento e análise de dados

Quivy & Campenhoudt (1992) entendem a realidade como muito mais rica que as primeiras questões elaboradas no início de uma investigação, pelo que a análise da informação recolhida permite interpretar os factos inesperados, e, muitas vezes leva a que se revejam essas mesmas questões para chegar a conclusões válidas. Também nós percorremos esse caminho.

Assim, a análise documental realizada teve extrema importância uma vez que as informações resumidas e obtidas numa investigação primária, direcionaram-nos, como refere Bardin (1977) para uma nova investigação, já na posse de informação relevante sobre o tema em estudo.

Nesta fase da investigação, percebemos o enquadramento legal que as problemáticas das burlas feita com recurso à plataforma MB Way, poderia ter em Portugal. Nem sempre o ilícito é tipificado da mesma forma, muito devido à maneira como os factos são praticados. Seguidamente, o objetivo foi perceber que métodos de pagamento existem e qual a sua evolução e consequente comportamento ao longo dos tempos. Desta forma, a análise documental realizada consistiu em perceber que tipo de métodos de pagamento existiram, e entre os quais que, atualmente, são utilizados requerem especial atenção por parte dos órgãos de polícia criminal. Assim, e após

enquadrar a plataforma MB Way num dos métodos de pagamento, o estudo mais aprofundado da mesma era essencial para que fosse possível entender como os ilícitos são praticados.

Numa fase seguinte da investigação foram realizados inquéritos por entrevista, analisados recorrendo à técnica de análise de conteúdo (Bardin, 1977; Vala, 2014). Adotou-se o rigor do método cujo processo é composto por três grandes fases: redução dos dados, disposição dos dados e obtenção de conclusões. Para chegar a estas últimas as categorias emergentes, o respeito pelas regras de objetividade, exaustividade, exclusividade e pertinência foram essenciais. Para tal, houve a preocupação durante a criação das sinopses de observar o referido por Guerra "que contêm a mensagem essencial da entrevista e são fiéis, inclusive na linguagem, ao que disseram os entrevistados" (2006, p. 73).

Os inquéritos por questionário foram tratados com recurso à estatística descritiva para caracterização sociodemográfica e resumo de forma simplificada das respostas dos participantes. Para ilustração adotou-se maioritariamente a representação gráfica, tendo o suporte sido efetuado através do Google Forms e o Microsoft® Office 365.

A triangulação dos dados oriundos das três estratégias distintas de recolha (análise documental, entrevistas e questionários), permitiram a validação das conclusões.

CAPÍTULO 5
APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

5.1. Apresentação, análise e discussão dos inquéritos por entrevista

No presente subcapítulo serão apresentados, analisados e discutidos, os resultados das questões dos inquéritos por entrevista realizados na presente investigação. Será feita a comparação com todo o conteúdo teórico analisado ao longo da investigação, obtido através de uma análise documental.

5.1.1 Apresentação, análise e discussão da questão nº1

A questão nº1 **"Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?"**, tem como objetivo compreender se os militares têm conhecimento da forma como a GNR realiza a prevenção dos ilícitos em estudo.

Os E1, E2, E3, E4, E5 e E7, fazem referência ao uso das redes sociais como método de divulgação do tema servindo de alerta para a população. Segundo E1, as redes sociais são utilizadas para fazer a divulgação dos métodos de burla existentes e alertar para novos métodos que possam surgir com o passar do tempo. E3 refere que as redes sociais são um instrumento utilizado para alertar a população para este fenómeno de burla e divulgar formas que evitar ser alvo deste ilícito.

Os E1, E3, E6, E7 e E8, fazem referência a ações de sensibilização sobre o tema junto de populações mais vulneráveis, usando métodos de policiamento de proximidade. O E1 refere que estas ações de sensibilização poderão ser realizadas em Juntas de Freguesia, coletividades ou outros locais onde exista um número considerado de população a alertar. Os E6 e E7, realçam o contacto direto com a população e a proximidade das patrulhas aos cidadãos considerados mais vulneráveis, como uma ferramenta chave para manter a população alerta.

É também reconhecida a importância da divulgação feita através do *site* da GNR e nos meios de comunicação social, sendo este facto sido expresso por todos os E. O E5 ressalva que a divulgação de resultados, nestes meios, das operações realizadas é relevante e serve de alerta para a população.

O E1 faz o destaque de algo que mais nenhum dos militares entrevistados referiu, dizendo que é importante manter os militares informados, para que assim, consigam manter a população informada, esclarecer dúvidas e não alimentar o sentimento de insegurança proporcionado pela desinformação existente.

5.1.2 Apresentação, análise e discussão da questão nº2

A questão nº2 **"Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?"**, pretende avaliar o conhecimento dos militares, referente ao trabalho desenvolvido no âmbito do policiamento de proximidade, na prevenção dos ilícitos em estudo.

Os E1, E3, E4 e E6 reconhecem a existência de ações de sensibilização sobre o tema das burlas relacionados com o recurso a plataformas eletrónicas de pagamento, sendo que os E1, E4 e E6, reconhecem que estas ações de sensibilização são realizadas juntos das populações mais vulneráveis com destaque para a população idosa. Neste temática E1 realça o papel fundamental das secções de prevenção criminal, no entanto, alerta que também os militares dos postos territoriais, que por terem uma presença mais abrangente e que por isso chega a um maior número de pessoas, também têm um papel de destaque nesta matéria.

Os E2, E5, E7 e E8 desconhecem o trabalho realizado pela GNR na matéria da prevenção feita através de.

Com a elaboração desta questão, é possível perceber que os militares não estão sensibilizados para a temática da prevenção da mesma forma.

5.1.3 Apresentação, análise e discussão da questão nº3

A questão nº3 **"Após receber uma denuncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?"**, tem como objetivo avaliar os conhecimentos dos militares num procedimento inicial, quando se recebe a denúncia do ilícito, momento fundamental para uma correta recolha de informações, que será utilizada para a futura investigação no âmbito criminal.

Os E1, E2, E3, E4, E5, E7 e E8 reconhecem os exposto e partilhado por todo o dispositivo, através da Instrução técnica nº 2020-04 da DIC, os E3, E4 e E5 explicam os procedimentos que adotam quando fazem a recolha de elementos de prova necessários para realizar a investigação criminal que se seguirá.

O E6, apenas reconhece que sabe os procedimentos a adotar não fazendo referência concreta aos mesmos nem à instrução técnica.

O E1 reconhece a importância da uniformização do processo de recolha de elementos essenciais a nível interno, dizendo que mesmo antes da Instrução Técnica da DIC, eu tento em conta que desempenha funções na SIIC do seu Comando Territorial, desenvolveu um relatório a alertar o escalão superior e todo o dispositivo sobre a problemática das burlas com recurso a plataformas eletrónicas de pagamento.

5.1.4 Apresentação, análise e discussão da questão nº4

A questão nº4 **"Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?"**, tem como objetivo perceber os métodos utilizados para a realização deste tipo de ilícito, já observados pelos militares.

Todos os E fazem referência ao facto de o agente criminoso ter sempre a intenção de obter um produto numa plataforma de compra e venda de produtos e serviços, como o OLX, por exemplo. Sendo que E1, E3 e E7, destacam que os burlões aceitam o preço inicial estipulado pelo vendedor (futura vítima) e negociam o mesmo a agilizam o processo de compra.

Todos os E descrevem como principal método de burla a associação do número de telemóvel do burlão ao cartão bancário da vítima, sendo que E1, E3, E4 e E5 referem que este método de burla só é possível pois a vítima não tem conhecimentos ou da aplicação ou do funcionamento do MB Way.

Os E1 e E5 explicam também um método de burla usado quando a vítima já tem MB Way, no entanto não tem conhecimento relevante sobre a utilização da mesma, conseguindo o burlão mais uma vez enganar a vítima.

As respostas dadas traduzem de facto conhecimento que os militares possuem na matéria, no entanto, reconhecem quase sempre o mesmo *modus operandi*, não estando tão familiarizados com outras formas de atuação descritas ao longo da investigação.

5.1.5 Apresentação, análise e discussão da questão nº5

Na questão nº5 **"Existem algum padrão entre os tipos de atuação dos burlões?"**, é importante perceber os padrões de atuação já identificados pelos militares, de forma a perceber, se existe alguma relação que poderá ser estabelecida nos ilícitos em estudo.

Os E revelam que o primeiro grade passo que os burlões dão para a realização das burlas é a procura de vendedores de produtos *online*, plataforma de compra e venda de produtos. Ao fazerem a abordagem para a venda, os E3, E4, E5 e E7 destacam que os burlões não fazem a negociação do preço do produto, sendo que E5 realça que os burlões muitas vezes exploram a necessidade de vender da vítima para que o processo de burla seja realizado ainda de forma mais célere.

O E1 destaca um modo de "atuação em cascata", ou seja, diz que os burlões trabalham em grupos organizados onde muitas vezes os lucros são divididos dentro dos mesmos, faz também referência a técnicas utilizadas na concretização das bulas, nomeadamente o uso de cartões descartáveis e o levantamento, preferencialmente, em caixas multibanco que não estejam equipadas com sistema de videovigilância.

Todos os E reconhecem padrões de atuação dos burlões, apesar de só o E1 ter de facto, demonstrado um conhecimento mais aprofundado no assunto.

5.1.6 Apresentação, análise e discussão da questão nº6

A questão nº6 **"Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?"**, é importante para analisar na temática do Combate a este tipo de ilícito, de forma a perceber quem são as principais vítimas e estudar em seguida as características padrão das mesmas, informação que poderá ser útil durante o processo de investigação, esta informação também é essencial para a prevenção, sendo possível assim analisar, onde a sensibilização para este tipo de fenómenos deverá ser reforçada.

Na identificação do perfil das possíveis vítimas os entrevistados dividem-se e não apresentam um padrão nas respostas. Para os E2, E5 e E6 não existe qualquer tipo de perfil da vítima, podendo qualquer cidadão independentemente da sua idade, habilitação ou local em que reside, ser alvo deste tipo de ilícito, desde que use uma plataforma de compra e venda de produtos e serviços *online*. Os E1, E3, E4 e E7, referem que a principal característica das vítimas que são alvo deste tipo de ilícito, é a falta ou pouco

conhecimento da plataforma MB Way. O burlão aproveita-se disso para iludir a vítima e assim concretizar a burla. Dentro desta temática, os E1 e E8 destacam que as vítimas mais vulneráveis são as pessoas idosas e com poucas habilitações académicas.

5.1.7 Apresentação, análise e discussão da questão nº7

A questão nº7 **"Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?"**, serve para perceber qual o contacto da GNR com instituições externas, no que aos ilícitos em estudo diz respeito.

Como identificada ao longo da investigação, o Ministério Público tem vindo a desenvolver procedimentos internos para que todo o processo realizado no âmbito destes ilícitos seja coordenado e o mais célere possível. Os E1, E2, E4 e E6, têm conhecimento do trabalho realizado, e têm conhecimento de documentos produzidos pelo Ministério Público sobre esta matéria. O resultado destes documentos, traduz-se numa maior sensibilidade perante o tema e tem como resultado um processo de investigação iniciado de forma mais célere, como referem os E E1, E3, E6, E7.

O E8 diz que não tem qualquer perceção de que o Ministério Público seja mais célere a tratar este tipo de processo em relação a outros.

O E5 foi o único entrevistado que defendeu que o Ministério Público ainda não está sensibilizado para a temática e que o processo de investigação não se realiza da forma mais célere. Justifica a sua posição dizendo que uma vez que o Ministério Público faz a atribuição da investigação na PJ mas que as diligências resultantes da mesma têm de ser solicitadas à GNR, uma vez que os investigadores da PJ não conhecem os locais ou os suspeito, torna o processo mais lento e complicado.

As posições dos militares demonstram a dificuldade existente na cooperação entre os diferentes órgãos de polícia criminal, no entanto reconhecem que já existe trabalho realizado nesta matéria.

5.1.8 Apresentação, análise e discussão da questão nº8

A questão nº8 **"Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?"**, pretende perceber qual o trabalho

desenvolvido em concreto, junto do Ministério Público, no que diz respeito aos ilícitos tratados na presente investigação.

Os dados e provas recolhidas neste tipo de processo têm um conjunto de características específicas, como é referido pelos E3, E4 e E7, já identificadas ao longo da investigação, que merecem um tratamento diferente para que a mesma tenha sucesso. Para isso e como foi identificado pelos E1 e E4, existem normas internas na GNR e Ministério Público para que a recolha destes elementos seja feitos da forma mais correta e célere possível.

Por outro lado, os E2, E5, E6 e E8 não reconhecem nenhuns procedimentos específicos de contato com o Ministério Público, no que diz respeito a este tipo de processo. Esta posição demonstra que a as diretrizes transmitidas ainda não são consensuais no dispositivo.

5.1.9 Apresentação, análise e discussão da questão nº9

A questão nº9 **"Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?"**, tem como objetivo identificar as principais dos militares na recolha de prova neste tipo de ilícito, sabendo que nestes casos, a maior parte da prova é de caráter digital.

O caracter da prova digital oriunda deste tipo de ilícitos acarreta dificuldades para a investigação, tem de ser recolhida de forma célere, por ter um caráter volátil e existe a necessidade de cooperação com entidades externas (instituições bancárias, empresas de telecomunicação) para que as mesmas sejam obtidas. Os E1, E3, E4, E5, E6 e E7 consideram que uma das maiores dificuldade é os levantamentos serem efetuados em caixas multibanco sem sistema de vigilância, não existindo assim forma de comprovar que o levantamento foi feito por determinado individuo. Os E1, E3 e E5 também realçam que a demora das entidades externa em dar resposta aos pedidos feitos pelas autoridades é um entrave para a investigação. Por fim o uso de cartões descartáveis, referido pelos E1 e E7 e a falta de conhecimentos técnicos para a análise e recolha de prova, referido pelo E5, traduzem as dificuldades identificadas pelos militares que trabalham na investigação deste tipo de ilícito.

5.2 Análise dos inquéritos por questionário

5.2.1 Caracterização da amostra

A definição da amostra é realizada através de uma análise, recorrendo à estatística descritiva, sendo possível obter os dados através das respostas dos militares ao inquérito por questionário aplicado. Os militares inquiridos são guardas, cabos e sargentos. A maioria dos militares inquiridos são cabos, 50%, seguindo-se guardas 32,8% e por fim os sargentos 17,2%.

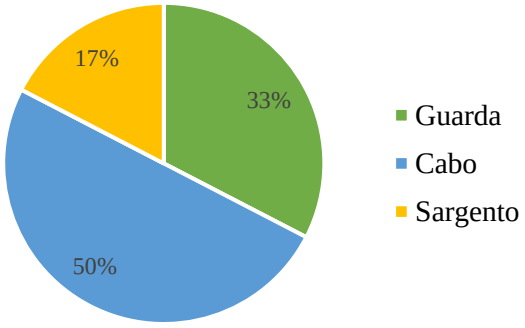


Figura 1- Posto dos militares inquiridos

Os militares inquiridos fazem parte da estrutura de investigação criminal do Comando Territorial em que desempenham funções, tendo o questionário por inquérito sido destinado a militares da secção de inquéritos dos Postos Territoriais, militares do NIC dos Destacamentos Territoriais e Militares da SIIC dos Comando Territoriais. O maior número de militares inquiridos registou-se nas secções de inquérito, 63,4%, em seguida os militares dos NIC, 25,3% e por último os militares das SIIC, 11,3%.

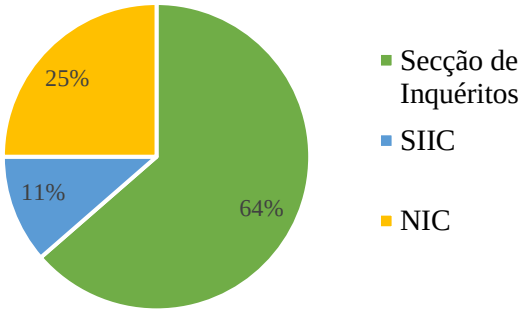


Figura 2- Área de trabalho dos militares inquiridos

No que diz respeito ao tempo de serviço que os militares desempenham funções na área de investigação criminal, foram estabelecidos três grandes grupos. Os militares que desempenham funções nesta área num período de menos de 2 anos, 16,7%, os

militares que desempenham estas funções entre 2 a 5 anos e os militares que desempenham as suas funções num período superior a 5 anos.

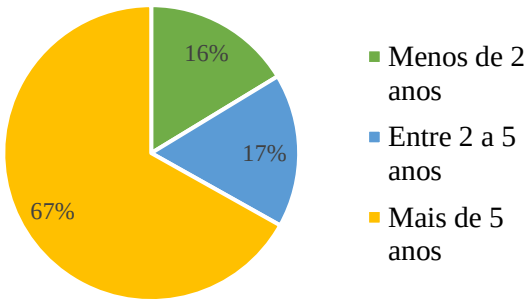


Figura 3- Tempo de serviço na área da investigação criminal dos militares inquiridos

5.2.2 Análise das questões

Relativamente à questão "***Tem conhecimento do que são as burlas cometidas através de plataformas eletrónicas de pagamento, como a do MB Way?***", todos os inquiridos responderam afirmativamente. Na questão "***Caso tenha de receber uma denúncia de burla realizada com recurso a uma plataforma eletrónica de pagamento, como a do MB Way, tem conhecimento dos seguintes procedimentos específicos a realizar?***", as respostas dos militares inquiridos traduzem-se em, 37,2% identificaram como relevante a recolha do contacto telefónico do suspeito e da vítima, 17,6% identificaram a necessidade de realização de um termo de consentimento de levantamento do sigilo bancário, 14,9% mencionaram como relevante o registo do número da conta NIB/ IBAM e13,3% consideram relevante a recolha dos dados do cartão associado de forma ilícita à aplicação MB Way. Do inquiridos, 16,3% identificam todos os procedimentos mencionados no momento da receção de uma denuncia de um dos ilícitos em investigação.

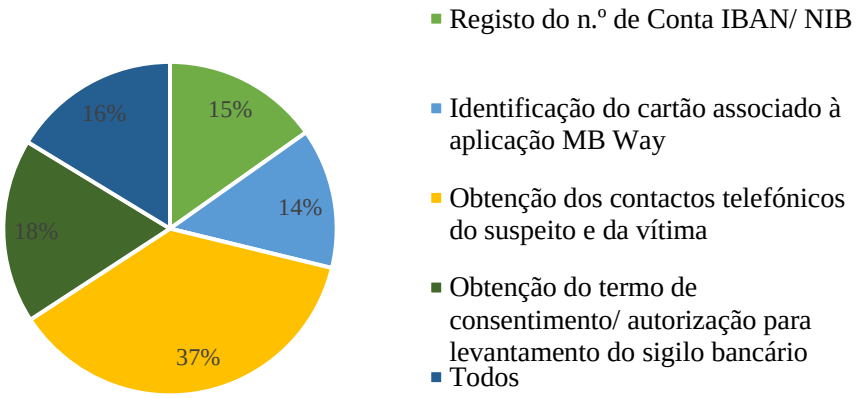


Figura 4- Procedimentos específicos identificados

No que diz respeito à questão "***Se receber uma denúncia de burla realizada com recurso a uma plataforma eletrónica de pagamento, como a do MB Way, considera que existe um perfil da(s) vítima(s)?***", é possível verificar que 61,4% é capaz de identificar um perfil da vítima e 38,6% considera que este não existe.

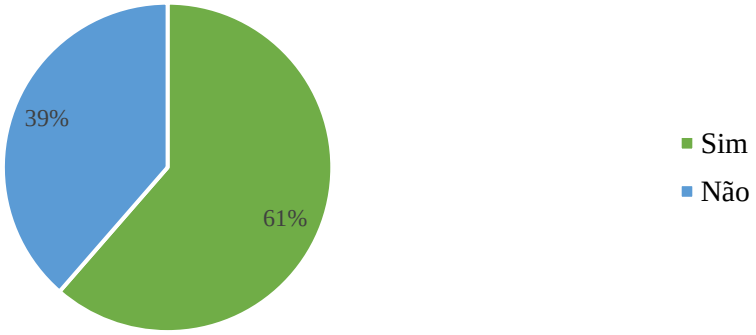


Figura 5- Perfil das vítimas

No que diz respeito à questão "***Quem são as vítimas mais comuns deste tipo de ilícitos?***", 75,1% dos inquiridos identifica como a idade das vítimas mais observada seja entre 35 e os 65 anos. 13,2% identifica como idade das vítimas mais observada entre os 18 e os 35 anos, 0,5% diz que a idade mais observada das vítimas corresponde a maiores de 65 anos e 11,1% diz desconhecer estes dados.

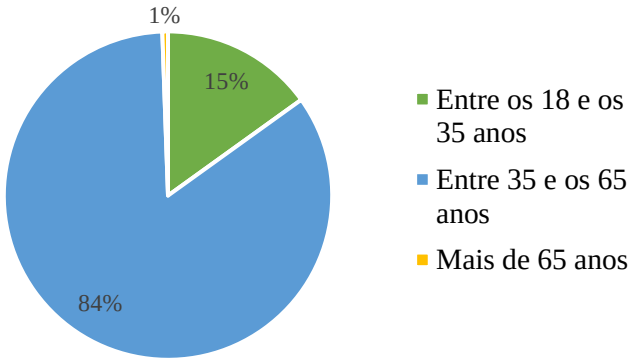


Figura 6- Idade mais comum das vítimas

Relativamente à questão "***Tem conhecimento dos modos de atuação dos agentes criminosos neste tipo de ilícitos?***", 94,2% dos inquiridos diz ter conhecimento do modo de atuação dos suspeitos e 5,8% desconhece os padrões de atuação. No que diz respeito à questão "***Ao receber uma denúncia relativa a uma burla realizada com recurso a uma plataforma eletrónica de pagamento, como a do MB Way, conseguirá identificar os***

modos de atuação usados para consumar o ilícito?", 93,7% dos inquiridos consegue identificar o modo de atuação do suspeito no momento de receção da denúncia e 6,3% reconhece que não tem esta capacidade.

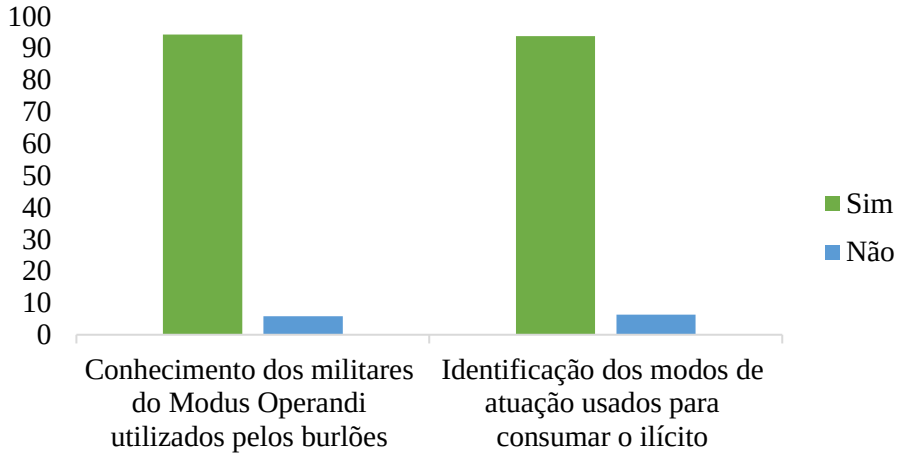


Figura 7- Conhecimento e identificação dos modos de atuação usados para consumar o ilícito

Relativamente à questão "***Qual o modo de atuação que considera mais praticado pelos agentes criminosos neste tipo de ilícitos?***", 51,6% dos inquiridos consideram que a manipulação da vítima no uso direto da aplicação MB Way é o método mais utilizado pelos suspeitos para a prática dos ilícitos, em seguida, com 35,8% das respostas, o método mais comum é a cedência dos dados do cartão da vítima através de códigos de levantamento. O *smishing* e o *phishing* também são identificados como métodos de burla com 2,6% e 7,9% respetivamente. Dos inquiridos, 1,6% diz não ter conhecimento dos modos de atuação utilizados.

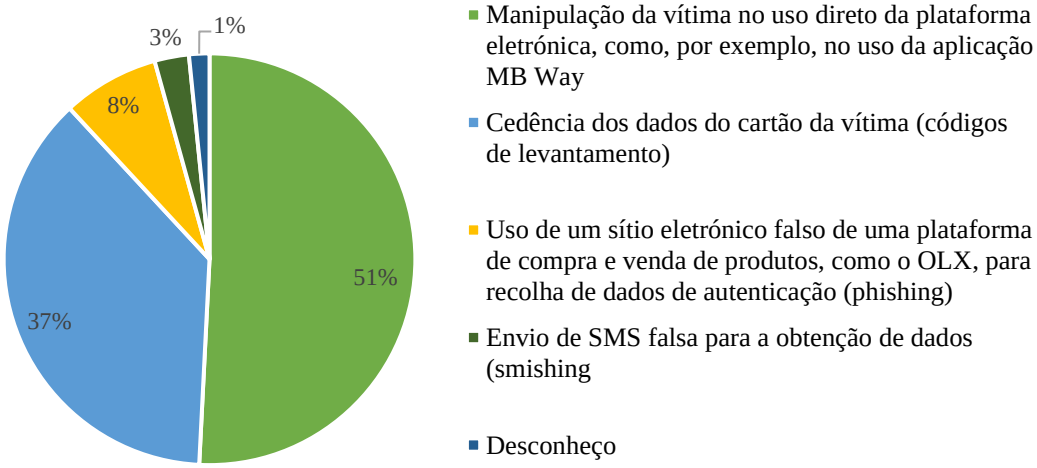


Figura 8- *Modus Operandi* mais praticado pelos burlões

No que diz respeito à questão "***Conhece alguma ação de sensibilização ou programa de prevenção da GNR direcionado para a temática das burlas realizadas com recurso a uma plataforma eletrónica de pagamento, como a do MB Way?***", 58,6% dos militares inquiridos não tem conhecimento de nenhuma das ações referidas relativamente à prevenção dos ilícitos em causa, e 41,4% tem conhecimento do desenvolvimento deste tipo de ações. Relativamente à questão "***Considera pertinente haver ações de sensibilização ou programas de prevenção criminal para a prevenção deste tipo de ilícito?***", 99,5% dos militares reconhecem a pertinência do desenvolvimento deste tipo de iniciativas, sendo que apenas 0,5% não o considera relevante.

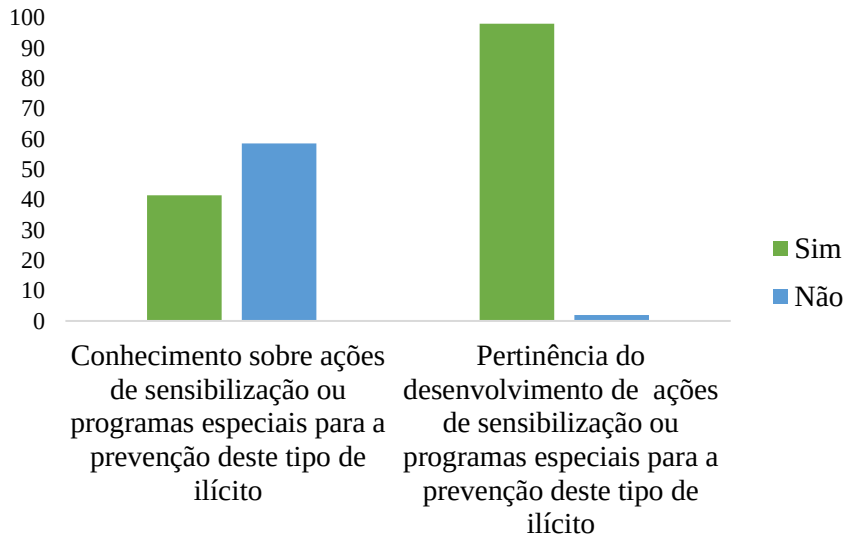


Figura 9- Conhecimento e pertinência de ações de sensibilização ou programas de prevenção criminal na prevenção de ilícitos relacionados com o uso da plataforma MB Way

Relativamente à questão "***Durante a fase de inquérito, considera que tem o(s) conhecimento(s) técnico(s) adequados para realizar as diligências de investigação para este tipo de ilícito, cometido através de plataformas eletrónicas de pagamento, como a do MB Way?***", 52,9% dos militares inquiridos considera que tem os conhecimentos técnicos suficientes para dar resposta às problemáticas introduzidas na investigação do tipo de ilícitos em causa, já 47,1% considera que os conhecimentos que possuí são insuficientes.

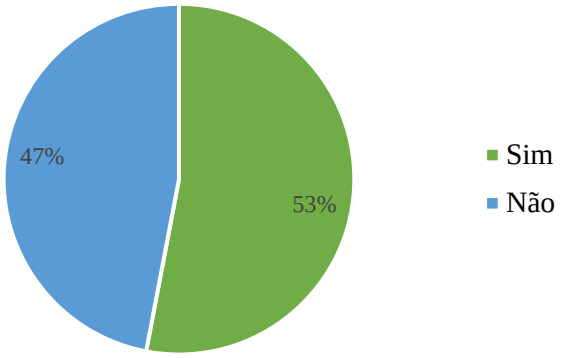


Figura 10- Consideração sobre os conhecimentos técnicos dos militares para a investigação das burlas MB Way

5.3 Discussão dos resultados obtidos nos inquéritos por questionário

Da análise efetuada, é possível afirmar que os militares que trabalham na área da investigação criminal possuem uma vasta experiência, sendo que a maior parte trabalha na área num período superior a 5 anos, tendo conhecimento do tipo de ilícito em estudo.

O número de participações deste tipo de ilícitos é significativo, o que origina um maior contacto dos militares com processos relacionados com este tipo de crimes, desta forma, os militares identificam os procedimentos que têm de realizar no momento de receção de uma denúncia, com principal destaque para a recolha do contacto telefónico do suspeito e da vítima.

A maior parte dos militares inquiridos reconhece que existe um perfil da vítima e que a idade mais comum destas se encontra entre os 35 e 65 anos. Estes fatores levam a um reconhecimento do modo de atuação dos suspeitos e consequente identificação do mesmo, com destaque para a manipulação da vítima no uso direto da aplicação MB Way.

Na área da prevenção deste tipo de ilícitos, os militares na sua maioria reconhecem a existência de ações de sensibilização ou programas de prevenção criminal para este tipo de ilícito, no entanto a parte que desconhece ainda é bastante significativa. Consequentemente, os inquiridos reconhecem na sua maioria a pertinência da existência de ações de sensibilização ou programas de prevenção criminal para a prevenção deste tipo de ilícitos.

Triangulando os dados obtidos verificou-se tanto nos inquiridos como nos entrevistados que subsistem défices de conhecimentos que para responder às necessidades existentes. Como referiu Pires (2013), o investigador, devido às características das provas digitais, encontra muitas dificuldades. Desta forma, o investimento na atualização e formação é premente.

CONCLUSÕES E RECOMENDAÇÕES

A presente investigação abordou a problemática das burlas realizadas através de plataformas eletrónicas de pagamento, com especial ênfase para a plataforma MB Way, a mais utilizada em Portugal. O foco ao longo da investigação dividiu-se numa componente teórica, que teve como objetivo perceber todos os conceitos inerentes à mesma, e uma análise do trabalho desenvolvido pela GNR, quer na área da investigação quer na área da prevenção.

A investigação foi toda desenvolvida tendo em conta a QC "Qual a capacidade da GNR para prevenir e investigar o crime de burla cometido através de plataformas eletrónicas de pagamento (MB Way)?", tendo sido possível através de uma recolha e análise de dados, e recorrendo à realização de inquéritos por entrevista e inquéritos por questionário, obter resultados que permitem retirar conclusões e adotar posições relativamente à temática em investigação.

Desta forma, importa dar resposta às questões levantadas no decorrer da investigação, nomeadamente à QC e às QD.

Relativamente à QD.1 "De que modo é feita a sensibilização / educação da população com vista à prevenção dos crimes de burla?", conclui-se que a GNR realiza ações de sensibilização e faz a elaboração e aplicação de programas de prevenção criminal, sendo assim possível informar toda a população, com principal destaque para o contacto com a população mais vulnerável, contribuindo, assim, para a segurança da mesma. As redes sociais, os meios de comunicação em geral, as ações de sensibilização em Juntas de Freguesias e escolas e o policiamento de proximidade, são as formas mais utilizadas para contactar com a população, sendo estas assim, alertas para este tipo de criminalidade em todo o território nacional.

No que diz respeito à QD.2 "De que forma as burlas são cometidas pelos autores (métodos, tipos)?", foram identificados 4 métodos. A característica comum a todos os métodos é a compra e venda de produtos *online*, utilizados como "isco" para a realização do ilícito. Os métodos são cedência dos dados do cartão da vítima; cedência dos dados do cartão da vítima e respetivos códigos de levantamento; método de *smishing* e método de *phishing*- falso serviço OLX. A falta de conhecimento das plataformas usadas *online*, a necessidade que vítima tem em vender os produtos e a facilidade que o agente criminoso proporciona ao processo, são os fatores mais decisivos para que o ilícito seja consumado.

No primeiro método são obtidos de forma ilícita os dados do cartão bancário da vítima, sendo o próprio burlão a associar os dados da conta da vítima ao seu número de telemóvel. No segundo método, o burlão conduz a vítima até um multibanco, onde é a própria que faz a associação dos dados. No terceiro método, o método de *smishing*, é utlizada uma plataforma de mensagens, através do qual é enviado um *link* que dá acesso a um *site* simulado, que aparenta ser do conhecido do lesado, onde é feito o preenchimento dos dados deste que são utilizados posteriormente, para a realização da burla. No último método, o método de *phishing*, similar ao processo do método de *smishing*, e diferente apenas pelo facto de a mensagem enganadora ser enviada antes por correio eletrónico, é introduzida uma falsa funcionalidade da plataforma *online*, onde são solicitados os dados da vítima que serão usados para realizar a burla.

Quanto à QD.3 "Qual a evolução que se tem observado nas burlas com recurso a plataformas eletrónicas de pagamento (MB Way)?", verifica-se que, tal como na sociedade em geral, a evolução da internet é constante, pelo que os métodos utilizados estão em constante alteração e os criminosos vão encontrando alternativas aos que já conseguem ser facilmente identificadas pelas forças de segurança. É necessária uma contante atualização por parte das autoridades e consequente formação dos militares. Só assim, será possível dar resposta a todos os pressupostos resultantes deste tipo de ilícitos.

Como resposta à QD.4 "De que modo a estrutura de investigação criminal da GNR, investiga / combate o crime de burla cometido através da aplicação MB Way e que métodos mobiliza na sua prática?", o processo de investigação tem início no momento de receção da queixa, seguindo-se a atribuição de competência de investigação por parte do Ministério Público. Posteriormente, inicia-se a fase de inquérito onde é efetuado o processo de recolha da prova, que nestes casos é na sua maioria prova de caráter digital. Internamente, a GNR desenvolveu instruções técnicas, através da DIC, onde são explanados os procedimentos a adotar pela estrutura de investigação criminal. Após a recolha de todos os elementos de prova, dá-se então início à análise da informação recolhida, de forma a solucionar o ilícito.

Em resposta à QD.5 "De que forma o enquadramento legal dos crimes de burla realizados através da aplicação MB Way implica a investigação?", as competências de investigação estão previstas na LOIC. No entanto, a tipificação destes ilícitos não é estanque, originando assim a atribuição da investigação a diferentes OPC. A tipificação é realizada pelo Ministério Público, que após analisar todos os pressupostos faz a

atribuição da investigação ao OPC competente. Tal facto gera uma dispersão dos processos, não existindo, muitas vezes, coordenação e articulação nas investigações.

Relativamente à QC "Qual a capacidade da GNR para prevenir e investigar o crime de burla cometido através de plataformas eletrónicas de pagamento (MB Way)?", com a presente investigação foi possível observar que a estrutura de investigação criminal da GNR está em permanente atualização, para que a resposta a este tipo de ilícitos seja o mais célere e competente possível, tanto na área da investigação como na área da prevenção. O trabalho desenvolvido no combate a este tipo de ilícitos é permanente. No entanto, ainda existem lacunas, nomeadamente na capacidade de acompanhamento da evolução dos novos métodos e na formação necessária, dos militares, para que a análise de informação resultante deste tipo de ilícitos, seja realizada na plenitude de capacidades.

Com este tipo de criminalidade a aumentar de ano para ano, de acordo com os dados dos RASI, o trabalho desenvolvido pela GNR é crucial para que esta tendência seja contrariada. Tal já é observado com processos a serem concluídos com sucesso, sendo os infratores julgados.

Importa referir a concordância entre os dados obtidos através da revisão bibliográfica e consequente análise documental e os dados obtidos através dos inquéritos por entrevista e os inquérito por questionário. Desta forma, é possível concluir que a GNR tem conhecimento do que são burlas cometidas através de plataformas eletrónicas de pagamento e, consegue identificar alguns dos procedimentos a adotar no momento de receção de uma denúncia. Pode ainda concluir-se, que a maioria dos militares tem conhecimento dos modos de atuação adotados pelos burlões.

Um dos pontos negativos traduz-se na falta de conhecimento dos militares das ações de prevenção desenvolvidas pela GNR, não sendo capazes de identificar estas ações. No entanto, na área da prevenção criminal praticamente todos os inquiridos consideram pertinente haver ações de sensibilização nesta área. Outro aspeto negativo, consiste na formação dos militares, que se demonstra insuficiente para dar resposta a todas as problemáticas originadas por este tipo de ilícito, a adaptação por parte dos criminosos aos métodos utilizados pelas forças de segurança para travar a prática de crimes é constante, existindo uma alteração sistemática dos métodos utilizados. Também, a legislação em vigor está em atualização permanente, o que exige dos militares um acompanhamento sistemático, para que se encontrem sempre atualizados.

A principal limitação a esta investigação traduz-se na dificuldade de recolha de um maior número de respostas aos inquéritos por entrevista, devido à limitação temporal

para realizar o trabalho. No que às recomendações diz respeito, a investigação permitiu demonstrar o trabalho já realizado e o que poderá ser melhorado na área da investigação e prevenção dos ilícitos em estudo. Por outro lado, importa destacar, como aspeto positivo, a atualidade do tema, que permitiu a realização de um estudo enriquecedor, possibilitando um conhecimento aprofundado sobre a legislação em vigor, os modos de atuação usados para a prática dos ilícitos e as capacidades da GNR na investigação e prevenção deste fenómeno.

Como futuras investigações, é sugerido o estudo aprofundado do perfil da vítima e dos burlões, para que desta forma, o trabalho desenvolvido seja o mais direcionado possível, proporcionando uma atuação da GNR direcionada e consequentemente mais capaz.

BIBLIOGRAFIA

Artigos científicos, obras literárias e outros documentos

Abdalla. R. (2017, julho). A evolução dos meios de pagamento, da pré-história à Internet das coisas. In Canaltech. Disponível em https://canaltech.com/mercado/a-evolucao-dos-meios-de-pagamento-da-pre-historia-a-internet-das-coisas-97812/

Alerta Gnr: Usa Mbway? Atenção Às Burlas No Olx E Custo Justo. Disponível em https://pplware.sapo.pt/informacao/alerta-gnr-usa-mbway-atencao-as-burlas-no-olx-e-custo-justo/

Alkaabi, Ali, Mohay, George M., McCullagh, Adrian J. e Chantler, Alan N. (2010). Dealing with the Problem of Cybercrime. Conference: Digital Forensics and Cyber Crime- Second International ICST Conference, Abu Dhabi, Emirados Árabes Unidos. Disponível em https://www.researchgate.net/publication/221511094_Dealing_with_the_Problem_of_Cybercrime

Almeida, I. (2014). A Prova Digital. (Tese de Mestrado em Ciências Jurídicas). Universidade Autónoma de Lisboa, Lisboa, Portugal.

Alves, D. (2017). E- commerce: Um novo Caminho para o Método de Pagamento (Tese de Mestrado em Gestão dos Sistemas de Informação). Instituto Superior de Economia e Gestão, Lisboa, Portugal.

Alves, D. (2017). Métodos, Instrumentos e Técnicas de recolha de dados. Disponível em https://cienciaeeducacao.com/2017/11/24/metodos-instrumentos-e-tecnicas-de-recolha-de-dado/

Amor, D. (2000). A (R)Evolução do E-business (1ª Ed). São Paulo: Makron Books.

Araújo, H. & Faria, L. (2007). Tecnologia e Sociedade: Tecnologia, humano e pós-humano, (1ª ed.). Universidade Católica, Lisboa.

Associação Portuguesa de Bancos [APB] (2017). SMSs de Phishing. Disponível em https://www.apb.pt/content/files/Smishing_PT.pdf

Bardin, L. (1977). Análise de conteúdo. Lisboa: Edições 70.

Beattie, A. (2021, setembro). The Pioneers of Financial Fraud. Investopidia. Disponível em https://www.investopedia.com/articles/financial-theory/09/history-of-fraud.asp

Biblioteca do Instituto Superior Técnico [BIST] (2015). Investigação Científica. Disponível em

https://bist.tecnico.ulisboa.pt/files/sites/37/Investiga%C3%A7%C3%A3 o-Cient%C3%ADfica.pdf

Borg, W. & Gall, M. (2002). Educational research: An introduction (7ª ed.) Nova Iorque: Longman

Brayman, A. (2012). Social research methods (4ª ed.). Oxford University Press

Brenner, S. W. (2006). Cybercrime jurisdiction. Crime Law Soc Change 46, 189–206. https://link.springer.com/article/10.1007/s10611-007-9063-7

Carvalho, L. (2015). Sebenta de Apoio: Metodologias e Técnicas de Investigação. Universidade Aberta. Lisboa, Portugal.

Comissão Europeia (2021). Eletronic Payment. Disponível em https://ec.europa.eu/growth/sectors/tourism/business-portal/financing-your-business/ele ctronic-payment_en

Correia, P. M. A. R., & Jesus, I. O. A. (2016, maio). Combate às Transferências Bancárias Ilegítimas pela Internet no Direito português: entre as experiências domésticas e políticas globais concentradas. Revista DireitoGV

Costa, C. (2017). As proibições de prova e a prova digital- aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade. (Tese de Mestrado em Direito Judiciário). Universidade do Minho, Braga, Portugal.

Costa, F. F. (1998). Algumas reflexões sobre o estudo dogmático chamado "Direito Penal Informático" (1ª ed.). Coimbra Editora, Coimbra, Portugal.

Deco Proteste (2019). MB Way para pagar compras e transferir dinheiro com o telemóvel. Disponível em MB Way para pagar compras e transferir dinheiro com o telemóvel (proteste.pt)

Dias, J. F. (1999). Comentário Conimbricense do Código Penal- Tomo II (1ª ed.). Coimbra Editora, Coimbra, Portugal.

Diogo Oliveira. Acedido a 25 de fevereiro de 2022 em https://www.publico.pt/2020/04/09/sociedade/noticia/confinamento-estimula-burlas-digitais-mbway-comum-1911690

Gauthier, B. (2003). Investigação Social: Da problemática à colheita de dados (3ª ed.). Loures: Lusiciência.

Gil, A. (2008). Métodos e técnicas de pesquisa social. 7ª Edição. São Paulo, Brasil: Atlas.

Gnr Alerta Para Diferentes Burlas Através De MB Way SÁBADO. Acedido a 25 de fevereiro de 2022 em https://www.sabado.pt/portugal/detalhe/gnr-alerta-para-diferentes-burlas-atraves-de-mb-way

Guarda Nacional Republicana [GNR] (2022). Burlas MB Way. Guarda Nacional Republicana, Lisboa, Portugal.

Guarda Nacional Republicana [GNR] (2022). Burlas. Disponível em https://www.gnr.pt/Cons_Burlas.aspx

Guerra, I. (2006). Pesquisa Qualitativa e Análise de Conteúdo: Sentidos e Formas de Uso. Estoril: Princípia.

Jeová, M. (2016). Conceitos Básicos de Amostragem. Disponível em https://pet-estatistica.github.io/site/download/posts/postJEOVA.html

Jung, C. (2009). Metodologia Científica e tecnológica. Disponível em https://scholar.google.com/citations?view_op=view_citation&hl=th&user=rRgZqU4AAAAJ&citation_for_view=rRgZqU4AAAAJ:OU6Ihb5iCvQC

Justiça.gov.pt (2022, maio). Portugal assina segundo protocolo adicional à Convenção sobre Cibercrime. Disponível em https://justica.gov.pt/Noticias/Portugal-assina-segundo-protocolo-adicional-a-Convencao-sobre-Cibercrime

Lapa, T. (2021). O omnicanal- Um estudo de caso de plataformas de comércio eletrónico dos retalhistas alimentares em Portugal (Tese de Mestrado). Instituto Superior de Contabilidade e Administração do Porto, Politécnico do Porto, Porto, Portugal.

Marques, P. (2013). Informática Forense. (Tese de Mestrado em Segurança em Sistemas de Informação). Universidade Católica Portuguesas, Faculdade de Engenharia, Lisboa, Portugal.

Mastercard. (2022, fevereiro). About Mastercard: Who We Serve. Site Mastercard. Disponível em https://www.mastercard.us/en-us/vision/who-we-are.html

Matos, J. (2015). Análise documental. Disponível em http://www.sabercom.furg.br/bitst

MB Way (2022). Perguntas Frequentes. Disponível em https://www.mbway.pt/perguntas/

Mello, R. (2018). Noção de Amostragem. Disponível em https://www.academia.edu/40070657/UNIVERSIDADE_FEDERAL_DO_ESP%C3%8DRITO_SNATO_CENTRO_DE_CIENCIAS_AGR%C3%81RIAS_E_ENGENHARIAS_DEPARTAME NTO_DE_ENGENHARIA_RURAL_-CCAE_RAYANE_LUIZA_DA_SILVA_DE_MEL LO

Multibanco [MB] (2022). Levantamentos. Disponível em https://www.multibanco.p/operacoes/levantamento/

Negri, P. (2014, janeiro). Como aconteceu a evolução dos meios de pagamento?. Disponível em https://www.iugu.com/blog/evolucao-dos-meios-de-pagamento

Neves, J. (2006). As ciências sociais: os prossupostos teóricos dos investigadores. Disponível em https://metodologia.blogs.sapo.pt/43718.html

Oliveira, D. (2020). Confinamento Estimula As Burlas Digitais; Mbway É O Mais Comum. Público.

Pardal, L. & Lopes, S. (2011). Métodos e técnicas de investigação social. Porto: Areal Editores.

Pessoa, F. (1976). *A Carta Mágica* (1ª ed.). Diabril, Lisboa Portugal.

Portal da Queixa. Burlas MB WAY. Acedido a 25 de fevereiro de 2022 em https://portaldaqueixa.com/brands/mb-way/complaints/mb-way-burla-29-31675819

Prodanov, C. & Freitas, E. (2013). Metodologia do trabalho científico: Métodos e técnicas da pesquisa e do trabalho académico. Disponível em https://books.google.pt/books?hl=ptPT&lr=&id=zUDsAQAAQBAJ&oi=fnd&pg=PA13&dq=m%C3%A9todo+dedutivo+&ots=dc5adwcDO&sig=gtOYFCDJAgMqzSoh6BBaL4_53FM&redir_esc=y#v=onepage&q=m%C3%A9todo%20dedutivo&f=false

Quivy, R. & Campenhoudt, L. (1992). Manuela de Investigação em Ciências Sociais. Lisboa: Gradiva

República Portuguesa [RP] (2010). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.parlamento.pt/Documents/XIILEG/RASI_%202010.pdf

República Portuguesa [RP] (2011). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.historico.portugal.gov.pt/media/555724/2012-03-30_relat_rio_anual_seguran_a_interna.pdf

República Portuguesa [RP] (2012). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.historico.portugal.gov.pt/pt/o-governo/arquivo-historico/governos-constitucionais/gc19/os-ministerios/mai/documentos-oficiais/20130327-rasi-2012.aspx

República Portuguesa [RP] (2013). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.historico.portugal.gov.pt/media/12362963/rasi-2013.pdf

República Portuguesa [RP] (2014). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.parlamento.pt/Documents/XIILEG/Abril_2015/relatorioseginterna2014.pdf

República Portuguesa [RP] (2015). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.portugal.gov.pt/pt/gc21/comunicacao/documento?i=20160331-pm-rasi

República Portuguesa [RP] (2016). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.portugal.gov.pt/pt/gc21/comunicacao/documento?i=20170331-pm-rasi-2016

República Portuguesa [RP] (2017). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.portugal.gov.pt/pt/gc21/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2017

República Portuguesa [RP] (2018). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.portugal.gov.pt/pt/gc21/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2018

República Portuguesa [RP] (2019). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.portugal.gov.pt/pt/gc22/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2019-

República Portuguesa [RP] (2020). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.portugal.gov.pt/pt/gc22/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2021

República Portuguesa [RP] (2021). Relatório Anual de Segurança Interna (RASI). Disponível em https://www.portugal.gov.pt/pt/gc23/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2021

Ribeiro, L. (1998). A História da Internet. Disponível em https://paginas.fe.up.pt/~mgi97018/historia.html

Ribeiro, M. (2015). Cibercrime e a Prova Digital (Tese de mestrado em Ciências Jurídico-forenses). Instituto Superior Bissaya Barreto, Aveiro, Portugal.

Rocha, M. (2019). As novas tecnologias e a investigação criminal: a obtenção de prova. Instituto Superior de Ciência Policiais e Segurança Interna, Lisboa, Portugal.

Romão, A. (2021). Definição, Delimitação e Problema. Academia Militar, Lisboa, Portugal.

Sá, P., Costa, A. & Moreira, A. (2021). Reflexões em torno da Metodologias de Investigação, recolha de dados- Volume 2. Aveiro: Universidade de Aveiro

Santos, C. (2005). O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos. Coimbra: Coimbra Editora.

Santos, M. (2020). O Fenómeno do Cibercrime, Prova Digital e Dificuldades Da Investigação. Portalegre, Portugal.

Severino, A. (2013). Metodologia do Trabalho Científico (21º edição). São Paulo, Brasil: Cortez Editora.

SIBS- Forward Payment Solutions [SIBS] (2020). Pagamentos Digitais: Evolução e Tendências. Lisboa, Portugal: SIBS.

SIBS. (2019, setembro). Multibanco. Site SIBS. Disponível em https://www.sibs.com/marcas/multibanco/

Sieber, U. (1992). Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique. Revue Internationale de Droit Penel, Wurzbourg, Alemanha.

Silva, A. & Pinto, J. (2014). Metodologia das Ciências Sociais. Edições Afrontamento, Porto.

Silva, M., Costa, E., Costa, A. (2013). Conhecimento Científico e Sensu Comum: Uma Abordagem Teórica. VII Colóquio Internacional São Cristóvão. Disponível em https://ri.ufs.br/bitstream/riufs/9718/96/95.pdf

Sousa, J., & Baptista, C. (2011). Como fazer investigação, dissertações, teses e relatórios. Lisboa: Pactor.

Souza, F. (2016, 26 de dezembro). Qualitativa: Semelhanças entre metodologias e metodologias. Universidade de Aveiro, Aveiro, Portugal.

Stefan F., William H. D. e Helen Margetts (2010). Mapping and Measuring Cybercrime. Oxford Internet. Institute University of Oxford. https://poseidon01.ssrn.com/delivery.php?ID=921074095001012090064065001070115089123035081036074048121092004014110001030092011026005050101 01

2008098014079004118094099123089102059062029068030029103001001016127018084063091127101121010071020094088104007112087089123006003001065087029103031067000127&EXT=pdf&INDEX=TRUE

The Supervisor of Banks (2021, setembro). Proper Conduct of Banking Business. Disponível em https://webcache.googleusercontent.com/search?q=cache:7jFpt2KhgUE J:https://www.boi.org.il/en/BankingSupervision/SupervisorsDirectives/ProperConduct OfBankingBusinessRegulations/367_et.pdf+&cd=1&hl=pt-PT&ct=clnk&gl=pt

Torga, M. (2011). Diário- Vols XII a XVI. Lisboa: Dom Quixote.

Ureche, O. & Plamondom, R. (2000). Digital Payment Systems for Internet Commerce: The state of the art. École Polytechnique de Montréal. Canada.

Vala, J. (2014). A análise de conteúdo. In Silva A. S. & Pinto, J. M. (Orgs). Metodologia das ciências sociais. Porto: Edições Afrontamento.

Vidigal, I. (2012). As Políticas de Combate ao Cibercrime na Europa. (Tese de Mestrado em Políticas Europeis). Universidade de Lisboa, Instituto de Geografia e Ordenamento do Território, Lisboa, Portugal.

Vidigal, I. M. A. (2012). As Políticas de Combate ao Cibercrime na Europa (Tese de Mestrado). Repositório Institucional da Universidade de Lisboa. https://repositorio.ul.pt/bitstream/10451/20508/1/igotul003907_tm.pdf

VISA. (2022, fevereiro). História dos cartões de crédito Visa: A nossa atividade. Site VISA. Disponível em https://www.visa.pt/sobre-a-visa/a-nossa-empresa/historia-dos-cartoes-de-credito-visa.html

Weeks, L. (2015, fevereiro). How Scams Worked In The 1800s. NPR History Dept.. Disponível em https://www.npr.org/sections/npr-history-dept/2015/02/12/385310877/how-scams-worked-in-the-1800s?t=1641479257832

Weisman, S. (2020, agosto). The History of Ponzi Schemes Goes Deeper Than the Man Who Gave Them His Name. TIME. Disponível em https://time.com/5877434/first-ponzi-scheme/

World Bank (2016). Innovation in Electronic Payment adoption: The case of small retailers. World Bank publications.

Yingyu, Z. (1617). A New Book for Foilinf Swindles, Based on Wordly Expirience (1º Edição). Fujian, China: Selections from a Late Ming Collection.

Legislação, Jurisprudência e outros documentos

Assembleia da República [AR]. (1995). DL n.º 47344/66, de 25 de novembro: Código Civil. Diário da República, nº 274/1966, Série I.

Assembleia da República [AR]. (1995). DL n.º 48/95, de 15 de março: Código Penal. Diário da República, série I-A, n.º 63.

Assembleia da República [AR]. (2008). Lei nº 49/2008, de 27 de agosto: Lei de Organização da Investigação Criminal. Diário da República nº 165/2008, Série I.

Assembleia da República [AR]. (2009). Lei nº 109/2009, de 24 de fevereiro: Lei do Cibercrime. Decisão Quadro nº 2005/222/JAI, do Conselho.

Código do Processo Penal. Revoga o Decreto-Lei n.º 16489, de 15 de fevereiro de 1929. Diário da República, série I, n.º 40.

Conselho Europeu [CE] (2009). Lei 109/ 2009: Lei do Cibercrime. Diária da República nº 179/2009, Série I.

Conselho Europeu [CE] (2009). Resolução da Assembleia da Republico nº 88/2009: Convenção sobre o cibercrime. Decreto do Presidente da República nº 91/2009.

Conselho Europeu [CE] (2019). Aderindo à Convenção de Budapeste sobre Cibercrime: Benefícios [Sessão de Conferência]. Convenção sobre o Cibercrime, Estrasburgo, França. https://rm.coe.int/cyber-buda-benefits-pt-final/1680a0544d

Direção de Investigação Criminal [DIC] (2020). Instrução Técnica MB Way. Guarda Nacional Republicana, Lisboa, Portugal.

Instrução nº 1/2020. Utilização fraudulenta da aplicação MB WAY (Coordenação da atividade do Ministério Público)

Nota Prática nº 16/2020 (19 de março de 2020) – Jurisprudência sobre a Prova Digital. Ministério Público, Portugal.

Nota Prática nº 20/2020 (14 de maio de 2020) - Utilização Fraudulenta da Aplicação MB WAY. Ministério Público, Portugal.

Nota Prática nº 22/2021 (4 de março de 2021) - Utilização Fraudulenta da Aplicação MB WAY. Ministério Público, Portugal.

Recomendação 1/2021 (2021). Burlas MB Way efetuadas por transferência bancária – Decisões já proferidas em conflito negativo de competência- Posição da Comarca de Portalegre. Ministério Público, Portugal.

APÊNDICES

Apêndice A- Inquérito por Entrevista-As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos

ACADEMIA MILITAR

As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos

Autor: Aspirante-Aluna Cavalaria da GNR Ana Marta de Sousa e Silva

Orientadora: Professora Doutora Sofia de Vasconcelos Casimiro

Coorientador: Tenente-Coronel Infantaria da GNR Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, junho de 2022

CARTA DE APRESENTAÇÃO

A presente investigação insere-se no âmbito do Relatório Científico Final do Trabalho de Investigação Aplicada, do mestrado em Ciências Militares, na Especialidade de Segurança da Academia Militar, que está subordinado ao tema: "As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos".

A finalidade desta investigação é identificar os contornos dos ilícitos relacionados com as burlas com recurso a plataformas eletrónicas de pagamento, nomeadamente os métodos utilizados e o enquadramento legal do tema. Adicionalmente, este trabalho de investigação pretende também perceber e abordar a vertente operacional da GNR sob dois prismas: inicialmente, sob o prisma da investigação criminal, analisando as respetivas competências e capacidades da GNR neste tipo de ilícito criminal, nomeadamente os seus constrangimentos e oportunidades; e, posteriormente, sob o prisma da prevenção criminal, analisando as competências e capacidades da GNR para sensibilizar a população nesta matéria, nomeadamente através dos programas de prevenção criminal desenvolvidos na área do policiamento comunitário.

Tendo em conta os objetivos da investigação, a realização de questionários por entrevista torna-se fundamental para recolher dados que possam dar resposta às questões levantadas ao longo da mesma e relacionar factos, ideias e opiniões que constituam doutrina de investigação. As entrevistas serão realizadas a militares de Secções de Inquéritos dos Comandos Territoriais, de diversos Núcleos de Investigação Criminal da GNR e a militares da SIIC dos Comandos Territoriais.

Face ao anteriormente explanado, solicito a Vossa Excelência que responda à entrevista sobre a temática em investigação, pois a sua colaboração será essencial para atingir os objetivos propostos.

Grata pela colaboração e disponibilidade.

Atenciosamente,

Ana Marta de Sousa e Silva

Aspirante Cavalaria da GNR

1. ENQUDRAMENTO

As denúncias por práticas fraudulentas relacionadas com a aplicação digital MB Way, geralmente enquadráveis no crime de burla, têm vindo a aumentar, segundo os dados partilhados pelas forças de segurança ao Ministério Público.

A pertinência da temática é reconhecida, sendo este tipo de crime mencionado na Lei nº 55/2020, de 27 de agosto, que define as prioridades de política criminal para o biénio 2020-2022, este tipo de crime é mencionado como um crime de prevenção prioritária, devido à necessidade de proteger as potenciais vítimas.

O ilícito envolve uma abordagem que explora de uma forma ardilosa o desconhecimento que os cidadãos têm sobre o funcionamento deste tipo de plataformas digitais, permitindo obter indevidamente valores monetários, por vezes de elevado montante.

Devida à não tipificação concreta da Burla MB Way, muitas vezes a sua classificação e consequente atribuição de investigação é dúbia, o que gera alguma discórdia e aplicação de critérios diferentes tornando a presente investigação pertinente para que seja possível encontrar respostas**.**

2. ENTREVISTA

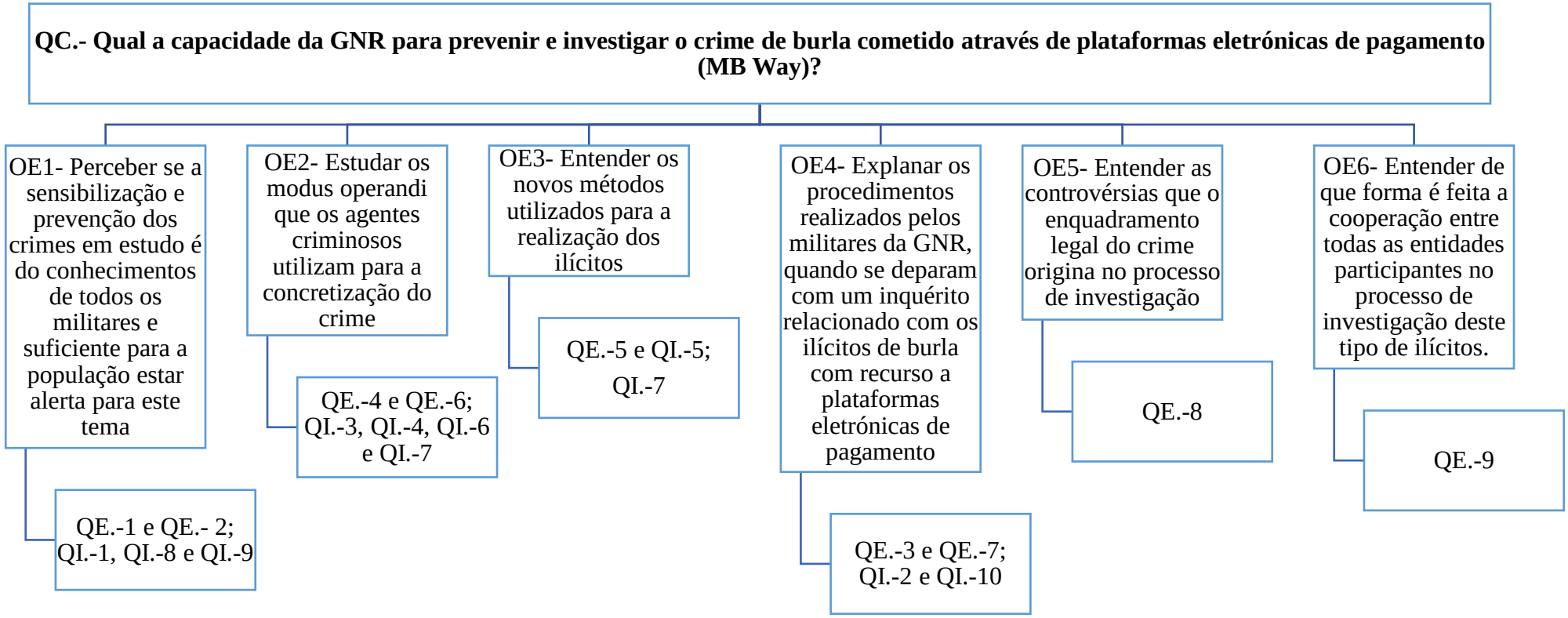
As respostas dadas às questões expostas seguidamente, servirão para alcançar os objetivos propostos para a presente investigação, deste modo, solicito que sejam o mais completas e pormenorizadas possíveis. As respostas apenas serão utilizadas para objeto de estudo desta investigação, pelo que solicito a autorização para que as mesmas sejam utilizadas e transcritas para a realização da investigação.

Nos casos em que a sensibilidade da informação partilhada assim o exija, as respostas dadas poderão ser consideradas como classificadas. Se for do seu interesse, a presente investigação também poderá ser partilhada após o seu término, assim que for aprovada.

Entrevista aos militares do NIC da GNR/ Militares da SIIC dos Comandos Territoriais

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?
2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?
3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?
4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?
5. Existem algum padrão entre os tipos de atuação dos burlões?
6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?
7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?
8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?
9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

Apêndice B- Matriz de Investigação



Capítulos: 1.1 Evolução da Convenção de Budapeste; 1.2 Enquadramento dos ilícitos penais cometidos através de plataformas eletrónicas de pagamento; 1.2.1 Crime de Burla, Artigo 217º Código Penal; 1.2.2 Crime de Burla Qualificada, Artigo 218º Código Penal; 1.2.3 Crime de Burla Informática e nas comunicações, Artigo 221º Código Penal; 1.2.4 Crime de Falsidade informática, Artigo 3º Lei do Cibercrime; 1.2.5 Crime de Acesso Ilegítimo, Artigo 6º Lei do Cibercrime; 1.2 Evolução da Burla (Conto do vigário por via digital); 1.3 Evolução dos crimes de burla em Portugal de acordo com os RASI (2014-2021); 1.4 Acompanhamento legislativo da evolução da sociedade tecnológica; 2.1 Evolução dos métodos de pagamento; 2.2 Banca eletrónica e E- commerce, enquadramento legal; 2.3 Mb Way em Portugal, soluções e problemas da plataforma; 3.1 Os tipos de ilícitos praticados com recurso a plataformas eletrónicas de pagamento; 3.2 Capacidades da GNR para investigação de crimes de burlas com recurso a plataformas eletrónicas de pagamento; 3.3 A problemática da Prova Digital, 3.4 Programas de prevenção criminal de policiamento comunitáriona prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento; 3.5 A posição do Ministério Público na temática das Burlas com recurso a plataformas eletrónicas de pagamento.

Figura nº 11- Matriz de Investigação
Fonte: Elaboração Própria

Apêndice C- Entrevistas aos Militares da GNR- Entrevistado 1

Função: Elemento da SIIC

Posto: Sargento-Ajudante

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

A GNR utiliza as redes sociais como o Facebook, o Instagram, o Twiter e outras para divulgar os riscos de fraude nas transações por meios eletrónicos, divulgando os modus operandi mais usuais e os novos modus operandi que vão emergindo a cada dia.
No entanto, existe consciência que esta informação não chega a toda a população, existindo ainda muitos infoexcluídos, devido ao enorme envelhecimento da população com mais de 22% da população com 65 e mais anos e um índice de envelhecimento de 161 idosos por cada 100 jovens, bem como pelos níveis de escolaridade dos habitantes, especialmente com mais de 50 anos, com a maioria a terem apenas o primeiro ciclo de ensino básico, a não terem qualquer grau de ensino ou a serem analfabetos. Note-se que mesmo considerando toda a população, em 2011, mais de 5% eram analfabetos, mais de 10 % não tinham qualquer grau de ensino e mais de 27% apenas tinham o primeiro ciclo.

Por isso, as ações de sensibilização levadas a cabo pelos Comandantes de Destacamento e pelas Secções Prevenção Criminal e Policiamento Comunitário (SPCPC) nas Juntas de Freguesia rurais e urbanas, nas coletividades e noutros locais são fundamentais para alertar as populações sobre estes tipos de criminalidade emergente e das formas como devem proceder para evitar cair no velho conto do vigário agora camuflado através das tecnologias de informação.

Por outro lado e também muito importante - fundamental mesmo, ou basilar a toda a atuação da Guarda - é manter os militares dos Postos Territoriais a par destes tipos de burlas, além dos militares das SPCPC, pois são eles que contactam diariamente com a população e podem levar até às pessoas mais vulneráveis os alertas para não se deixarem enganar, mostrando que a Guarda está próxima, não caindo no erro de alarmar demasiado as pessoas e assim poder aumentar o sentimento de insegurança, o que também acaba por ser prejudicial para as populações em termos sociais.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Sei que procuram manter-se atualizados para poderem divulgar este tipo de ilícitos e assim prevenir algumas burlas junto daqueles que entendem poder ser mais suscetíveis a este tipo de criminalidade. Sei também que fazem algumas ações de sensibilização da população, no entanto, as medidas preventivas e restritivas no âmbito da pandemia por Covid vieram limitar a atuação destas equipas em geral, por um lado, e, por outro, as pessoas têm sentido necessidade de recorrer às plataformas digitais para comprar e vender coisas, o que tem transformado o terreno fértil, isto é, o ambiente favorável ao crescimento deste tipo de criminalidade. Sem dúvida que estas Secções podem ter um papel preponderante no alerta deste e de outros tipos de criminalidade, mais tradicional ou emergente. No entanto, apesar do seu caráter mais generalista, é nos Postos Territoriais que continuam a estar os militares que de uma forma mais terra a terra lidam diariamente com as populações e por isso, devem também estar sensibilizados para estas temáticas a fim de as poderem passar de uma forma natural e abrangente.

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

Sim, mas no meu caso não sou eu que recebo as denúncias, uma vez que me cabe fazer a análise dos processos já no decurso das investigações criminais. No entanto, desperto para as necessidades da investigação e da análise, num espírito *intelligence-led policing*, logo no início de 2020, quando as burlas MB Way estavam a iniciar a forte escalada, elaboramos um relatório a alertar o escalão superior e o efetivo da Unidade, expondo o modus operandi utilizado, as vítimas habituais e os locais onde eram «caçadas» pelos delinquentes, por forma a possibilitar ao dispositivo a prevenção destes ilícitos, incluindo um anexo com as medidas imediatas e mediatas a ter em conta por quem recebe as queixas e por quem procede às investigações, respetivamente, já numa perspetiva de repressão / investigação criminal.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

O mais usual é pesquisarem pessoas que tenham artigos à venda em plataformas digitais como o Olx (maioria dos casos) ou outras, telefonando às pessoas manifestando interesse em adquirir os produtos, preferindo o pagamento por MB Way, na expectativa que as pessoas digam que não conhecem a aplicação, caso em que usam toda a manha para ludibriar as pessoas, prestando-se a ensinar as pessoas a fazer a transação, dizendo-lhes logo que não tem nada que saber, que basta irem a um multibanco e que lhes explicam mesmo por telefone como fazer e logo poderão confirmar que já têm o dinheiro na conta. Na expetativa de vender os artigos e receber o dinheiro, as pessoas desconhecedoras da aplicação e mais incautas, acabam por seguir as indicações dos burlões que as levam a dar acesso às suas contas bancárias através dos telemóveis dos burlões que depois fazem levantamentos bancários (sujeitos a limites diários de €400,00) e transferências bancárias (geralmente sem limite) através do telemóvel, só descobrindo mais tarde que afinal não foram depositadas quaisquer quantias, mas sim levantadas ou transferidas pelos burlões.

Depois há o método aplicado quando a vítima tem a aplicação ativa, pelo que o suspeito lhe pede o número de telemóvel associado e a informa que lhe vai fazer a transferência, dizendo à vítima que vai receber uma mensagem para confirmar o valor do pagamento, mas em vez disso, o burlão faz um pedido de transferência no valor acordado à vítima escrevendo na mensagem livre um texto do tipo "O MB Way recebeu ordem de transferência para o seu número no valor de €500. Aceita enviar o dinheiro para a sua conta?", sendo assim a vítima induzida a carregar no botão "Enviar dinheiro".

Já há outros métodos mais elaborados, mas este continua a ser o grosso das burlas ocorridas nesta Unidade.

5. Existem algum padrão entre os tipos de atuação dos burlões?

Sim, os burlões são geralmente das mesmas famílias e atuam em cascata, uns vão ensinando os outros das novas formas e depois todos vão replicando os modus operandi. Suspeita-se inclusive que existe organização criminosa e divisão de dividendos entre os membros. O processo é geralmente associado a uma «caça» ou «pesca» de vítimas em *sites* de vendas *online*, independentemente do local ser no norte ou no sul do país, fazendo centenas de telefonemas através da utilização de cartões descartáveis que são utilizados até que uma ou duas vítimas «caia na rede», pois aí esvaziam a conta dessas vítimas

através de levantamentos ou transferências – utilizando contas de pessoas terceiras que se sujeitam a receber e levantar o dinheiro das contas a troco de uma percentagem, ou de droga ou outras situações – e deitam fora esses cartões de telemóvel e continuam a fazer telefonemas com outros cartões descartáveis. Em termos organizativos até há já vários níveis de atuação dos criminosos: uns fazem telefonemas - geralmente pessoas mais bem-falantes e persuasivas – outros fazem os levantamentos preferencialmente em caixas ATM sem câmaras de vigilância, outros deixam utilizar as suas contas, etc. Note-se que os que fazem os telefonemas podem estar fisicamente distantes dos seguintes, pois geram códigos, enviam aos outros que fazem os levantamentos nos ATM (…).

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

A vítima mais comum é a pessoa que não conhece a aplicação MB Way e que na expetativa de vender algum determinado artigo se deixa enganar por alguém que do outro lado da linha de uma forma persuasiva se disponibiliza a dar as indicações para a vítima receber o dinheiro, alegando que depois uma transportadora ou o próprio, passa por casa da vítima a buscar o artigo ou artigos. Geralmente escolhem os novos anunciantes, pois os mais antigos já foram vítimas de burla ou de várias tentativas de burla e como a maioria das plataformas de vendas *online* referem há quanto tempo o anunciante vende naquela plataforma é fácil "lançar a rede e tentar pescar a vítima". As pessoas de mais idade e com menores habilitações também são mais facilmente ludibriadas, embora neste caso concreto estejamos a falar de vítimas de todas as idades, com maior incidência de pessoas entre os 40 e os 60 anos. Isto porque de entre os mais vulneráveis são aqueles que já possuem alguns conhecimentos que lhe permitem tentar fazer vendas *online*. Quem conhece a aplicação já não se deixa enganar tão facilmente.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Sim, já está mais desperto para o fenómeno e tem inclusive emanado diversas orientações - Ordens de Serviço - para os magistrados a fim de fazer face de uma forma mais eficiente, concentrando as investigações nos DIAP.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Sim, no âmbito de orientações da Guarda e até das Ordens de Serviço do MP.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

A utilização de cartões descartáveis e de muitos telemóveis diferentes por parte dos burlões, dada a facilidade de aquisição e elevados «lucros» da atividade.

Os levantamentos em locais sem câmaras de vigilância e a utilização de máscaras (covid) e gorros ou casacos com capuz aquando dos levantamentos em multibancos com câmaras.

A enorme demora no fornecimento dos dados dos clientes por parte das operadoras de comunicações móveis e a deficiente informação, mesmo quando solicitado pelos magistrados do MP.

Idem por parte das entidades bancárias.

A não formalização de denúncias por parte de muitos lesados.

A utilização de intricados esquemas de transferências bancárias entre várias contas, incluindo de outros países, até chegar ao destinatário final.

Grande volume de processos-crime e relações entre processos que motiva incorporações que nunca mais acabam (processos com mais de 100 crimes incorporados, com dezenas de burlões e com centenas de contas bancárias, por exemplo).

Apêndice D- Entrevistas aos Militares da GNR- Entrevistado 2

Função: Chefe do NIC

Posto: Primeiro-Sargento

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

Divulgação /comentários em que a GNR aconselha o cidadão a que este tenha algum cuidado e atenção no momento de efetuar pagamentos por MB Way.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Desconheço.

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

N. de telemóvel que foi solicitado e extrato das contas a fim de tentar perceber para onde foi aquele movimento, ponto principal. De seguida tentar perceber se a pessoa que efetuou a burla deixou algum indício de onde possa ter estado podendo esta ter deixado cair alguma informação que possa ser seguida. Pois essa burla pode ter sido de uma pessoa de perto, algo que se nota algum conhecimento sobre o objeto, por ex.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

Em regra será o burlão um comprador de algo e quer pagar e o bem que a vítima detém, está em venda. Na conversa, o burlão consegue ludibriar a vítima, fazendo acreditar nesta ao ponto que quando lhe diz para colocar o n.º de telemóvel, a vítima coloca aquele que o burlão lhe vai dizer. Quando a vítima repara, quando assim o é, liga mas esta "burlão" já não tem o telemóvel ligado.

5. Existem algum padrão entre os tipos de atuação dos burlões?

Normalmente será este acima mencionado.

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

Não existe perfil, qualquer pessoa que não esteja com atenção será uma próxima vítima.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Relativamente ao MP, parece-me que este tipo de crime passou a estar centralizado num DIAP a fim de se poder efetuar alguma investigação que possa trazer resultados.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Desconheço, poderá cada comarca ter uma maneira de tratar esse tipo de crime.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

Por vezes as contas para onde vai esse dinheiro acabam por não ter uma identificação correta do tutelar.

Apêndice E- Entrevistas aos Militares da GNR- Entrevistado 3

Função: Elemento do NIC SIIC

Posto: Cabo

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

Ações de sensibilização, junto das populações mais idosas, escolas, etc, onde se encontrem maiores aglomerados de pessoas. Bem como de outras formas de divulgação da informação como acontecem esse tipo de burlas, e as formas de tentarem evitá-las.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Sim as secções de prevenção criminal, tem desenvolvido ações de esclarecimentos e divulgação desse tipo de crime, no sentido de a população estar informado dos eventuais riscos.

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

Após a receção da denúncia é necessário: obter descrição pormenorizada sobre os factos; obter cópia ou impressão do anúncio, a identificação da plataforma, o ID do anúncio e a referência do anúncio de venda colocado pela vítima; questionar a data e hora da colocação do anúncio e data e hora em que se recebe o contacto do autor do crime, normalmente o contacto é feito poucas horas após a colocação do anúncio.

Em relação ao suspeito: obter descrição sobre o interlocutor (características, homem, mulher, sotaque, erros na linguagem, nome, localidade, ou outras informações mesmo que falsas, permitem detetar coincidências noutras situações idênticas.

Em relação à vítima: informar/aconselhar as mesmas a não apagar os dados e registo dos telemóveis, sobretudo as mensagens SMS ou de correio eletrónico que tenham recebido ou enviado.

Se possível recolher imagens de todas as mensagens ou outros registos que estejam disponíveis nos telefones ou outros dispositivos do queixoso: n.º de telefone que o autor utilizou para o contacto, n.º de telefone inserido no ATM aquando a instalação da aplicação MB Way, indicando no caso de contacto telefónico se o mesmo é pertença da vítima ou do agente do crime; deve estar descrito o código PIN (código 6 dígitos) indicado pelo agente do crime, que foi utilizado pelo denunciante para adesão ao MB Way.

Se o contacto foi por correio eletrónico, indicar o endereço de e-mail do suspeito.

Identificação da conta e do/s cartão/ões bancário/s associado/s.

Identificação do ATM em caso de levantamento por parte do suspeito (local e entidade)

Obter o extrato de movimentos do cartão.

Diligenciar na preservação das imagens da ATM onde foram efetuados os levantamentos.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

Mantêm com a vítima contato com a intenção de adquirir o artigo que a mesma colocou à venda nas plataformas OLX, Custo Justo, etc. Mostrando-se interessado na compra e prático no pagamento, disponível para ajudar a vítima a receber o dinheiro, dando-lhe indicações de como o fazer, deslocar-se ao multibanco, aceder à aplicação, introduzir códigos, n.ºs de telemóvel, conforme tenha MB Way ou não, etc.

5. Existem algum padrão entre os tipos de atuação dos burlões?

Por norma os burlões não questionam muitas informações dos artigos à venda, ou seja, não regateiam valores, condições de entrega/levantamento, etc, mas sim facilmente aceitam as condições de venda que a vítima propõe, para que esta seja encorajada a vender e rapidamente a receber o dinheiro (coisa que depois não sucede e aí sim ocorre a burla).

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

São pessoas que têm algum artigo à venda nas plataformas OLX, Custo Justo, pessoas que tenham em outras plataformas ou redes sociais aluguer de imóveis, férias,

etc. Pessoas essas que não tenham MB Way ativo ou que o tenham, mas não sabem trabalhar com a aplicação.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Certamente não será ainda o desejado, mas sim com o crescimento deste tipo de crime, considero que o Ministério Público está mais sensibilizado e é mais célere no tratamento desses ilícitos.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Sim, aquando da comunicação desse tipo de crime e para a recolha de alguns dados que só o Ministério Público tem a possibilidade de ter acesso ou de o solicitar, terá de haver uma melhor comunicação para que o mesmo seja alertado em tempo útil e diligenciar nesse sentido.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

Dificuldades em obter informações bancárias (nomes de titulares das contas suspeitas, movimentos, etc). Tendo em conta a proteção de dados, prazos. Não existir captação de imagens, pois os suspeitos selecionam ATM que não possuam tal equipamento. Fornecimento por parte das operadoras da identificação dos titulares dos n.ºs de telemóvel suspeitos utilizados e respetivos IMEI(s).

Apêndice F- Entrevistas aos Militares da GNR- Entrevistado 4

Função: Elemento do NIC

Posto: Cabo

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

Divulgação das burlas cometidas através da plataforma MB Way nas redes sociais, em reportagens televisivas e outros meios de comunicação.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Penso que tenham sido ministradas sessões de esclarecimento junto da população mais idosa.

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

Verificar a existência de Imagens no local onde foi efetuado o Levantamento/Transferência/Pagamento (multibanco) e garantir a sua preservação;

Verificar no SIIOP-P se os números utilizados (o número que o suspeito utilizou para falar com a vítima e o número que a vítima associou ao MB Way) se encontram associados a alguém e em caso afirmativo mencionar essa informação no auto ou em aditamento;

Solicitar ao Lesado que peça junto do seu Banco a fim de ser anexado ao auto:

O contacto telefónico associado ao Levantamento/Pagamento;

Os Multibancos e locais onde foram efetuados os Levantamentos ou Pagamentos;

As lojas/locais onde foram efetuados os Pagamentos de Compras;

O IBAN e a identificação do respetivo titular da conta para onde foi efetuada a Transferência;

Se possível, que o banco, por suspeita de fraude, congele as contas para onde foram efetuadas as transferências (temos conhecimento de Bancos que tiveram esse

procedimento por iniciativa dos próprios serviços de segurança ou a pedido dos clientes burlados.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

a) O suspeito contacta a vítima com o intuito de adquirir o artigo pelo valor solicitado e insiste em pagar com a aplicação MB Way;

b) A vítima não tem a aplicação ativa, pelo que o suspeito se disponibiliza a ajudar, indicando à mesma para se deslocar a uma caixa multibanco;

c) A vítima, seguindo as indicações do suspeito, dirige-se a uma ATM, coloca o cartão multibanco e o pin, seleciona a opção MB Way, insere o n.º de telemóvel fornecido pelo suspeito e um código de 6 dígitos (que o suspeito recebe assim que a vítima confirma o número de telemóvel na opção MB Way);

d) O suspeito de imediato consegue aceder à aplicação, podendo transferir dinheiro para outras contas bancárias/telemóveis, efetuar pagamentos ou levantar dinheiro em qualquer caixa ATM.

5. Existem algum padrão entre os tipos de atuação dos burlões?

O facto de as vítimas terem bens à venda em plataformas como o OLX e de terem desconhecimento de como funciona o MB Way.

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

São na maioria pessoas com pouco conhecimento em relação a plataformas automáticas de pagamento ou na utilização de meios eletrónicos.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Sim. Foram criadas equipas específicas para o tratamento deste tipo de crimes.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Deve-se propor ao MP que oficialize a respetiva Operadora de Telecomunicações em causa no sentido de prestar informação sobre:

a) Identificação completa, incluindo os NIF, do(s) titular(es) do(s) número(s) utilizado(s);

b) Todos os números de telemóvel detidos por aqueles clientes (aquele NIF) naquela operadora nos 90 dias anteriores ao momento da burla e nos dias posteriores até à atualidade;

c) O(s) IMEI(s) associado(s) ao(s) número(s) utilizado(s) na burla e a todos os outros números detidos pelo mesmo cliente (NIF) naquele período;

d) Todos os outros números que tenham sido utilizados naquele(s) IMEI(s) nos 90 dias anteriores ao momento da burla e nos dias posteriores até à atualidade, bem como a identificação completa dos clientes (incluindo os NIF) a eles associados;

e) Informação da existência de carregamentos ou pagamentos desses cartões SIM que permitam a identificação de números de contas bancárias utilizadas e respetiva remessa de IBAN, a fim de posteriormente se poderem identificar os seus titulares.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

A maior dificuldade prende-se pelo facto de no caso dos levantamentos em caixas ATM não existirem captação de imagens, ou quando existem não permitirem a identificação cabal dos autores, uma vez que a dispersão territorial é muito grande.

Apêndice G- Entrevistas aos Militares da GNR- Entrevistado 5

Função: Elemento do NIC

Posto: Cabo

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

Segundo julgo, a GNR efetuou alguns comunicados e publicações em redes sociais, no intuito de alertar, na medida do possível, a população em geral sobre a problemática. Divulgou ainda os resultados de algumas ações efetuadas no territorial, quer ao nível de operações desenvolvidas e processos que se encontravam em investigação, quer de ações esporádicas desenvolvidas em flagrante delito.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Não sou conhecedor de qualquer trabalho desenvolvido quer pela GNR ou PSP, mas, no entanto, sei que existiram diversos trabalhos desenvolvidos, creio, pela Procuradoria-Geral da República, dando indicações quanto á temática e como abordá-la, ao nível do Ministério Publico.

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

Sim. Ao receber uma denúncia, para além de todos os elementos identificativos da vítima ou lesado e eventuais testemunhas, deverá ainda constar:

a) Qual a conta de onde foi retirada a quantia monetária (IBAN ou NIB);
b) Qual o cartão multibanco associado (número) á conta, há data dos factos;
c) O lesado deve assinar uma declaração de levantamento do sigilo bancário;
a) Posteriormente deverão ser solicitados os elementos SIBS, onde existe diversa informação importante;
b) Qual o grupo data hora dos movimentos;
c) Qual o local onde foram efetuados os levantamentos;

d) Proceder com o pedido de preservação de imagens de CFTV, caso existam;
e) Qual o número de telemóvel que contactou a vítima, ou seja, qual o número ou números utilizados pelo suspeito;
f) Elementos referentes á identificação do suspeito, nomeadamente se é masculino ou feminino, se tem sotaque, qual o nome com que se identificou, etc.;
g) Qual o número de telefone que associou ao serviço MB Way;
h) Qual o código de ativação, código PIN de acesso ao serviço;
i) Se esse código foi transmitido pelo suspeito, ou se foi o gerado pela plataforma;
j) No caso de existirem transferências para outra conta bancária, efetuadas pelo suspeito, apurar qual é o IBAN/NIB, ou número de telefone recetor.

Deverá SEMPRE, ter em atenção e apurar quem é o real ofendido, já que a pessoa burlada, que recebeu a chamada telefónica e foi ludibriada a aceitar o negócio e a receber o pagamento por MB Way, pode utilizar, por diversos motivos, uma conta facultada por terceiros.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

São conhecidas várias técnicas, mas habitualmente são utilizadas:

a) Numa primeira fase e após a vítima ter acedido ao pagamento através da aplicação, tentam os burlões apurar se a vítima é conhecedora do funcionamento da aplicação. No caso de não ser, levam-na a deslocar-se a um ATM, onde lhe indicam todos os passos a efetuar, levando a vítima a associar o seu número de telemóvel (do burlão) ao cartão multibanco da vítima, passando assim este a ter pleno acesso á conta bancária. Posteriormente e com recurso á aplicação que detêm instalada no seu smartphone, os burlões geram as necessárias referências e, junto de um ATM, procedem com os levantamentos bancários, no máximo de 400€. Caso verifique que a conta se encontra com saldo positivo, procedem ainda com transferências bancárias para contas que eles controlam.

b) Verifica-se ainda que por vezes os lesados, na altura em que o burlão lhes diz que deverá inserir o seu número de telemóvel (o do burlão), contestam que o número a associar deverá ser o seu (o da vítima) e não o dele, altura em que o suspeito acede e contínua com todas as indicações. Após esta associação, o burlão informa a vítima de que irá receber um código e que deverá fornecer-lhe esse código, de sete algarismos, para que ele (o burlão) possa proceder com a transferência do dinheiro, o que não tardará mais do

que alguns minutos. Assim, sabendo o burlão o número de telefone da vítima, bem como o código de acesso, utilizando a aplicação que detêm instalada no seu smartphone, gera as necessárias referências e, junto de um ATM, procede com os levantamentos bancários, no máximo de 400€. Caso verifique que a conta se encontra com saldo positivo, procedem ainda com transferências bancárias para contas que eles controlam.

c) Constata-se ainda um outro *"modus operandi"*, nomeadamente o de o burlão ludibriar e obter acesso a uma conta de uma vítima "**A**", a qual verifica, por consulta de saldo, que não tem dinheiro disponível, pelo que não tem interação com a mesma. Posteriormente, burla uma segunda pessoa "**B**" e, após os levantamentos (400€ máximo), verifica que existe ainda uma quantia significativa de dinheiro na conta. Assim e a fim de ocultar o seu rasto e uma vez que não pode levantar mais dinheiro, procede com transferência para a conta da vítima "**A**", da qual procede com levantamentos (400€ máximo) e volta a transferir para outra conta, sobre a qual detenha plenos poderes.

d) Existe ainda uma outra forma de burla, mesmo que pouco utilizada. Quando o burlão se depara com alguém que é conhecedor da plataforma, procede com um "*pedido de dinheiro*" ao invés de um "*envio de dinheiro*", escrevendo no campo das observações "*para pagamento de******". O recetor, ao ver a mensagem e por o sistema apresentar um botão de "*enviar dinheiro*", pensando a vítima que é para receber, acaba por clicar o que faz com que envie a quantia para o burlão, ao invés de a receber.

5. Existe algum padrão entre os tipos de atuação dos burlões?

Sim. Os burlões aproveitam-se da necessidade de as vítimas procederem com a venda de determinado artigo, não regateando preço e voluntariando-se de imediato para proceder com o pagamento total do objeto á venda. Assim e por as vítimas terem a necessidade de "*fazer*" dinheiro rapidamente e por estarem, na maioria das vezes, a vender um artigo por um valor bem acima do real valor, acedem de imediato, não se apercebendo que estão a ser burladas.

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

Da minha experiência, não existirá qualquer padrão, para além da "*avareza*" das vítimas em receberem uma quantia monetária, imediatamente e normalmente bem superior ao real valor de um qualquer artigo que pretendem vender.

Verifiquei que as vítimas tanto são mulheres como homens, com idade avançada, média e até jovens, com parcas habilitações ou bastante instruídos, residentes em zonas rurais e residentes em grandes centros populacionais, etc.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Não, bem pelo contrário.

Devido ao crescimento exponencial deste tipo de criminalidade, e por o MP delegar a esmagadora maioria dos processos na PJ, aliado ao facto de aquela polícia não ser conhecedora dos suspeitos, são as diligências solicitadas a esta Guarda, para proceder com os visionamentos das imagens e consequente identificação dos suspeitos, bem como são solicitadas as diligências inerentes com a constituição de arguido e subsequente interrogatório nessa qualidade.

Com esta prática, ainda que esta Guarda proceda com a esmagadora maioria do processo, nomeadamente em diligências, não possui a delegação para proceder com a investigação, o que impossibilita que sejam desenvolvidas outras ações policiais que venham a criar um maior sentimento de segurança nas populações.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Ao nível da comunicação, creio que não.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

Em 18/06/2020, foi desenvolvida a operação "*MB Reverse*", em Campo Maior, onde estiveram cerca de 250 militares das mais variadas valências da Guarda, dando cumprimento a 19 mandados de busca domiciliária e 19 mandados de busca não domiciliária.

Desta operação resultou a apreensão de diversa prova material, nomeadamente ouro, dinheiro, telemóveis, computadores portáteis, PEN's USB, cartões de

telecomunicações, cartões SD, diversa documentação bancária e não só, armas, outros objetos furtados, etc.

Posto isto, referir que na ZA do DTer Elvas verificou-se numa primeira fase e por volta do mês de janeiro de 2020, um decréscimo muito significativo de crimes contra o património, aliado ao facto de inúmeros OPC procederem com pedidos de preservação de imagens remetidos para o Posto Territorial de Campo Maior.

Referir que a problemática se verificava também noutros locais de responsabilidade de policiamento do Comando Territorial de Portalegre, motivo que levou o NAIC a elaborar relatório sobre o "*boom*" deste tipo de criminalidade.

Nesse seguimento, foram desenvolvidas reuniões de trabalho da IC do CTER Portalegre, tendo sido delineadas linhas orientadoras para desenvolver a investigação destes ilícitos e as quais assentaram, numa primeira fase, em alguns pilares:

a) Imagens de CFTV das dependências bancárias;
b) Números de telemóvel utilizados pelos suspeitos;
c) IMEI's associados;
d) Outros números associados;

Levou-se em linha de conta os IMEI's associados, uma vez que logo se percebeu que os suspeitos adquiriam inúmeros cartões pré-pagos, os quais detêm uma pequena verba, utilizavam-nos em alguns contactos e, logo que com ele conseguissem fazer uma burla, ou caso fossem detetados e desmascarados, destruíam-nos. Ainda assim o equipamento que era utilizado era repetido, já que é fácil adquiri cartões SIM, mas os telemóveis são mais dispendiosos.

Há data e devido ao crescimento que se verificava, logo foram levantadas várias questões que dificultaram uma boa investigação, nomeadamente:

a) Qual o enquadramento da tipologia criminal, outras burlas, burla simples, burla informática?
b) Qual o tribunal competente para tomar conhecimento dos factos, nomeadamente o da área de residência da vítima, ou o do lugar onde haviam sido feitos os levantamentos indevidos?
c) Qual o OPC competente para desenvolver a investigação, GNR/PSP ou PJ?

Face a tais dúvidas, verificou-se que diversos NUIPC foram enquadrados em tipologias diferentes, correram termos, numa primeira fase, em tribunais dispersos, bem como estiveram em OPC diferentes.

Assim, urgiu existir esclarecimento, tendo sido emanadas orientações aos dignos Procuradores da Republica, informando de que os crimes desta natureza deveriam ser enquadrados na tipologia de burla informática, falsidade informática e acesso ilegítimo, cabendo ter conhecimento dos fatos o tribunal da área onde eram efetivamente efetuados os levantamentos bancários, caso fosse conhecido, pois era aí onde a vítima perdia o "*poder*" sobre o seu dinheiro e, nesse seguimento, seria um crime de competência reservada da Policia Judiciária.

Foram ainda emanadas orientações de que toda a matéria recolhida nas investigações, deveria ser remetida ao DCIAP, o qual a trataria e compilava.

Uma vez que estas orientações tardaram e os crimes avolumavam-se diariamente, foram sendo desenvolvidas investigações e, no nosso caso, por sermos conhecedores das identidades dos autores dos factos e por se encontrarem alguns processos distribuídos ao NIC de Elvas para proceder com a investigação, solicitamos, foram promovidos e posteriormente foram emanados diversos mandados de busca e apreensão, aos quais demos o devido cumprimento em 18/06/2020, como acima referi.

Com aquelas diligências de busca domiciliária e não domiciliária, obtivemos inúmera prova material.

No seguimento das diligências de busca, foram remetidas informações às diversas entidades bancárias, dando notícia das contas bancárias que se suspeitava estavam a ser utilizadas pelos arguidos, para receberem quantias monetárias, retiradas indevidamente a inúmeras vítimas dispersas por todo o território português, pelo que, caso assim entendessem, deveriam as mesmas ser alvo de congelamento.

Face às orientações da Procuradora Coordenadora Distrital, por ordem da Procuradora do TJ de Elvas, foram os processos-crime que se encontravam em investigação no NIC e no âmbito dos quais haviam sido desenvolvidas as diligências de busca, apensos e levados á consideração do DIAP Regional de Évora, onde foram alvo de redistribuição, passando lá a correr termos. Em virtude de o NIC de Elvas ser largamente conhecedor do processo e face ao estado avançado da investigação, apesar de ser de competência reservada da PJ, a investigação manteve-se delegada na Guarda e no NIC de Elvas.

Devido às apreensões de telemóveis e demais equipamentos, recorreu-se á DIC, nomeadamente ao NDF, tendo sido elaborados os necessários exames digitais forenses.

Uma vez que existia inúmera matéria que se julgou ser relevante de ser tratada, analisada e compilada, recorreu-se á RAIC, bem como ao NAIC, órgãos que foram procedendo com a análise dos exames digitais forenses, análise de extratos bancários, etc.

Por anteriormente ter sido solicitado às operadoras de telecomunicações que informassem sobre os IMEI's associados aos números de telemóvel, utilizados para contactar as vítimas, encontrando-nos na posse de diversos telemóveis apreendidos, onde se constatou, entre outra informação, qual o IMEI, bem como quais os números de telefone que haviam estado inseridos naqueles equipamentos, compulsado com as diversas imagens de CFTV que se encontravam já devidamente vertidas nos autos, foi carreada prova da autoria, por parte dos arguidos, da prática de inúmeros crimes.

Dizer ainda que também foram apreendidos diversos cartões de suporte de cartão SIM, nos quais consta o ICCID. Recorrendo mais uma vez às operadoras de telecomunicações, foi solicitado que informassem a que número de telemóvel correspondia determinado ICCID e assim, consequentemente, chegar a mais uma eventual prática ilícita (NUIPC).

Munidos de um manancial de informação, mais uma vez resultou a necessidade de delinear linhas orientadoras para a investigação, tendo-se procedido, com a necessária concordância da AJ, a apensar processos-crime que tivessem a sua origem no lapso temporal compreendido entre DEC19 e 18JUN20.

Os pressupostos para tais apensações teriam de se enquadrar no facto de os arguidos serem os mesmos, vistas as imagens de CFTV, ou naqueles em que fosse possível atribuir a culpabilidade, em virtude da ausência de imagens de CFTV, mas por existir nexo de causalidade, nomeadamente naqueles em que a data dos factos coincidisse entre outras ocorrências em que os arguidos tivessem sido devidamente identificados sendo o IMEI ou o ICCID utilizados apreendido na posse dos arguidos.

Na presente data, face ao grande volume de processos e de intervenientes, encontra-se o processo em fase de relatório final, procedendo-se a elaborar um relatório final por cada NUIPC apenso, elaboração de diagramas de conexões e eventual correlação de informação e prova, no intuito de uma eventual acusação de associação criminosa.

Apêndice H- Entrevistas aos Militares da GNR- Entrevistado 6

Função: Elemento da Secção de Inquéritos

Posto: Cabo

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

No Posto Territorial, atendendo á proximidade com a população, existe no imediato uma "prevenção" através do contato pessoal, informando as pessoas dos cuidados a ter aquando da utilização das plataformas eletrónicas, tipo MB Way / outras.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Sim. As SPC´S, realizam algumas palestras, em norma direcionada à população mais idosa, para informação / prevenção.

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

Sim.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

Em norma, o Suspeito ao observar, por exemplo um anúncio para venda de um "objeto" num determinado *site*, mostra interesse em adquirir o mesmo. Após vários contatos telefónicos / troca de SMS (sempre num curto espaço de tempo), o Suspeito fornece um código / referência através de SMS, para que a o vendedor se desloque a uma ATM, informando que só assim consegue proceder ao pagamento. Quando o vendedor introduz o referido código para pagamento, o Suspeito não efetua qualquer pagamento, mas sim consegue realizar um levantamento de dinheiro da conta do vendedor, o qual só

se apercebe após a transação ter sido concluída, sendo que não consegue manter mais qualquer tipo de contato com o Suspeito.

5. Existem algum padrão entre os tipos de atuação dos burlões?

Por norma, alegam estar interessados na compra do objeto constante no *site*, bem como que para efetuar a transferência / pagamento, tem de ser introduzido pelo vendedor, o código cedido pelo mesmo.

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

Atualmente não existe um padrão pré-definido, pois este tipo de crime é recorrente em qualquer "estrato social" da sociedade.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Sim, em regra o MP assim que recebe a respetiva denúncia, inicia no imediato diligências, que posteriormente farão parte do Inquérito, o que torna o Processo / investigação mais célere.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Não.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

Por norma, os Suspeitos atuam em grupos e na maioria das vezes utilizam caixas ATM, sem videovigilância, tornando-se bastante difícil a sua identificação.

Apêndice I- Entrevistas aos Militares da GNR- Entrevistado 7

Função: Elemento da Secção de Inquéritos

Posto: Cabo

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

É do meu conhecimento a divulgação nas redes sociais de ações de sensibilização para a prevenção de crimes de Burla por MB Way, bem como no *site* oficial da GNR.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Desconheço a existência

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

Tento recolher todos os elementos relevantes e constantes na instrução técnica n.º 2020-04/DIC, difundida pelo efetivo.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

Os burlões manifestam o interesse em adquirir os bens que são colocados pelos burlados, nos vários *sites* disponíveis para o efeitos (os quais dominam), sem negociar o preço, sem colocar entraves em relação à forma de entrega do bem, mas sempre com a exigência de utilizar apenas o MB Way como forma de pagamento, descartando as restantes formas de pagamento, apercebendo-se da falta de conhecimento dos burlados sofre o funcionamento dos pagamentos através da referida plataforma.

5. Existem algum padrão entre os tipos de atuação dos burlões?

Sim, a atuação dos diferentes burlões tem se verificado bastante uniforme, utilizando praticamente o mesmo tipo de discurso para ludibriar as vítimas, recorrendo os mesmos da narrativa que referi na resposta n.º 4.

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

As vítimas mais comuns serão pessoas com idade média, maioritariamente pertencentes à classe média, com algum nível de instrução, mas que não têm conhecimento aprofundado de toda a plataforma MB Way.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Sim, tem se verificado tal sensibilização, dadas as consequências das burlas nos patrimónios das vítimas, bem como a importância da celeridade da investigação / medidas urgentes para tentar recolher prova e identificar os autores do ilícito.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Sim, o instrutor do processo deve diligenciar junto dos Procuradores, a possibilidade de requer de imediato junto das operadoras de telecomunicações as identificações dos titulares dos números de telemóvel utilizados pelos burlões, bem como quaisquer outras informações que permitam as suas identificações ou localizações, tendo também em conta o mesmo procedimento juntos das instituições bancárias node se verifiquem os levantamentos.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

As maiores dificuldades prendem-se com o facto de os burlões melhorarem as suas técnicas com o passar do tempo, utilizando cartões de telemóvel pré-pagos, que descartam imediatamente a seguir à concretização da burla, procurando ainda ATM’s sem câmaras de videovigilância.

Apêndice J- Entrevistas aos Militares da GNR- Entrevistado 8

Função: Elemento da Secção de Inquéritos

Posto: Guarda Principal

1. Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?

A resposta dada pela GNR no âmbito da prevenção dos crimes de burla com recurso a plataformas de pagamento eletrónico, prende-se essencialmente com o policiamento de proximidade.

2. Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?

Não tenho qualquer conhecimento de algum trabalho desenvolvido pelas secções de prevenção criminal.

3. Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?

Após receber uma denuncia por Burla com recurso ao MB Way, na descrição dos factos devem estar presentes, o mais pormenorizadamente possível, todas as informações que a vítima conseguir recolher, sendo que por norma o único meio de prova passível de recolher acaba por ser o número de telemóvel utilizado para o efeito e a caixa de multibanco onde efetuou o solicitado pelo burlão.

4. Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

As técnicas utilizadas pelos burlões para a prática deste tipo de ilícito prendem-se especialmente, de acordo com a minha experiência, com a demonstração de interesse por parte dos mesmos em adquirir algo que a vítima esteja a tentar vender através de uma qualquer plataforma *online*. Depois de demonstrar o seu interesse, o burlão diz à vítima

que para que a mesma não venda o produto a uma outra pessoa, ou utilizando uma outra desculpa, demonstra a intenção de proceder logo ao pagamento por MB Way, pedindo à vítima que se desloque a uma caixa multibanco, consumando aí o ilícito.

5. Existem algum padrão entre os tipos de atuação dos burlões?

Por norma, de acordo com a minha experiência, os burlões costumam ser pessoas de que têm facilidade de acesso à internet.

6. Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?

O perfil mais comum nas vítimas é o de pessoas com alguma idade ou com pouca escolaridade.

7. Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?

Não tenho qualquer informação relativa à celeridade com que decorre este tipo de processos no Ministério Público.

8. Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Não existe nenhuma especificidade na comunicação deste tipo de crimes ao Ministério Público.

9. Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?

Não sei quais as maiores dificuldades na aquisição de prova neste tipo de crimes uma vez que me encontro numa secção de inquéritos de um Posto Territorial, não me sendo atribuídos Inquéritos relativos a este tipo de ilícito.

Apêndice K- Quadro-Relação para a Elaboração das Entrevistas

Questão Central	Questões derivadas	Questões para a Entrevista (Guião nº1)
QP. - Qual a capacidade da GNR para prevenir e investigar o crime de burla cometido através de plataformas eletrónicas de pagamento (MB Way)?	QD.1- De que modo é feita a sensibilização / educação da população com vista à prevenção dos crimes de burla?	QE.1- Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)? QE.2- Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?
	QD.2- De que forma as burlas são cometidas pelos autores (métodos, tipos)? QD.3- Qual a evolução que se tem observado nas burlas com recurso a plataformas eletrónicas de pagamento (MB Way)? QD.4- De que modo a estrutura de investigação criminal da GNR, investiga / combate o crime de burla cometido através da aplicação MB Way e que métodos mobiliza na sua prática?	QE.3- Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados? QE.4- Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?

		QE.5- Existem algum padrão entre os tipos de atuação dos burlões? QE.6- Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way? P.7- Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?
	QD.5- De que forma o enquadramento legal dos crimes de burla realizados através da aplicação MB WAY implica a investigação?	QE.8- Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way? QE.9- Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?

Quadro 1- Quadro-Relação para a Elaboração das Entrevistas
Fonte: Elaboração Própria

Apêndice L- Apresentação e Análise das Respostas às Questões das Entrevistas

1. Apresentação e análise da questão nº1

Questão nº1: Que tipo de ações são utilizadas pela GNR para a prevenção dos crimes de burla com recurso a plataformas eletrónicas de pagamento (MB Way)?	
Nº	**Resposta**
E1	• Utilização das Redes Sociais • Divulgação dos *modus operandi* mais usuais • Divulgação da evolução dos *modus operandi* utilizados para realizar novos ilícitos • Desenvolvimento de ações de sensibilização pelos Comandos Territoriais • Permanente atualização dos militares
E2	• Divulgação/ comentários da GNR que alertam a população
E3	• Desenvolvimento de ações de sensibilização • Outras formas de divulgação
E4	• Ações de sensibilização nas Redes Sociais • Reportagens televisiva sobre os ilícitos • Outros meios de comunicação
E5	• Utilização das Redes Sociais • Divulgação dos resultados das operações desenvolvidas no âmbito destes ilícitos
E6	• Contacto direto com a população
E7	• Utilização das Redes Sociais • Divulgação no *site* oficial da GNR
E8	• Desenvolvimento de ações de policiamento comunitário

Quadro 2- Apresentação e análise da questão nº1
Fonte: Elaboração Própria

2. Apresentação e análise da questão nº2

Questão nº2: Tem conhecimento se existe algum trabalho desenvolvido na temática dos crimes de burla com recurso ao pagamento MB Way, elaborado pelas secções de prevenção criminal?	
Nº	**Resposta**
E1	• Permanente atualização das secções • Contacto com as populações mis sensíveis

E2	• Desconhece
E3	• Ações de esclarecimento e sensibilização
E4	• Desenvolvimento de sessões de esclarecimento junto da população mais idosa
E5	• Desconhece
E6	• Realização de palestras
E7	• Desconhece
E8	• Desconhece

Quadro 3- Apresentação e análise da questão nº2
Fonte: Elaboração Própria

3. Apresentação e análise da questão nº3

Questão nº3: Após receber uma denúncia de uma burla com recurso ao pagamento MB Way, sabe quais os elementos concretos de prova e descrição dos factos que tem de recolher para completar o processo e dar melhor resposta a todos os tópicos a serem investigados?	
Nº	**Resposta**
E1	• Uniformização do processo de recolha de informação • Uniformização do modo de atuação da GNR
E2	• Identifica os procedimentos presentes na Instrução Técnica 2020-04 DIC
E3	• Identifica os procedimentos presentes na Instrução Técnica 2020-04 DIC
E4	• Identifica os procedimentos presentes na Instrução Técnica 2020-04 DIC
E5	• Identifica os procedimentos presentes na Instrução Técnica 2020-04 DIC
E6	• Demonstra conhecer os procedimentos mas não os enumera
E7	• Identifica os procedimentos presentes na Instrução Técnica 2020-04 DIC
E8	• Identifica os procedimentos presentes na Instrução Técnica 2020-04 DIC

Quadro 4- Apresentação e análise da questão nº3
Fonte: Elaboração Própria

4. Apresentação e análise da questão nº4

Questão nº4: Quais as técnicas utilizadas pelos burlões para a realização do crime de burla com recurso ao pagamento MB Way?	
Nº	**Resposta**
E1	• Vítimas que querem vender produtos em plataformas *online* • Alguém que esteja interessado na compra de um produto • Desconhecimento da aplicação MB Way • Usa a aplicação MB Way, mas não tem conhecimento suficiente sobre o funcionamento da mesma
E2	• Alguém que esteja interessado na compra de um produto
E3	• Vítimas que querem vender produtos em plataformas *online* • Pagamento realizado de forma rápida, sem negociação • Desconhecimento da aplicação MB Way
E4	• Interesse na aquisição de produtos • Desconhecimento da aplicação MB Way
E5	• Desconhecimento da aplicação MB Way
E6	• Interesse na aquisição de produtos • Desconhecimento da aplicação MB Way
E7	• Interesse na aquisição de produtos • Desconhecimento da aplicação MB Way
E8	• Interesse na aquisição de produtos • Desconhecimento da aplicação MB Way

Quadro 5- Apresentação e análise da questão nº4
Fonte: Elaboração Própria

5. Apresentação e análise da questão nº5

Questão nº5: Existem algum padrão entre os tipos de atuação dos burlões?	
Nº	**Resposta**
E1	• Atuação em família • Atuação em esquema (trabalham em cascata) • Procura das vítimas indicadas para a prática deste tipo de ilícitos • Uso de cartões de telemóvel descartáveis • Uso de caixas multibanco sem sistema de vigilância
E2	• Não identifica

E3	• Venda de produtos rápida • Venda realizada sem qualquer negociação
E4	• Venda de produtos • Desconhecimento da aplicação MB Way
E5	• Fácil negociação • Explora a necessidade de vender da vítima
E6	• Venda de produtos rápida
E7	• Utilização de um padrão de atuação semelhante em todos os ilícitos realizados
E8	• Facilidade de acesso à internet

Quadro 6- Apresentação e análise da questão nº5
Fonte: Elaboração Própria

6. Apresentação e análise da questão nº6

Questão nº6: Qual o perfil da vítima mais comum do crime de burla com recurso ao pagamento MB Way?	
Nº	**Resposta**
E1	• Desconhecimento da aplicação MB Way • Procura de novos utilizadores das plataformas de compra e venda de produtos e serviços • Procura de pessoas com poucas habilitações ou idosos
E2	• Não existe perfil, qualquer pessoa pode ser sujeita ao ilícito
E3	• Desconhecimento da aplicação MB Way • Conhecimento da aplicação MB Way, mas desconhecimento sobre a sua utilização
E4	• Desconhecimento total ou muito reduzido da aplicação MB Way
E5	• Desconhecimento da aplicação MB Way • Qualquer tipo de pessoa poderá ser vítima deste ilícito
E6	• Qualquer pessoa pode ser alvo deste tipo de ilícito
E7	• Pessoas que usem plataformas de compra e venda de produtos e serviços *online*
E8	• Pessoas idosas • Pessoas com poucas habilitações

Quadro 7- Apresentação e análise da questão nº6
Fonte: Elaboração Própria

7. Apresentação e análise da questão nº7

Questão nº7: Considera que o Ministério Público, devido ao crescimento deste fenómeno, está mais sensibilizado e é mais célere quando se trata de processos de burla com recurso ao pagamento MB Way?	
Nº	**Resposta**
E1	• Ministério Público mais sensibilizado para os ilícitos
E2	• Centralização do trabalho do Ministério Público • Mais rapidez na resposta do Ministério Público
E3	• Ministério Público mais sensibilizado para os ilícitos • Resposta mais célere por parte de Ministério Público
E4	• Centralização do trabalho sobre estes ilícitos em equipas específicas, dentro do Ministério Público
E5	• Delegação da investigação feita pelo Ministério Público dificulta a mesma • Ministério Público pouco sensibilizado para este tipo de ilícitos
E6	• Ministério público é mais célere na resposta a este tipo de ilícitos
E7	• Reconhece que o Ministério Público está sensibilizado para este tipo de ilícitos
E8	• Desconhece

Quadro 8- Apresentação e análise da questão nº7
Fonte: Elaboração Própria

8. Apresentação e análise da questão nº8

Questão nº8: Existe alguma especificidade na comunicação ao Ministério Público quando se trata de um crime de burla com recurso ao pagamento por MB Way em relação a outro tipo de crime?	
Nº	**Resposta**
E1	• Desenvolvimento de orientação pelo Ministério Público sobre o tipo de ilícitos
E2	• Desconhece
E3	• Desenvolvimento de orientação pelo Ministério Público sobre o tipo de ilícitos • Recolha de dados específicos sobre o ilícito
E4	• Recolha de dados específicos sobre o ilícito

E5	• Não identifica
E6	• Não identifica
E7	• Desenvolvimento de orientação pelo Ministério Público sobre o tipo de ilícitos
E8	• Não identifica

Quadro 9- Apresentação e análise da questão nº8
Fonte: Elaboração Própria

9. Apresentação e análise da questão nº9

Questão nº9: Quais são as maiores dificuldades na aquisição de prova aquando da investigação do crime de burla com recurso ao pagamento MB Way?	
Nº	**Resposta**
E1	• Uso de cartões de telemóvel descartáveis • Caixas multibanco sem sistema de vigilância
E2	• Dificuldade na identificação do titular da conta para onde vai o dinheiro resultante da prática ilícita
E3	• Demora das respostas das entidades externas aos pedidos realizados pelas forças de segurança • Caixas multibanco sem sistema de vigilância
E4	• Caixas multibanco sem sistema de vigilância
E5	• Falta de militares com conhecimento especializado para a análise de prova digital • Caixas multibanco sem sistema de vigilância • Demora das respostas das entidades externas aos pedidos realizados pelas forças de segurança
E6	• Caixas multibanco sem sistema de vigilância
E7	• Uso de cartões de telemóvel descartáveis • Caixas multibanco sem sistema de vigilância
E8	• Desconhece

Quadro 10- Apresentação e análise da questão nº9
Fonte: Elaboração Própria

Apêndice M- Inquérito por Questionário- As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos

ACADEMIA MILITAR

As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos

Autor: Aspirante-Aluna Cavalaria da GNR Ana Marta de Sousa e Silva

Orientadora: Professora Doutora Sofia de Vasconcelos Casimiro

Coorientador: Tenente-Coronel Infantaria da GNR Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, junho de 2022

CARTA DE APRESENTAÇÃO

A presente investigação insere-se no âmbito do Relatório Científico Final do Trabalho de Investigação Aplicada, do mestrado em Ciências Militares, na Especialidade de Segurança da Academia Militar, que está subordinado ao tema: "As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionado com o uso de plataformas eletrónicas de pagamentos".

A finalidade desta investigação é identificar os contornos dos ilícitos relacionados com as burlas com recurso a plataformas eletrónicas de pagamento, nomeadamente os métodos utilizados e o enquadramento legal do tema. Adicionalmente, este trabalho de investigação pretende também perceber e abordar a vertente operacional da GNR sob dois prismas: inicialmente, sob o prisma da investigação criminal, analisando as respetivas competências e capacidades da GNR neste tipo de ilícito criminal, nomeadamente os seus constrangimentos e oportunidades; e, posteriormente, sob o prisma da prevenção criminal, analisando as competências e capacidades da GNR para sensibilizar a população nesta matéria, nomeadamente através dos programas de prevenção criminal desenvolvidos na área do policiamento comunitário.

Tendo em conta os objetivos da investigação, a realização de questionários por inquérito torna-se fundamental para recolher dados que possam dar resposta às questões levantadas ao longo da mesma e relacionar factos, ideias e opiniões que constituam doutrina de investigação. Os inquéritos serão realizados a militares de Secções de Inquéritos dos Comandos Territoriais, de diversos Núcleos de Investigação Criminal da GNR e a militares da SIIC dos Comandos Territoriais.

Face ao anteriormente explanado, solicito a Vossa Excelência que responda ao inquérito sobre a temática em investigação, pois a sua colaboração será essencial para atingir os objetivos propostos.

Grata pela colaboração e disponibilidade.

Atenciosamente,

Ana Marta de Sousa e Silva

Aspirante Cavalaria da GNR

1. ENQUADRAMENTO

As denúncias por práticas fraudulentas relacionadas com plataformas eletrónicas de pagamento, nomeadamente com a aplicação digital MB Way, geralmente enquadráveis no crime de burla, têm vindo a aumentar, segundo dados partilhados pelas forças de segurança ao Ministério Público.

A pertinência da temática é reconhecida, sendo este tipo de crime mencionado na Lei nº 55/2020, de 27 de agosto, que define as prioridades de política criminal para o biénio 2020-2022. Neste diploma legal, este tipo de crime é mencionado como um crime de prevenção prioritária, devido à necessidade de proteger as potenciais vítimas.

O ilícito em causa explora de uma forma ardilosa o desconhecimento que os cidadãos têm sobre o funcionamento das plataformas eletrónicas de pagamento, assim permitindo obter indevidamente valores monetários, por vezes de elevado montante.

Devido à não tipificação concreta das burlas praticadas através das plataformas eletrónicas de pagamento, como a plataforma MB Way, muitas vezes o seu enquadramento e consequente processo de investigação suscitam dúvidas, que conduzem à aplicação de critérios diversos para a mesma realidade. A presente investigação procura esclarecer algumas destas dúvidas**.**

2. INQUÉRITO

As respostas dadas às questões seguidamente apresentadas servirão para alcançar os objetivos propostos para a presente investigação. Por essa razão, solicita-se que sejam as mais ponderadas possíveis. As respostas apenas serão utilizadas para objeto de estudo desta investigação, pelo que é solicitada a sua autorização para se proceder à sua análise e transcrição.

Nos casos em que a sensibilidade da informação partilhada assim o exija, as respostas dadas poderão ser classificadas e o respetivo acesso poderá ser restringido. Se assim pretender, as respostas ser-lhe-ão facultadas, bem como, o trabalho final que também lhe poderá ser facultado na íntegra, assim que for aprovado e caso não tenha acesso restrito.

Inquérito por Questionário

As respostas ao presente questionário têm um caráter anónimo, não permitindo a identificação do participante, e têm como objetivo a recolha de dados para um Trabalho de Investigação Aplicada, no âmbito do Mestrado Integrado em Ciências Militares na Especialidade de Segurança, da Academia Militar. As suas respostas serão usadas meramente para fins estatísticos.

Agradece-se a sua disponibilidade e colaboração.

Posto

a. Guarda
b. Cabo
c. Sargento

Área onde trabalha

a. SIIC
b. NIC
c. Secção de Inquéritos

Tempo de serviço na área da Investigação Criminal

a. Menos de 2 anos
b. Entre 2 a 5 anos
c. Mais de 5 anos

1. **Tem conhecimento do que são as burlas cometidas através de plataformas eletrónicas de pagamento, como a do MB Way?**
   a. Sim
   b. Não

2. **Caso tenha de receber uma denúncia de burla realizada com recurso a uma plataforma eletrónica de pagamento, como a do MB Way, tem conhecimento dos seguintes procedimentos específicos a realizar?**
   a. Registo do n.º de Conta IBAN/ NIB

b. Identificação do cartão associado à aplicação MB Way
c. Obtenção dos contactos telefónicos do suspeito e da vítima
d. Obtenção do termo de consentimento/ autorização para levantamento do sigilo bancário
e. Todos
f. Outro procedimento

3. **Se receber uma denúncia de burla realizada com recurso a uma plataforma eletrónica de pagamento, como a do MB Way, considera que existe um perfil da(s) vítima(s)?**
   a. Sim
   b. Não

4. **Quem são as vítimas mais comuns deste tipo de ilícitos?**
   a. Menos de 18 anos
   b. Entre os 18 e os 35 anos
   c. Entre os 35 e os 65 anos
   d. Maiores de 65 anos
   e. Desconheço

5. **Tem conhecimento dos modos de atuação dos agentes criminosos neste tipo de ilícitos?**
   a. Sim
   b. Não

6. **Qual o modo de atuação que considera mais praticado pelos agentes criminosos neste tipo de ilícitos?**
   a. Manipulação da vítima no uso direto da plataforma eletrónica, como, por exemplo, no uso da aplicação MB Way
   b. Cedência dos dados do cartão da vítima (códigos de levantamento)
   c. Uso de um sítio eletrónico falso de uma plataforma de compra e venda de produtos, como o OLX, para recolha de dados de autenticação (*phishing*)
   d. Envio de SMS falsa para a obtenção de dados (*smishing)*
   e. Desconheço

7. **Ao receber uma denúncia relativa a uma burla realizada com recurso a uma plataforma eletrónica de pagamento, como a do MB Way, conseguirá identificar os modos de atuação usados para consumar o ilícito?**
    a. Sim
    b. Não

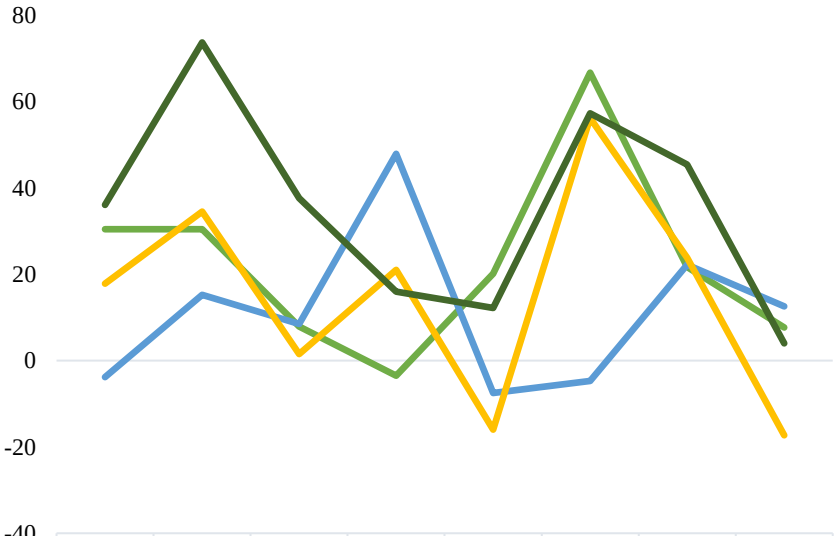
8. **Conhece alguma ação de sensibilização ou programa de prevenção da GNR direcionado para a temática das burlas realizadas com recurso a uma plataforma eletrónica de pagamento, como a do MB Way?**
    a. Sim
    b. Não

9. **Considera pertinente haver ações de sensibilização ou programas de prevenção criminal para a prevenção deste tipo de ilícito?**
    a. Sim
    b. Não

10. **Durante a fase de inquérito, considera que tem o(s) conhecimento(s) técnico(s) adequados para realizar as diligências de investigação para este tipo de ilícito, cometido através de plataformas eletrónicas de pagamento, como a do MB Way?**
    a. Sim
    b. Não

Obrigada pela sua colaboração.

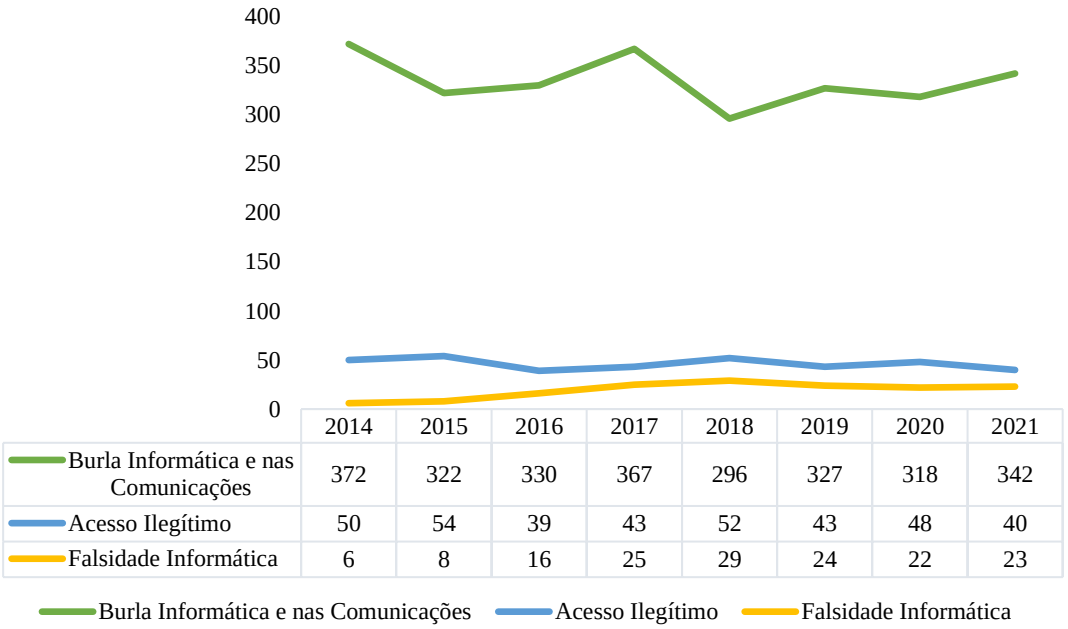
Apêndice N- Gráfico da variação da criminalidade de acordo com os RASI (2014-2021)



	2014	2015	2016	2017	2018	2019	2020	2021
Burlas Informática e nas Comunicações	30,4	30,4	7,9	-3,5	20,1	66,7	21,7	7,7
"Outras Burlas"	-3,8	15,2	8,5	47,9	-7,5	-4,7	22,2	12,6
Acesso Ilegítimo	17,8	34,5	1,5	21	-16	56,2	23,87	-17,3
Falsidade Informática	36,1	73,7	37,6	16	12,2	57,3	45,4	4

Figura 12- Variação da Criminalidade (2014-2021)
Fonte: Elaboração Própria

Apêndice O- Gráfico da variação do número de arguidos constituídos de acordo com o RASI (2014-2021)



	2014	2015	2016	2017	2018	2019	2020	2021
Burla Informática e nas Comunicações	372	322	330	367	296	327	318	342
Acesso Ilegítimo	50	54	39	43	52	43	48	40
Falsidade Informática	6	8	16	25	29	24	22	23

Figura 13- Variação do número de arguidos constituídos (2014-2021)
Fonte: Elaboração Própria