



ACADEMIA MILITAR

Prevenção Criminal: Estudo de caso a furtos a terminais de multibanco

Aspirante de Infantaria da GNR Licínio André Capela do Rêgo

Trabalho de Investigação Aplicada

Mestrado Integrado em Ciências Militares na Especialidade de Segurança

Orientadora: Major de Infantaria Doutorada da GNR Adriana Filipa Martins Gameiro

Júri

Presidente do Júri: Professora Associada Paula Manuela dos Santos Lopes do Rego Figueiredo

Arguente: Tenente-Coronel de Infantaria da GNR Tiago Gonçalves Silva

Orientadora: Major de Infantaria Doutorada da GNR Adriana Filipa Martins Gameiro

Diretora de Curso: Tenente-Coronel de Cavalaria da GNR Lucília de Jesus Mendes da Silva

Junho de 2025



ACADEMIA MILITAR

Prevenção Criminal: Estudo de caso a furtos a terminais de multibanco

Aspirante de Infantaria da GNR Licínio André Capela do Rêgo

Trabalho de Investigação Aplicada

Mestrado Integrado em Ciências Militares na Especialidade de Segurança

Orientadora: Major de Infantaria Doutorada da GNR Adriana Filipa Martins Gameiro

Júri

Presidente do Júri: Professora Associada Paula Manuela dos Santos Lopes do Rego Figueiredo

Arguente: Tenente-Coronel de Infantaria da GNR Tiago Gonçalves Silva

Orientadora: Major de Infantaria Doutorada da GNR Adriana Filipa Martins Gameiro

Diretora de Curso: Tenente-Coronel de Cavalaria da GNR Lucília de Jesus Mendes da Silva

Junho de 2025

EPÍGRAFE

“If my mind can conceive it, if my heart can believe it, then I can achieve it.”

Muhammad Ali

DEDICATÓRIA

Aos meus pais.

AGRADECIMENTOS

A presente investigação assinala o culminar de cinco anos de formação numa casa na qual muito me orgulho em pertencer, a Academia Militar, e representa a concretização de um sonho e de um objetivo profissional pelo qual sempre ambicionei.

Aos meus pais, a mais profunda gratidão por todo o apoio, dedicação e sacrifício com que, ao longo da minha vida, me proporcionaram todas as condições necessárias para alcançar os meus objetivos.

À Mariana, por estar ao meu lado ao longo de toda esta jornada. Esta conquista não é apenas minha, mas sim nossa.

À minha orientadora, Major da GNR Adriana Filipa Martins Gameiro, expresso o meu profundo agradecimento pelo apoio constante desde o primeiro dia. A sua disponibilidade permanente, dedicação e orientação foram fundamentais para a realização desta etapa.

Aos militares oficiais, sargentos e guardas da Direção de Informações (DI) e da Direção de Investigação Criminal (DIC), expresso o meu agradecimento pela constante disponibilidade e pela valiosa partilha de conhecimentos e experiência, cujo contributo foi essencial para esta investigação.

Ao Inspetor-Chefe Santos Martins, da Polícia Judiciária, agradeço pela grande disponibilidade e pela generosa partilha do vasto conhecimento adquirido ao longo da sua longa carreira, que muito contribuíram para o desenvolvimento desta investigação.

A todos os entrevistados que gentilmente disponibilizaram o seu tempo para contribuir para esta investigação e partilharam as suas experiências e conhecimentos, expresso o meu sincero agradecimento.

Aos meus camaradas do XXX Curso de Formação de Oficiais da Guarda Nacional Republicana da qual muito me orgulho em pertencer, por todos os momentos passados ao longo destes cinco anos que guardarei com saudade.

Aos Diretores de Curso da Guarda Nacional Republicana que me acompanharam ao longo destes anos na Academia Militar, Coronel Paulo Gomes e Tenente-Coronel Lucília Silva, agradeço pela dedicação demonstrada e pelo contributo prestado ao meu percurso formativo.

À minha família e amigos, agradeço profundamente todo o apoio, incentivo e presença ao longo deste percurso.

A todos aqueles que ao longo da minha curta carreira de alguma maneira contribuíram para o meu sucesso nesta etapa.

A todos o meu sincero agradecimento,

Licínio Rêgo

RESUMO

A evolução recente do número de furtos a terminais de multibanco em Portugal, paralela a tendências observadas no contexto europeu, tem constituído um desafio significativo para a segurança. Nesse sentido, a presente investigação procura compreender como a Guarda Nacional Republicana pode direccionar a prevenção deste tipo de criminalidade. Nesse sentido urge a necessidade de identificar os *Modus Operandi* mais frequentes em Portugal, assim como identificar padrões de interesse relevantes na debelação deste fenómeno.

Para alcançar esses objetivos, foi adotada uma metodologia mista. Por um lado, realizou-se uma análise estatística de todos os furtos a terminais multibanco registados, entre 2016 e 2024, na área de jurisdição da Guarda Nacional Republicana, completada pela realização de entrevistas com elementos das Forças e Serviços de Segurança com responsabilidade sobre a matéria. Esta abordagem permitiu integrar uma perspetiva quantitativa do fenómeno (incidência e distribuição territorial e temporal dos furtos) com uma compreensão qualitativa das práticas e vulnerabilidades associadas.

Os resultados evidenciam múltiplos *Modi Operandi*, englobando ataques de natureza física, como arrombamentos e ataques com recurso a explosivos, e ataques lógicos, como a introdução de *malware* para retirar dinheiro do terminal. Verificou-se uma maior incidência em determinadas locais e períodos do dia. Foram também identificadas vulnerabilidades relacionadas com as características do local e do terminal, como a localização, o tipo de local, locais de fuga e fragilidades nas instalações ou nos próprios terminais.

As conclusões salientam a necessidade de implementar uma abordagem multidimensional. Entre as principais recomendações, destacam-se a elaboração de perfis de risco individualizados para cada terminal, um patrulhamento direccionado nos períodos mais críticos, identificados estatisticamente como os mais propícios à ocorrência deste tipo de furtos e reforçar a cooperação entre as forças de segurança e demais instituições com competências na área.

Palavras – Chave: Guarda Nacional Republicana; Furtos a terminais de multibanco; Prevenção Multidimensional; *Modus Operandi*; Perfis de risco; Cooperação.

ABSTRACT

The recent evolution in the number of thefts from ATM terminals in Portugal, mirroring trends observed across Europe, has posed a significant challenge to security. In this context, the present study seeks to understand how the Guarda Nacional Republicana can better direct the prevention of this type of crime. This highlights the urgency of identifying the most frequent *Modus Operandi* in Portugal, as well as detecting relevant patterns of interest in tackling this phenomenon.

To achieve these objectives, a mixed-methods approach was adopted. On one hand, a statistical analysis was carried out on all ATM thefts recorded between 2016 and 2024 within the Guarda Nacional Republicana area of jurisdiction. The analysis was complemented by interviews with members of the Security Forces and Services responsible for this area. This approach enabled the integration of a quantitative perspective on the phenomenon (incidence and territorial and temporal distribution of the thefts) with a qualitative understanding of the associated practices and vulnerabilities.

The findings reveal multiple *Modus Operandi*, that include physical attacks, like break-ins and explosive-based attacks, as well as logical attacks, such as the insertion of malware to extract money from the terminal. A higher incidence was observed in specific locations and during certain times of day. Vulnerabilities were also identified in relation to the characteristics of both the site and the terminal, such as its location, type of setting, escape routes, and weaknesses in the infrastructure or the ATM itself.

The conclusions highlight the need for a multidimensional approach. Among the main recommendations, are the development of individualised risk profiles for each terminal, targeted patrols during statistically identified high-risk periods, and the reinforcement of cooperation between security forces and other institutions with responsibilities in this area.

Keywords: National Republican Guard; Thefts from Automated Teller Machines; Multidimensional Prevention; Modus operandi; Risk profiles; Cooperation

ÍNDICE GERAL

INTRODUÇÃO.....	1
PARTE I – REVISÃO DA LITERATURA.....	4
CAPÍTULO I – PREVENÇÃO CRIMINAL	4
1.1. Teorias do Crime e a Prevenção Situacional.....	4
1.2. Tipos de Criminalidade	7
CAPÍTULO II – FURTO A ATM.....	9
2.1. Modus Operandi de furtos a ATM	9
2.1.1. Ataque físicos	10
2.1.2. Ataques lógicos	13
2.2. Contexto Europeu	16
2.3. Contexto Nacional	18
2.4. Enquadramento jurídico.....	20
2.5. Fatores preponderantes para um furto a ATM.....	21
2.6. Prevenção de furtos de ATM segundo o REPC e EUROPOL	24
2.7. Prevenção de furtos de ATM em Portugal	26
2.8. Implementação das ATM em Portugal.....	27
PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO ...	29
CAPÍTULO III – METODOLOGIA, MÉTODOS E MATERIAIS	29
3.1. Objetivos da investigação	29
3.2. Definição do desenho e da estratégia de investigação	30
3.3. Técnicas e procedimentos de recolha de dados	30
3.4. Tratamento de dados	32
CAPÍTULO IV – APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS	34
4.1. Apresentação e análise dos resultados quantitativos.....	34
4.1.1 Distribuição por Distrito e por Concelho	34
4.1.2 Distribuição mensal e semanal.....	36
4.1.3 Análise da distribuição horária.....	38
4.1.4 <i>Modus Operandi</i>	39
4.1.4.1. <i>Modus Operandi</i> Ataques Físicos	39
4.1.4.2 <i>Modus Operandi</i> Ataques Lógicos	42

4.1.5 Local da ATM	42
4.1.6 Veículos e fuga.....	44
4.1.7. Número de indivíduos.....	44
4.1.8. Sistemas de Videovigilância	45
4.2 Apresentação e análise das entrevistas	46
4.3 Discussão dos resultados	50
CONCLUSÕES E RECOMENDAÇÕES.....	58
REFERÊNCIAS BIBLIOGRÁFICAS E OUTRAS FONTES	64
APÊNDICES.....	I
ANEXO.....	XIV

ÍNDICE DE FIGURAS

FIGURA N.º 1 - TERMINOLOGIA DE ATAQUES FÍSICOS A ATM	13
FIGURA N.º 2 - ESTRUTURA ATM.....	14
FIGURA N.º 3 - VARIAÇÃO ATAQUES FÍSICOS E LÓGICOS	18
FIGURA N.º 4 - EVOLUÇÃO FURTOS DE ATM EM PORTUGAL	19
FIGURA N.º 5 - COMPARAÇÃO ENTRE RASI E O RAGNR RELATIVAMENTE A FURTOS A ATM	20
FIGURA N.º 6 - RELAÇÃO ENTRE OS OE E AS PD	30
FIGURA N.º 7 - MAPA COROPLÉTICO DE FURTOS A ATM NA ÁREA DA GNR DE 2016 A 2024	36
FIGURA N.º 8 - NÚMERO DE FURTOS (TENTATIVAS E CONSUMADOS) POR MÊS DE 2016 A 2024	37
FIGURA N.º 9 - NÚMERO DE FURTOS (TENTATIVAS E CONSUMADOS) POR DIA DA SEMANA DE 2016 A 2024.....	38
FIGURA N.º 10 - NÚMERO DE FURTOS (TENTATIVAS E CONSUMADOS) POR HORA DO DIA DE 2016 A 2024	38
FIGURA N.º 11 - JANELA TEMPORAL DOS FURTOS SEM HORA DEFINIDA DE 2016 A 2024	39
FIGURA N.º 12 - COMPARAÇÃO ENTRE ATAQUES FÍSICOS E LÓGICOS DE 2016 A 2024.....	39
FIGURA N.º 13 - MODUS OPERANDI ATAQUES FÍSICOS DE 2016 A 2024	40
FIGURA N.º 14 – COMPARAÇÃO ATAQUES EXPLOSIVOS DE 2016 A 2024.....	40
FIGURA N.º 15 - TIPO DE LOCAL.....	43
FIGURA N.º 16 - FURTOS ATM POR BANCO	44
FIGURA N.º 17 - MARCAS DAS VIATURAS SUSPEITAS	44
FIGURA N.º 18 - NÚMERO DE INDIVÍDUOS SUSPEITOS	45
FIGURA N.º 19 - PRESENÇA DE CCTV	45
FIGURA N.º 20 - COMPARAÇÃO MARCAS/GRUPOS DE VIATURAS	55

ÍNDICE DE QUADROS E TABELAS

QUADROS

QUADRO N.º 1 - SUBTIPOS DE FURTOS DA ATM – NO LOCAL	12
QUADRO N.º 2 - TIPOS DE <i>MALWARE</i> PARA ATAQUES LÓGICOS	16
QUADRO N.º 3 - PERFIL DE RISCO INDIVIDUALIZADO PARA ATM.....	25
QUADRO N.º 4 - PREVENÇÃO CONTRA FURTOS A ATM.....	25
QUADRO N.º 5 - MEDIDAS PARALELAS NA PREVENÇÃO DE FURTOS A ATM...	26
QUADRO N.º 6 - REQUISITOS TÉCNICOS MÍNIMOS DE ATM.....	28
QUADRO N.º 7 - ANÁLISE ENTREVISTAS: INDICADORES DE ALERTA.....	47
QUADRO N.º 8 - ANÁLISE ENTREVISTAS: CARREGAMENTO DO ATM.....	47
QUADRO N.º 9 - ANÁLISE ENTREVISTAS: CARACTERÍSTICAS DO LOCAL	48
QUADRO N.º 10 - ANÁLISE ENTREVISTAS: CARACTERÍSTICAS DA ATM.....	49
QUADRO N.º 11 - ANÁLISE ENTREVISTAS: PREVENÇÃO DE FURTO DE ATM....	50

TABELAS

TABELA N.º 1 - FURTOS A ATMS NA EUROPA ENTRE 2015 A 2023	17
TABELA N.º 2 - FURTOS ATM EM PORTUGAL ENTRE 2016 A 2024.....	19
TABELA N.º 3 - FURTOS ATM NA ÁREA DE JURISDIÇÃO DA GNR ENTRE 2016 A 2024.....	19
TABELA N.º 4 - FURTOS ATM POR DISTRITO DE PORTUGAL DE 2016 A 2024	35
TABELA N.º 5 – ATAQUES FÍSICOS A ATM POR ANO DE 2016 A 2024.....	41
TABELA N.º 6 - TAXA DE CONSUMAÇÃO FURTOS A ATM DE 2016 A 2024.....	42
TABELA N.º 7 - ATAQUES LÓGICOS A ATM POR ANO DE 2016 A 2024.....	42

LISTA DE APÊNDICES E ANEXOS

APÊNDICES

APÊNDICE A – TABELA ANÁLISE DOS DADOS QUANTITATIVOS	II
APÊNDICE B – GUIÃO DE ENTREVISTA	III
APÊNDICE C - CARACTERIZAÇÃO DOS ENTREVISTADOS	VIII
APÊNDICE D - CODIFICAÇÃO DAS ENTREVISTAS	IX
APÊNDICE E - NÚMERO DE FURTOS POR DISTRITO E ANO (PORTUGAL CONTINENTAL)	X
APÊNDICE F- NÚMERO DE FURTOS POR DISTRITO E ANO (PORTUGAL CONTINENTAL)	XI

ANEXOS

ANEXO A – RECOMENDAÇÕES PARA UMA ABORDAGEM PREVENTIVA: RESUMO	XV
--	----

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

Al.	Alínea
AM	Academia Militar
AN	Autos de Notícia
APA	<i>American Psychological Association</i>
AR	Assembleia da República
Art.º	Artigo
ATM	<i>Automated Teller Machine</i>
ATMIA	<i>ATM Industry Association</i>
CCA	Caixa de Crédito Agrícola
Cfr.	Conforme
CPP	Código Penal Português
CTT	Correios e Telégrafos de Portugal
DI	Direção de Informações
DIC	Direção de Investigação Criminal
E	Entrevista
EAST	<i>European Association for Secure Transactions</i>
EGAP	<i>East Expert Group on ATM and ATS Physical</i>
EMPACT	Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas
EUROPOL	Agência da União Europeia para a Cooperação Policial
FS	Forças de Segurança
GNR	Guarda Nacional Republicana
GCO	Grupo Criminoso Organizado
IBNS	<i>Intelligent Banknote Neutralisation System</i>
LOGNR	Lei Orgânica da GNR
MAI	Ministério da Administração Interna
MO	<i>Modus operandi</i>
n.º	Número
OE	Objetivo Específico
OG	Objetivo Geral
PC	Computador
PD	Pergunta Derivada

PE	Pergunta da Entrevista
PP	Pergunta de Partida
PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública
QD	Questões Derivadas
QP	Questão Principal
RAGNR	Relatório de Atividades da GNR
RASI	Relatório Anual de Segurança Interna
REPC	Rede Europeia de Prevenção da Criminalidade
RJSP	Regime Jurídico da Segurança Privada
SI	Sistema de Informação
SIBS	<i>Forward Payment Solutions</i>
SIC	Secção de Investigação Criminal
SSI	Sistema de Segurança Interna
SOCTA	<i>Serious and Organised Crime Threat Assessment</i>
TIA	Trabalho de Investigação Aplicada

INTRODUÇÃO

O presente Trabalho de Investigação Aplicada (TIA) subordinado ao tema “Prevenção Criminal: Estudo de caso a furtos a terminais de multibanco”, surge no âmbito da conclusão do Mestrado Integrado em Ciências Militares, na especialidade de Segurança, lecionado na Academia Militar (AM), cuja realização e posterior apresentação culminará na conclusão do Tirocínio para Oficiais e consequente atribuição do grau de mestre, necessário ao futuro oficial da Guarda Nacional Republicana (GNR) para o exercício das funções que estatutariamente lhes serão cometidas¹.

As *Automated Teller Machine* (ATM), vulgarmente conhecidas como multibancos, são parte essencial da infraestrutura financeira atual. Não obstante dessa importância, as ATMs “(...) representam alvos em que a relação custo-benefício das ações criminosas se revela amplamente remuneratória face aos valores monetários obtidos e ao risco que a ação em si envolve (...)” (SSI, 2013, p. 181). Os ataques físicos contra ATM, em 2023, registaram na Europa o maior número de ataques da última década, com um aumento sensivelmente de 121 % no espaço de dez anos (EAST, 2023). No mesmo período, em Portugal, segundo o Relatório Anual de Segurança Interna (IASI) foram reportados cerca de 1672 furtos a ATM.

Os crimes que têm por objeto equipamentos ATM, segundo Joana Marques Vidal, Procuradora-geral da República no período compreendido entre 2012 e 2018, são praticados, “(...) em regra, com recurso a armas de grande calibre e explosivos ou meios equiparados, e que, para além dos prejuízos decorrentes da subtração de elevados valores em dinheiro, colocam em risco a vida e a integridade física dos cidadãos (...)”² (Ministério Público, 2017, p. 1).

Em Portugal, tem-se registado, nos últimos anos, um aumento significativo da percentagem deste tipo de furtos nas áreas sob jurisdição da Guarda Nacional Republicana (GNR), em comparação com períodos anteriores, durante os quais a percentualmente a incidência destes crimes era substancialmente inferior.

A GNR enquanto Força de Segurança (FS) de natureza militar, tem à sua responsabilidade sensivelmente 94% de área do território nacional, na qual residem cerca de

¹ Academia Militar (2023). Disponível em <http://academiamilitar.pt/curso-de-ciencias-militares-na-especialidade-de-seguranca.html>.

² Ministério Público (2017). Disponível em https://www.ministeriopublico.pt/sites/default/files/documentos/pdf/despacho_pgr_equipa_conjunta_atm_06-12-2017.pdf

54% da população (GNRa, 2020). A presença da GNR em grande parte do território nacional conjugada com o espectro de atribuições conferidas por lei³ à GNR, em especial a Lei Orgânica da GNR⁴ (LOGNR), entre elas: garantir a ordem e a tranquilidade públicas e a segurança e a proteção das pessoas e dos bens⁵, prevenir a criminalidade em geral⁶, e manter a vigilância e a proteção de pontos sensíveis, leva a que a GNR desempenhe um papel extramente relevante na segurança destas infraestruturas e principalmente dos cidadãos que direta ou indiretamente possam sofrer algum tipo de prejuízo com estes ataques, quer na sua segurança, quer no sentimento de insegurança e na segurança dos seus bens.

Em 2023, o número de ATM instalados em Portugal era de 12.501 (Pordata, 2023). Dada a ampla dispersão territorial destes equipamentos e a natureza da atividade criminosa, caracterizada como sendo de "(...) elevada gravidade e territorialmente dispersa (...)" (Ministério Público, 2017, p. 1), bem como a constante evolução dos métodos utilizados (Europol, 2021), torna-se fundamental que uma prevenção eficaz se baseie num conhecimento atualizado e aprofundado sobre esta problemática (Prates, 2011).

Esta investigação tem como objetivo analisar como pode a GNR direcionar a prevenção contra crimes de furto a ATM, analisando e identificando *Modus Operandi* (MO) bem como padrões ou indicadores que possam contribuir para uma prevenção mais eficaz deste tipo de crimes.

Perante o aumento contínuo dos furtos a ATM na Europa, compreender as novas tendências e dinâmicas deste fenómeno é essencial para desenvolver estratégias de prevenção e mitigação a nível nacional. Deste modo, examinar-se-ão todas as ocorrências registadas em Portugal, que envolveram furtos a ATM, em particular, os casos que implicam a subtração ou tentativa de subtração do dinheiro acondicionado no mesmo nas áreas da responsabilidade da GNR no período compreendido entre 2016 e 2024. Sendo certo que o desenvolvimento de conhecimento nesta área constitui um importante contributo para o eficiente emprego de meios das Forças de Segurança, e em particular da GNR.

Por conseguinte esta investigação tem como Objetivo Geral (OG) "Analisar como pode a GNR direcionar a prevenção contra crimes de furto a ATM"

³ Cfr. n.º 1 do art.º 3 da Lei Orgânica da GNR (LOGNR)

⁴ Cfr. Lei n.º 63/2007 de 06 de novembro

⁵ Cfr. Al. j) do n.º 1 do art.º 3.º da LOGNR

⁶ Cfr. Al. b) do n.º 1 do art.º 3.º da LOGNR

Por sua vez o O_G desdobra – se em objetivos específicos (O_E) que devem representar, de forma lógica, clara e precisa, em cada fase da investigação, as etapas necessárias para a consecução do objetivo geral (Camoleze, 2022):

- O_{E1}: Analisar o *Modus Operandi* de furtos a ATM, em Portugal Continental, na área de jurisdição da GNR.
- O_{E2}: Compreender quais os padrões de interesse para a GNR para prevenir os furtos a ATM em Portugal.

Neste sentido o presente trabalho encontra-se dividido em duas partes: a Parte I relativa à Contextualização Teórica que integra os Capítulos I e II e a Parte II que agrega o Enquadramento Metodológico e Trabalho de Campo, Capítulos III e IV respetivamente.

No que diz respeito à Parte I – Contextualização Teórica, a mesma integra o Capítulo I dedicado à Prevenção Criminal onde é elaborada uma abordagem teórica a um conjunto de conceitos fundamentais na prevenção criminal e em especial a prevenção situacional. O Capítulo II é dedicado ao furto a ATM, na qual é abordado este fenómeno na Europa e em Portugal, quer através da análise do *Modus Operandi* (MO) e de todo o planeamento por de trás de um furto a ATM, quer através da análise estatística oficial nacional e europeia, medidas preventivas implementadas, enquadramento legal.

Quanto à Parte II – Enquadramento Metodológico e Trabalho de Campo, no Capítulo III são definidos os objetivos da investigação e a respetiva estratégia que será empregue para a aquisição dos objetivos, bem como as respetivas técnicas de recolha e análise de dados. Posteriormente, no Capítulo IV são apresentados os resultados observados no trabalho de campo, quer através da análise de todos os furtos registados, entre 2016 a 2024, na área de jurisdição da GNR, bem como das entrevistas efetuadas, sendo posteriormente articulados com os dados obtidos no decorrer da revisão de literatura.

Por fim, nas Conclusões, Recomendações e por fim nas Limitações, é sistematizado o conhecimento produzido ao longo da investigação, respondendo ao O_G. Seguem-se as Referências Bibliográficas, elaboradas de acordo com a 7.^a edição das normas da American Psychological Association (APA), bem como os Apêndices e Anexos considerados relevantes.

PARTE I – REVISÃO DA LITERATURA

CAPÍTULO I – PREVENÇÃO CRIMINAL

A atividade criminosa continua a ser um dos grandes flagelos nas civilizações modernas (Anderez et al., 2021). A prevenção criminal surge como parte do dever / tarefa do Estado de promover a prevenção de crimes futuros, enquanto alicerce da segurança (Valente, 2022).

1.1. Teorias do Crime e a Prevenção Situacional

A Decisão 2009/902/JAI⁷ do Conselho da União Europeia, que criou a Rede Europeia de Prevenção da Criminalidade⁸ (REPC), define⁹ prevenção criminal como:

(...) todas as medidas destinadas a reduzir ou a contribuir para a redução da criminalidade e do sentimento de insegurança dos cidadãos, tanto quantitativa como qualitativamente, quer através de medidas directas de dissuasão de actividades criminosas, quer através de políticas e acções destinadas a reduzir os factores potenciadores as causas da criminalidade.

As medidas destinadas à redução, ou contribuição para a redução, da criminalidade e do sentimento de insegurança¹⁰ podem assumir diferentes abordagens (Silva, 2023). A prevenção criminal pode incidir sobre diversos fatores ou domínios, abrangendo dimensões individuais, sociais, comunitárias e ambientais (Corrado et al., 2017). Estas intervenções não se circunscrevem exclusivamente à esfera das Forças de Segurança (FS), podem igualmente ser implementadas por entidades de cariz público e privado, dentro dos seus domínios e competências legalmente previstas, possibilitando dessa forma respostas mais contextualizadas e eficazes (Crawford & Evans, 2012).

Diferenciando-se das abordagens que se focam nas causas sociais ou económicas, a criminologia ambiental analisa a forma como o espaço e o tempo influenciam e potencia a ocorrência de determinados crimes (Sánchez-Delgado, 2024). O seu objetivo é identificar as características e especificidades dos contextos espaciais que, direta ou indiretamente,

⁷ Conselho Justiça e Assuntos Internos

⁸ *European Crime Prevention Network (EUCPN)*

⁹ Cfr. n.º 2 do Art.º 2.º da Decisão 2009/902/JAI do Conselho da União Europeia, de 30 de novembro de 2009

¹⁰ Este sentimento pode ser analisado em três dimensões distintas: a) a dimensão afetiva, traduzida no medo do crime; b) a dimensão cognitiva, relacionada com a perceção do risco criminal, isto é, a avaliação de determinadas situações como potencialmente perigosas ou lesivas; e, por fim, c) a dimensão comportamental, expressa em atitudes como evitar certos locais ou grupos de pessoas, ou adotar medidas de autoproteção que reforcem a perceção de segurança (Kuhn & Agra, 2010).

possam favorecer ou limitar as oportunidades para a prática de certos crimes (Hollis et al., 2013).

Algumas teorias intimamente relacionadas com a criminologia ambiental, são fundamentais para compreender como o ambiente contribui para potencializar determinados fenômenos criminais, como é o caso dos furtos.

A Teoria das Atividades Rotineiras defende que quando três elementos coincidem no tempo e no espaço favorecem a ocorrência de determinados crimes: um transgressor motivado, a ausência de vigilância / defensor capaz e um alvo adequado ou desejado (Cohen & Felson, 1979).

O conceito de defensor capaz é bastante alargado, incluindo, entre outros, as FS, sistemas de videovigilância ou alarmes, ou mesmo a vigilância natural resultante da presença da população. Por sua vez, o objeto desejado, segundo com o conceito VIVA (Valor, Inércia, Visibilidade e Acesso) conforme a conceptualização posteriormente desenvolvida por Felson (1998) não se define apenas pelo seu valor monetário, mas também pela facilidade com que pode ser subtraído. Este aspeto envolve as características do objeto, a acessibilidade ao alvo e a facilidade de fuga (Rebocho, 2009). A oportunidade para determinados crimes emerge assim da conjugação entre a ausência de vigilância e a presença de um objeto atrativo (Sánchez-Delgado, 2024).

A Teoria do Padrão Criminal, defende que os crimes não são aleatórios, ou seja, não se distribuem ao acaso pelo tempo e pelo espaço (Brantingham & Brantingham, 1991). Seguem antes padrões baseados nas rotinas dos indivíduos e do ambiente urbano. Determinados locais, derivado das especificidades das suas características, acabam por ser mais propícios a determinados crimes (Brantingham et al., 2017).

A eficácia na prevenção da criminalidade resulta da análise integrada de múltiplas variáveis e respetivas características associadas à ocorrência de delitos. Quando as entidades responsáveis, em especial as FS, possuem um conhecimento aprofundado do território, das potenciais vítimas, sejam elas pessoas ou objetos, dos possíveis perpetradores, bem como das naturezas das infrações e dos seus *Modos Operandi* (MO), torna-se viável definir estratégias direcionadas ao cerne do problema.

À medida que aumenta a experiência no mundo do crime, a seleção dos seus alvos é cada vez mais criteriosa, movimentando-se estrategicamente, identificando novos alvos e explorando vulnerabilidades (Brantingham et al., 2017). A delimitação espacial e temporal influencia significativamente a incidência de certos tipos de criminalidade (Elias, 2008).

A Teoria da Escolha Racional introduzida por Derek Cornish e Ronald Clarke (1986) é um modelo que explica o crime como resultado de uma decisão racional do indivíduo, baseada na avaliação dos custos e benefícios de determinada ação criminosa. O crime é, em grande parte, resultado de escolhas deliberadas por parte dos seus perpetradores, que avaliam se o lucro de determinado facto ilícito se superioriza aos riscos a que estão sujeitos (Radosteva, 2020). Fatores como iluminação, visibilidade e sentimento de falta de medidas de segurança influenciam diretamente a escolha do alvo (Nagin et al., 2024).

Para além da localização, o horário ou período do dia revela-se igualmente determinante na incidência de determinados crimes. O principal fator está associado às rotinas diárias da população. Estas variam ao longo do dia, influenciando os níveis de vigilância nos espaços públicos, quer exercida por FS ou por empresas de segurança privada, quer pela vigilância natural proporcionada pela presença e atividade dos cidadãos (Thomas et al., 2024).

Durante o dia, a maior circulação de pessoas nas ruas tende a reduzir a probabilidade de crimes mais violentos. Já durante o período noturno, principalmente durante a madrugada, a menor presença de testemunhas e de policiamento, favorece a prática de crimes mais violentos (Sánchez-Delgado, 2024). Neste contexto, é fundamental que as políticas de prevenção criminal sejam dinâmicas e ajustáveis, adaptando-se às diferentes fases do dia e do ano, de modo a responder de forma eficaz às variações nos padrões de criminalidade (Almeida et al., 2023).

Estas teorias contribuem para a compreensão de que o crime não ocorre de forma aleatória. Determinados locais ou objetos, devido às suas características específicas, associadas à natureza do fenómeno criminal e ao MO de certos indivíduos ou grupos, apresentam uma maior propensão para se tornarem alvo de determinados tipos de crime.

A prevenção situacional¹¹, estreitamente relacionada com Teoria da Escolha Racional e com a Criminologia Ambiental (Radosteva, 2020), é entendida como todas as medidas “(...) dirigidas a formas de crime altamente específicas que envolvem a gestão, design ou manipulação sistemática e permanente do ambiente, de modo a reduzir as oportunidades do crime e aumentar os riscos para o criminoso (...)” (Clarke, 1983, p. 225).

Esta estratégia, direcionada para tipos específicos de crime, baseia-se na sua principal premissa: a redução de oportunidades para a prática de crimes (Cornish & Clarke, 2003). Tal

¹¹ A prevenção situacional é uma das principais abordagens na prevenção do crime, identificada por Tonry e Farrington (1995).

é alcançado através da manipulação dos locais ou infraestruturas onde esses crimes ocorrem, com o objetivo de dificultar a ação criminosa. Para isso, procura-se aumentar o esforço necessário, elevar os riscos envolvidos e, simultaneamente, reduzir as potenciais recompensas (Clarke, 1992; Cozens et al., 2005). Em suma, a prevenção situacional permite diminuir a incidência de crimes por meio da gestão eficiente dos espaços e da implementação de medidas de segurança (Lynch et al., 2018).

1.2. Tipos de Criminalidade

Alguns crimes são perpetrados por redes organizadas e hierarquizadas com atuação transnacional¹², enquanto outros envolvem indivíduos ou grupos com intervenção circunscrita a contextos locais. Importa reconhecer que existem variações significativas quanto à sua estrutura, *Modus Operandi* (MO), grau de organização, âmbito territorial e mobilidade dos seus perpetradores.

Quando falamos em indivíduos que procuram oportunidades fruto da negligência na segurança por exemplo em residências, como janelas abertas ou destrancadas, ou então que sejam de fácil arrombamento falamos em criminalidade local (Silva, 2023).

Na criminalidade local, não existe um prévio planeamento ou reconhecimento, o MO é pouco sofisticado, recorrendo a modos de atuação rudimentares, em alguns casos movimentando-se inclusive através de transportes públicos ou então em viaturas furtadas, e em regra, praticando os crimes a curtas distâncias do seu local de residência (até 15 km) (Silva, 2023).

No entanto uma das principais ameaças ao Estado de Direito, é a criminalidade organizada, pela sua atuação transnacional, bem como pela elevada complexidade e sofisticação que estas organizações criminosas possuem. (Alperstedt et al., 2022).

Atualmente, não existe uma definição absoluta de criminalidade organizada, dada a complexidade deste fenómeno (Europol, 2017b). Contudo, desde 2000, a Convenção¹³ das Nações Unidas contra o Crime Organizado Transnacional¹⁴ (Convenção de Palermo¹⁵) tem

¹² Segundo o n.º 2 do art.º 3 da Convenção das Nações Unidas Contra a Criminalidade Organizada Transnacional uma infração será de carácter transnacional se: a) For cometida em mais de um Estado; b) For cometida num só Estado, mas uma parte substancial da sua preparação, planeamento, direção ou controlo tenha lugar noutro Estado; c) For cometida num só Estado, mas envolva a participação de um grupo criminoso organizado que pratique atividades criminosas em mais de um Estado; ou d) For cometida num só Estado, mas produza efeitos substanciais noutro Estado.

¹³ A Convenção “tem como objeto promover a cooperação para prevenir e combater mais eficazmente a criminalidade organizada transnacional” (art.º 1 da Convenção de Palermo).

¹⁴ Aprovada em nome da Comunidade pela Decisão do Conselho 2004/579/CE, de 29 de abril de 2004

¹⁵ Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional – Disponível em <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>

fornecido uma definição¹⁶ amplamente aceite de grupo criminoso organizado (GCO): “(...) um grupo estruturado¹⁷, de três ou mais pessoas, existente por um período de tempo e atuando concertadamente com o objetivo de cometer crimes graves¹⁸, visando obter, direta ou indiretamente, um benefício económico ou material (...)”. Esta definição foi posteriormente adotada pela Decisão-Quadro 2008/841/JAI¹⁹ do Conselho da União Europeia e continua a ser utilizada pelas autoridades internacionais no combate à criminalidade organizada (SOCTA, 2017).

A criminalidade organizada caracteriza-se por uma grande diversidade²⁰ quer de organização quer no modo de atuação. Estas organizações não são estáticas, evoluem continuamente, ajustando-se a novos contextos e capacitando-se para explorar novas oportunidades, inclusive em diferentes territórios, quando necessário (Wyatt et al., 2020; Allum, 2025).

Mais de 80% das redes de criminalidade organizada identificadas estão envolvidas em tráfico de droga, crimes contra a propriedade²¹, fraude fiscal, tráfico de seres humanos, fraudes e contrabando de migrantes. Os crimes contra a propriedade envolvem a prática sistemática e reiterada de furtos ou assaltos por grupos organizados. Entre os crimes mais comuns incluem-se os furtos a ATM, furtos de cargas em veículos, furtos em lojas, carteirismo e furtos de metais (Europol, 2021).

Os grupos de criminalidade organizada móvel²², deslocam-se entre regiões e países com o objetivo de praticarem crimes contra a propriedade de forma organizada. Estes grupos caracterizam-se pela sua elevada adaptabilidade e mobilidade, conseguindo alternar entre diferentes tipologias criminais. Esta alternância depende frequentemente da época do ano, das oportunidades disponíveis e das condições do mercado (Europol, 2021).

¹⁶ Cfr. al. a) do art.º 2 da Convenção de Palermo.

¹⁷ Grupo estruturado – “um grupo formado de maneira não fortuita para a prática imediata de uma infração e cujos membros não tenham necessariamente funções formalmente definidas, podendo não haver continuidade na sua composição nem dispor de uma estrutura desenvolvida” (al. c) do art.º 2 da Convenção de Palermo).

¹⁸ Crime grave – “um ato que constitua uma infração punível com uma pena privativa de liberdade não inferior a quatro anos ou com pena superior” (al. b) do art.º 2 da Convenção de Palermo).

¹⁹ Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008F0841>

²⁰ As diferenças entre GCO, deve-se a uma grande diversidade de atividades desenvolvidas por estes, proporcionando uma multiplicidade de estruturas, variando entre estruturas muito hierarquizadas e outras extremamente flexíveis e voláteis (Elias, 2022). Estas organizações variam também quanto ao número de elementos, podendo operar a diferentes escalas, com dinâmicas próprias e diferentes MO (Muggah & Diniz, 2013; Wyatt et al., 2020).

²¹ O crime organizado contra a propriedade é apontado como o mais visível, devido ao seu impacto direto sobre os cidadãos, bem como sobre os setores público e privado (Europol, 2021).

²² *Mobile Organised Crime Groups – MOCGs*

CAPÍTULO II – FURTO A ATM

Os crimes que têm por objeto equipamentos ATM podem assumir diversas formas, desde roubos²³ direcionados aos utilizadores durante as operações de levantamento de dinheiro, tentativa de obtenção ilícita de dados pessoais e bancários, através por exemplo da clonagem de cartões multibanco, roubos contra funcionários das empresas responsáveis pelas operações de abastecimento das ATM, bem como furto do dinheiro acondicionado no cofre ou caixa de segurança da ATM através de diversos MO (Scott, 2006; SSI, 2013).

Cada fenómeno dever ser estudado de forma isolada, diferenciado dessa forma os diferentes crimes associados a ATM, potenciando assim uma resposta adequada a cada problema (Scott, 2006). Este TIA versa sobre os ataques realizados ao próprio ATM com o objetivo de retirar o dinheiro armazenado no mesmo quer através dos designados ataques físicos quer através dos ataques lógicos, onde há numa fase inicial o uso da força para aceder aos componentes da ATM.

2.1. Modus Operandi de furtos a ATM

A European Association for Secure Transactions²⁴ (EAST), constituída²⁵ pela Europol²⁶, pela Interpol²⁷, entre outras organizações,²⁸ e por 32 países membros²⁹, inclusive Portugal e outros 26 países europeus, criou o EAST Expert Group on ATM and ATS Physical Attacks (EGAP)³⁰, com objetivo de promover a cooperação entre o setor financeiro e as FS através da análise de novas tendências de ataque a ATM, definição de MO e formulação e coordenação de ações conjuntas para reduzir os ataques físicos (EAST, 2024).

Não obstante dos MO associados a esse tipo de crime evoluírem rapidamente (REPC & Europol, 2019), segundo as definições e terminologias adotadas no *Terminal Physical*

²³ O crime de furto (Art.º203 do Código Penal Português) consiste na subtração de coisa móvel alheia sem uso de violência ou ameaça, enquanto o crime de roubo (Art.º 210 do Código Penal Português) consiste na subtração de coisa móvel alheia com recurso a violência, ameaça grave ou coação sobre a vítima.

²⁴ Associação Europeia de Transações Seguras

²⁵ Disponível em <https://www.association-secure-transactions.eu/east-membership/>

²⁶ Agência da União Europeia para a Cooperação Policial

²⁷ Organização Internacional de Polícia Criminal

²⁸ BNP Paribas, HSBC, Loomis, Netcetera e Worldline

²⁹ Áustria, Bélgica, Chéquia, Chipre, Dinamarca, Finlândia, França, Alemanha, Grécia, Hungria, Irlanda, Itália, Liechtenstein, Luxemburgo, Malta, Países Baixos, Noruega, Polónia, Portugal, Romênia, Eslováquia, Espanha, Suécia, Suíça, Reino Unido. Brasil, Canadá, Indonésia, México, Sérvia, Turquia, Ucrânia.

³⁰ Disponível em <https://www.association-secure-transactions.eu/about-east/>

*Attack Definitions & Terminology*³¹ desenvolvido pelo EGAP, e adotadas neste TIA, os furtos a ATMs podem ser separados em duas grandes categorias: ataques físicos e ataques lógicos.

Os ataques físicos a ATM centram-se na extração de dinheiro das ATM, através de métodos que violam fisicamente, a caixa de segurança ou cofre, compartimento onde está acondicionado dinheiro (EGAP, 2023; NCR, 2018). Por outro lado os ataques lógicos recorrem a ataques informáticos que permitem retirar o dinheiro acondicionado no ATM sem ter de abrir o cofre onde o dinheiro está acondicionado (Europol, 2017a), podendo, no entanto, ser necessário que haja um acesso físico à ATM, sobretudo aos componentes que controlam a mesma (REPC & Europol, 2019).

2.1.1. Ataque físicos

A EGAP subdivide os ataques físicos em:

- Ataques explosivos;
- Furtos da ATM – no local;
- Furtos da ATM – arrancamento;
- Ataques não específicos.

Os ataques explosivos (*explosive attacks*)³², consistem na abertura do cofre da ATM recorrendo a diferentes tipos de materiais explosivos. Estes tipos de ataques acontecem rapidamente e muitas vezes causam danos avultados quer na ATM como nas imediações. Este tipo de ataque subdivide-se em ataques com explosivos gasosos e com explosivos sólidos (EGAP, 2024).

Nos ataques com explosivos gasosos há uma introdução de uma mistura de gás, normalmente gases hidrocarbonetos, sendo o mais comum a oxiacetileno, no cofre da ATM, seguida de uma ignição que permitirá abrir a porta da caixa de segurança ou cofre.

Nos ataques com explosivos sólidos, o mais comum é o uso de dinamite, gelignite, explosivo plástico (tipo massa), como o C4, e explosivos emulsificados, como o power gel. Neste tipo de ataques, especialmente quando há o recurso a explosivos sólidos podem ser realizadas duas explosões. Uma primeira destinada a criar uma abertura na estrutura da ATM, e uma segunda para abrir a caixa de segurança ou cofre (ATMIA, 2014a).

³¹ Disponível em <https://www.association-secure-transactions.eu/industry-information/terminal-physical-attack-definitions-terminology/>

³² ou também designados de Plofkraak

Contrariamente aos cofres tradicionais que são completamente fechados, a caixa de segurança ou cofre de uma ATM possui orifícios que permitem a movimentação de dinheiro entre a ATM e o consumidor, além da passagem de cabos que fornecem energia e controlo aos módulos no interior da estrutura de segurança. Estes orifícios, no entanto, são também utilizados pelos perpetradores para introduzir os explosivos dentro da ATM (ATMIA, 2014a).

A forma mais comum de introduzir explosivos seja gás ou explosivos sólidos nas ATM, especialmente nas ATM integrados na parede (*Through the Wall*) é através da abertura forçada do *shutter*³³ (ATMIA, 2014a).

Os métodos mais recorrentes para se dar abertura forçada do *shutter*, é através do uso de ferramentas, como o pé de cabra ou uma chave de fendas com objetivo de o partir ou dobrar. Em alguns casos podem também optar por cortar ou perfurar o *shutter*, ou então junto do mesmo (ATMIA, 2014a). Após a abertura do *shutter*, introduzem o gás explosivo, para a caixa de segurança ou cofre, através de tubos ou canos de pequeno diâmetro ligados a umas botijas de gás. O *shutter* é igualmente utilizado para introduzir o fio elétrico, o qual se encontra ligado a uma fonte de alimentação, geralmente uma bateria de um automóvel, que é responsável por fornecer a ignição necessária à deflagração do gás introduzido no interior do equipamento, provocando assim uma explosão e subsequente abertura do cofre da ATM (ATMIA, 2014a).

Nos casos dos explosivos sólidos, que geralmente são maiores do que os tubos utilizados para introduzir o gás explosivo, é mais comum que o perpetrador insira a carga explosiva sólida partindo os *shutters* ou através de um levantamento de dinheiro, recorrendo recorrentemente a cartões multibanco pré-pagos, aproveitando o momento em que a ATM abre o *shutters* para fornecer as notas ao utilizador da ATM para introduzir o explosivo no interior da ATM (ATMIA, 2014a).

Nos casos em que conseguem aceder à parte posterior de uma ATM, independentemente de esta se encontrar integrada numa parede ou isolada (*free-standing*), aumentam significativamente as possibilidades de explorarem os orifícios destinados à cablagem como ponto de entrada para comprometer a integridade estrutural do equipamento. Embora a maioria desses orifícios apresente dimensões reduzidas, impedindo a introdução de quantidades suficientes de explosivos sólidos e respetivos detonadores, são, por vezes, suficientemente amplos para permitir a inserção de tubos e fios elétricos utilizados em

³³ Consiste na tampa ou barreira metálica que protege a abertura por onde o dinheiro é disponibilizado ao utilizador da ATM (ATMIA, 2014a)

ataques com recurso a gás explosivo. A principal vantagem desta abordagem reside na possibilidade de preparar o ataque sem causar danos estruturais visíveis na ATM, o que contribui para evitar a ativação prematura de sistemas de alarme ou de outras medidas de segurança antes da deflagração (ATMIA, 2014a).

Este tipo de ataque pode requerer apenas um minuto para a introdução de uma quantidade suficiente de gás ou para a colocação de uma carga explosiva sólida na estrutura de segurança da ATM. A detonação e o subsequente acesso ao numerário, quando executados por indivíduos com experiência, podem ser concretizados em cerca de quatro minutos (ATMIA, 2014a).

Já nos designados Furtos da ATM - no local (*ATM Burglary - In-Situ*) a abertura forçada do cofre da ATM é realizada no próprio local onde esta se encontra instalada, recorrendo a diversas ferramentas e técnicas. Este tipo de ataque subdivide-se em diferentes categorias, previstas no Quadro n.º 1, consoante os métodos ou equipamentos utilizados para comprometer a estrutura de segurança da ATM.

Quadro n.º 1 - Subtipos de Furtos da ATM – no local

Furtos da ATM – no local	
Corte com maçarico	Utilização de um maçarico para abrir o cofre
Perfuração	Utilização de uma broca para abrir o cofre
Corte	Utilização de uma serra ou rebarbadora para abrir o cofre
Arrombamento	Utilização de pés de cabra ou expansores hidráulicos para forçar a abertura do cofre
Extração da porta do cofre	A porta do cofre é arrancada com a ajuda de um veículo através de um guincho ou de uma corrente que é presa à porta do cofre

Fonte: EGAP (2023)

Por outro lado, alguns grupos optam por remover a ATM do local onde se encontra instalada, num método designado de Furtos da ATM - arrancamento (*ATM Thef - Rip Out*). Regra geral, a abertura do cofre ocorre posteriormente, já noutra localização. Este método envolve frequentemente o recurso a veículos industriais, utilizados principalmente para retirar a máquina do local onde está fixada a ATM (REPC & Europol, 2019).

Por último, num ataque não específico (*Non - Specific Attack*), estamos perante um ataque a uma ATM que não resultou no furto do dinheiro armazenado na mesma. Neste tipo de ocorrências não pode ser atribuído um tipo específico de ataque. Podemos estar inclusive perante uma situação de crime de dano, vandalismo ou furto de componentes (EGAP, 2024).

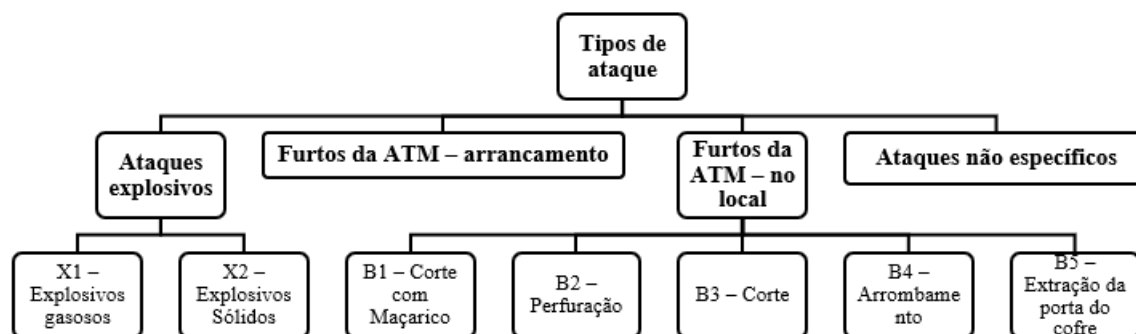


Figura n.º 1 - Terminologia de ataques físicos a ATM

Fonte: EGAP (2024)

2.1.2. Ataques lógicos

Segundo “*Guidance and recommendations regarding logical attacks on ATMs: Mitigating the risk, setting up lines of defence identifying and responding to logical attacks*” da Europol um ataque lógico (*logical attack*) a uma ATM ou a uma rede de ATMs é definido como um “(...) conjunto coordenado de ações maliciosas realizadas por indivíduos ou organizações criminosas com o objetivo de obter acesso aos sistemas informáticos ou componentes das ATM, com a finalidade de extrair dinheiro ou dados sensíveis da ATM (...)” (2018, p.4).

Uma subcategoria dos ataques lógicos são os ataques com recurso a *malware*³⁴. Nestes ataques³⁵ o objetivo é instalar um *software*³⁶ no computador (PC) da ATM, de modo a que o *software* seja executado em segundo plano enquanto a ATM funciona normalmente (Europol, 2018, p.4).

As ATM, independentemente do fabricante, salvo algumas exceções, têm estruturas de funcionamento semelhante (Figura n.º 2). Esta particularidade leva a que, em regra, todas as ATM estejam em risco de sofrerem ataques de *malware* (Europol, 2017). As ATM são compostas por um mecanismo de dispensa de dinheiro (1-Dispensador) controlado por um

³⁴ É um tipo de software desenvolvido com a intenção de causar danos, acessar informações sem autorização ou comprometer sistemas (Skoudis & Zeltser, 2021).

³⁵ Existem duas variações principais de ataques com malware a ATMs (NCR, 2018): ataques online, realizados com o sistema operativo em funcionamento, geralmente através de uma pen disk ou com recurso a uma palavra-passe de administrador do Windows (Europol, 2017a); e ataques offline, executados com o sistema desligado, recorrendo a um dispositivo externo (como um portátil ou minicomputador) ligado diretamente aos componentes do ATM, ou ao acesso direto ao sistema operativo. Os ataques offline podem ainda ser usados para preparar ataques online, por exemplo para desativar medidas de segurança (Europol, 2018).

³⁶ Conjunto de instruções e dados que controlam o hardware e executam tarefas específicas (Silberschatz et al., 2018).

sistema operativo através de um pc (2-PC), localizado no compartimento superior da ATM. PC esse que está simultaneamente ligado a um *host*³⁷ externo (3-Host) e ao dispensador de dinheiro (Europol, 2018).

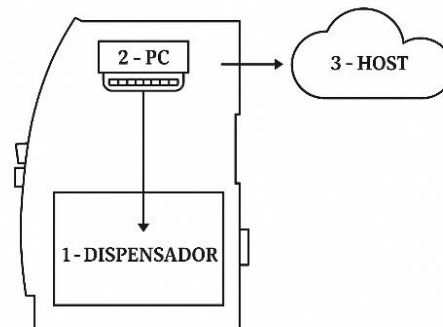


Figura n.º 2 - Estrutura ATM

Fonte: Europol (2017a, p.5)

Segundo o “*Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types*” da TrendMicro em conjunto com a Europol, os ataques lógicos podem ser divididos em ataques cujo o acesso ao ATM é feito por meio físico³⁸ ou acesso via rede³⁹. No entanto, este TIA prende-se apenas com o primeiro tipo de ataque.

Quando se trata de ataques onde é necessário o acesso físico à ATM, podemos categorizar os ataques a ATM com *malware* relativamente ao seu MO da seguinte forma (Europol, 2017):

O *Jackpotting*,⁴⁰ que é o termo utilizado para descrever os ataques em que o *malware* introduzido no ATM assume o controlo do PC da ATM e da função de dispensadora do dinheiro, permitindo dessa forma retirar diretamente o dinheiro. Na maioria dos casos, o *malware* é adaptado a um ambiente específico, isto é, a um fabricante, *software* ou características específicas da ATM, no entanto pode ser adaptado para diferentes ambientes (Europol, 2017a).

³⁷ Refere-se a qualquer dispositivo (geralmente um computador, servidor ou máquina virtual) conectado a uma rede, que possui um endereço IP e é capaz de enviar, receber ou processar dados (Tanenbaum & Wetherall, 2011).

³⁸ Através da utilização de ferramentas que permitam a abertura da ATM como berbequins com brocas cranianas e maçaricos ou então através das chaves ou réplicas usadas na manutenção destas máquinas.

³⁹ Geralmente envolvem a intrusão prévia na rede corporativa do banco, permitindo posteriormente o controlo remoto da ATM (TrendMicro & Europol, 2017).

⁴⁰ Também conhecido por *cash out attack*.

O *Black Box* é uma variante do *Jackpotting*, no entanto neste tipo de ataques o PC da ATM não é utilizado, em vez disso, é utilizado um dispositivo externo que pode ser um dispositivo eletrónico com um *hardware*⁴¹ bastante simples, de baixo custo e tamanho reduzido como uma *pen disk* ou dispositivo *Raspberry Pi*⁴², até dispositivos mais sofisticados como computadores portáteis modificados, smartphones e tablets (ATMIA, 2014b). Independentemente do dispositivo utilizado, o objetivo é intersear a comunicação entre o computador da ATM e a unidade dispensadora de dinheiro (Europol, 2017b).

Existe uma grande diversidade de MO neste tipo de ataques, não obstante, a grande maioria dos ataques atualmente observados requerem acesso físico ao ATM. Essencialmente, o ataque divide-se em duas fases.

Numa primeira fase é necessário ter acesso ao interior da ATM de forma a ser possível conectar ou instalar os dispositivos que permitam controlar a ATM (Europol, 2017b). Esse acesso pode acontecer de várias formas: através de uma chave, pode ser verdadeira ou uma réplica semelhante às utilizadas pelas equipas de manutenção para abrir a ATM; através de um funcionário das empresas responsáveis pela manutenção e pelo abastecimento destas máquinas que dissimuladamente conectam o dispositivo; ou através do uso da força, recorrendo para isso a instrumentos como pés de cabra para forçar abertura da ATM ou ainda através do uso de maquinaria, normalmente com o objetivo de realizar um buraco que permita ter acesso ao PC que controla a ATM, que em regra, está instalado na parte superior da ATM, zona essa com menor proteção em relação ao cofre, recorrendo por tal recorrentemente a berbequins e a maçaricos (ATMIA, 2014b ; Fraile et al., 2016).

Numa segunda fase conectam o dispositivo externo que vai carregar um *malware* que vai explorar as vulnerabilidades de um *firmware* desatualizado para dar comandos à ATM para que esta dispense o dinheiro (Europol, 2017b). O intervalo entre a instalação do *malware* e a sua utilização pode variar, ocorrendo de forma imediata ou, em alguns casos, com um atraso significativo. Além disso, o *malware* pode permanecer no sistema por um período prolongado ou pode inclusive já estar pré-programado para ser removido logo após a sua execução (TrendMicro & Europol, 2017).

Ao longo do tempo foram sendo desenvolvidos diferentes *malwares* com o objetivo de desenvolver este tipo de ataques. Cada *malware* foi desenvolvido para dar resposta a determinadas características das ATM, explorar determinadas vulnerabilidades das ATM,

⁴¹ É a parte física de um sistema de computação. Inclui todos os componentes tangíveis, como o processador, memória RAM, disco rígido, placa-mãe, teclado, monitor, entre outros (Stallings, 2018).

⁴² Microcomputador de baixo custo e tamanho reduzido.

seja determinados fabricantes, seja determinado *software*⁴³ ou até as características físicas da ATM ou dos respetivos componentes (TrendMicro & Europol, 2017).

Quadro n.º 2 - Tipos de *malware* para ataques lógicos

Malware	Alvo	Características do Sistema
Skimer	Diebold (fabricante de ATM) mais antigos com Windows XP	Primeiro <i>malware</i> de ATM conhecido e ainda ativo com várias evoluções. Permite não só ativar o dispensador de dinheiro como permite a clonagem de cartões e códigos PIN.
Ploutus	NCR (fabricante de ATM) e multifornecedor com XFS ¹	Permite através de SMS ativar o dispensador do ATM, possui uma arquitetura modular o que permite adaptação para multimarca/fornecedor.
Padpin / Tyupkin	NCR com Windows XP e McAfee Solidcore	Permanece adormecido até receber um comando específico. São usados códigos de autenticação temporários e horários específicos, em regra entre 1h e 5h da manhã, para reduzir o risco de deteção
GreenDispenser	Qualquer modelo com XFS e fraca proteção física	O ATM exibe uma mensagem no ecrã indicando que a máquina está fora de serviço, com o objetivo de camuflar o ataque. No <i>malware</i> encontra-se ativo e pronto para ser controlado por atacantes. Após o ataque apaga-se automaticamente
Alice	Qualquer ATM com XFS e acesso físico facilitado	Dispensa rápida de dinheiro via teclado físico, sem necessidade de instalação complexa. Ataques rápidos e discretos; foco total em <i>jackpotting</i> .

Fonte: (TrendMicro & Europol, 2017)

2.2. Contexto Europeu

No último relatório europeu da EAST relativo a Crimes em Terminais de Pagamento⁴⁴ referente a 2023, verificou-se um aumento nos ataques físicos a ATM, que aumentaram 24% (de 3.728 para 4.637)⁴⁵, quando comparado com o ano anterior, aumento esse que na última década só é superado em 2015 e 2018.

⁴³ XFS (eXtensions for Financial Services) é um *software* intermédio, conhecido como *middleware*, utilizado em ATM, funcionando como uma ponte entre o software bancário e os componentes físicos do equipamento, tais como o leitor de cartões, o teclado PIN, a impressora de talões e o dispensador de dinheiro. A sua principal função é permitir que o *software* comunique e controle estes dispositivos, mesmo quando são provenientes de diferentes fabricantes (TrendMicro & EUROPOL, 2017).

⁴⁴ Disponível em <https://www.association-secure-transactions.eu/atm-physical-attacks-rise-in-europe/>

⁴⁵ Dentro deste total, os ataques furtos da ATM – arrancamento / furtos da ATM – no local aumentaram 5% (de 484 para 506 incidentes), enquanto os ataques explosivos diminuíram 2% (de 727 para 714 incidentes). Quando analisados os dados de anos anteriores (Tabela nº4) é possível verificar que de 2015 a 2019, houve um aumento constante nos ataques físicos, atingindo um pico em 2019 (4.571 ataques). Já em 2020, houve uma queda expressiva de 19%, seguida por oscilações nos anos seguintes, acabando por voltaram a subir significativamente (+24%) em 2023.

O *Serious and Organised Crime Threat Assessment (SOCTA)*⁴⁶ refere que alguns Estados Membros reportaram um aumento na utilização de explosivos sólidos em ataques a ATM (2025). A pirotecnia com elevada potência, obtida de forma ilícita, tem sido cada vez mais empregue por GCO como meio de ataque a ATM, funcionando como carga explosiva para comprometer fisicamente os cofres e os mecanismos de segurança. Este tipo de material, devido à sua disponibilidade no mercado ilegal e à sua elevada capacidade destrutiva, constitui um vetor significativo na intensificação deste tipo de criminalidade, representando um desafio crescente para as FS (Europol, 2025).

Por outro lado, os ataques lógicos a ATM diminuíram 77% (de 31 para 7) em 2023. Analisando os ataques entre 2015 a 2023 é possível verificar que estes tipos de ataques aumentaram drasticamente até 2017, mas a partir de 2018 têm registado progressivamente uma diminuição deste tipo de ataques (Tabela n.º 1).

Tabela n.º 1 - Furtos a ATMs na Europa entre 2015 a 2023

Ano	2015	2016	2017	2018	2019	2020	2021	2022	2023
Ataques físicos	2657	2974	3584	4549	4571	3722	3947	3728	4637
Variação anual	-	+12%	+21%	+27%	+0.5%	-19%	+6%	-6%	+24%
Ataques lógicos	15	58	192	157	140	202	52	31	7
Variação anual	-	+287%	+231%	-18%	-10%	+44%	-74%	-40%	-77%

Fonte: EAST (2015 a 2023)

Na Europa, tal como se pode verificar na Figura n.º 3, contrariamente aos ataques físicos os ataques lógicos têm vindo a cair drasticamente, em 2023 registaram-se apenas sete ataques contra os 4637 ataques físicos.

⁴⁶ Relatório de Avaliação da Ameaça do Crime Grave e Organizado na União Europeia - relatório com o objetivo de fornecer uma avaliação completa e exaustiva das ameaças de crime graves e organizado, identificando as áreas em que a resposta do Estado e de quem o representa, como neste caso em específico as FS, se deve direccionar.

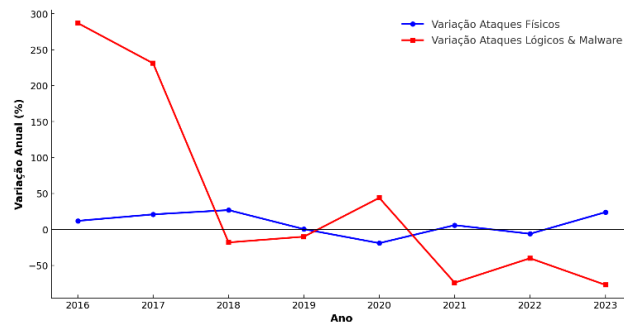


Figura n.º 3 - Variação ataques físicos e lógicos

Fonte: EAST (2016 a 2023)

Ao contrário de outros tipos de furtos mais comuns, dentro dos crimes contra o património, como furtos em residências ou em viaturas, que dependem fundamentalmente da recetação⁴⁷, dos bens furtados, isto é, venda e a obtenção de materiais obtidos através de factos ilícitos, como é o caso dos objetos furtados, no caso dos furtos a ATM o acesso ao dinheiro é imediato.

Este acesso imediato ao dinheiro elimina a necessidade de uma extensa rede de venda de bens furtados, uma vantagem logística e operacional significativa reduzindo os riscos e simplificando substancialmente a execução destes furtos (Europol, 2021). Esta particularidade torna as ATM alvos especialmente atrativos, sobretudo para as redes de criminalidade organizada que se dedicam a crimes contra o património (Europol, 2021).

2.3. Contexto Nacional

Segundo o Relatório Anual de Segurança Interna (IASI)⁴⁸, no período compreendido entre 2016 e 2024 foram registados em Portugal 644 furtos a ATM, sendo que o distrito de Lisboa regista o maior número de ocorrências, seguida dos distritos Porto e Setúbal.

⁴⁷ O crime de recetação consubstancia-se na conduta de quem, com a intenção de obter vantagem patrimonial, própria ou de terceiro, dissimula, adquire, recebe, detém, conserva, transmite, contribui para a transmissão ou, por qualquer meio, assegura a posse de coisa ou animal que tenha sido obtido por outrem mediante a prática de facto ilícito típico contra o património, ainda que não tenha participado na infração antecedente (Art.º 231 do Código Penal Português).

⁴⁸ Documento que reúne anualmente os dados mais atuais das tipologias criminais mais gravosas em Portugal, dentro dos crimes de furto, na última década tem vindo a dar alguma relevância a furtos a ATM, apresentando anualmente dados específicos sobre este fenómeno, demonstrativo do impacto social deste tipo de furtos.

Tabela n.º 2 - Furtos ATM em Portugal entre 2016 a 2024

Ano	2016	2017	2018	2019	2020	2021	2022	2023	2024	Total
RASI	262	203	27	37	25	14	21	24	33	1672
	+21,30%	-22,52%	-86,70%	+37,04%	-32,43%	-44,00%	+50,00%	+14,29%	+37,2%	-

Fonte: RASI (2016 a 2024)

Dentro deste espaço temporal, é possível observar na Figura n.º 4 que o pico do número de furtos ocorreu em 2016 e 2017, seguida de uma queda acentuada em 2018. A partir de 2018 têm-se registado uma certa estabilidade no número de furtos, no entanto, nos últimos quatro anos, têm se registado de forma consecutiva um aumento no número de furtos a ATM, contrariando o que se vinha a verificar nos três anos anteriores.

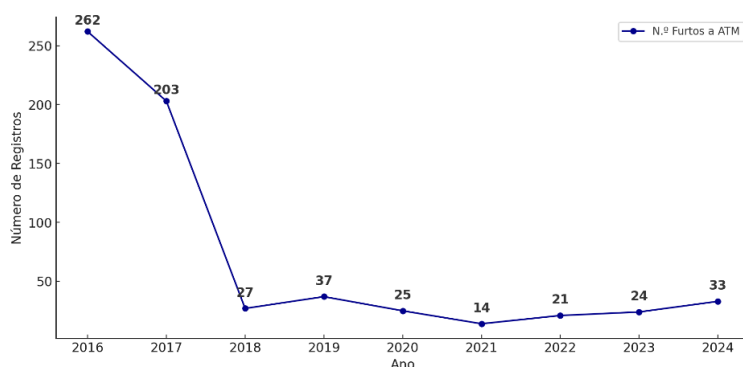


Figura n.º 4 - Evolução furtos de ATM em Portugal

Fonte: RASI (2012 a 2024)

Segundo os dados fornecidos pelo Relatório de Atividades da GNR (RAGNR), na área de jurisdição da GNR, entre 2016 a 2022 (último relatório disponível), foram contabilizados 195 furtos a ATMs. Após o pico de 2017 que registou um total de 96 furtos a ATM, os furtos a ATM têm vindo a estabilizar, apesar do ligeiro aumento em 2022, face ao ano anterior.

Tabela n.º 3 - Furtos ATM na área de jurisdição da GNR entre 2016 a 2022

Ano	2016	2017	2018	2019	2020	2021	2022	Total
RAGNR	27	96	10	15	12	14	21	-

Fonte: RAGNR (2016 a 2022)

Ainda assim, quando comparados os dados disponíveis no RASI e RAGNR (Figura n.º 5), em 2016, que corresponde ao pico de furtos no espaço temporal analisado, é possível observar que apenas sensivelmente 10% dos furtos ocorreram na área da GNR. A partir de 2017 tem - se registado um aumento significativo dessa percentagem. Entre 2017 e 2020 a média de furtos ocorridos na área da GNR corresponde a cerca de 43% do total de furtos registados em território nacional, uma subida bastante significativa quando comparada com o biénio anterior (2015 e 2016, onde a média era aproximadamente de 7%). De sublinhar ainda, que no biénio de 2021 e 2022, a GNR registou na sua zona de atuação a totalidade dos casos registados a nível nacional.

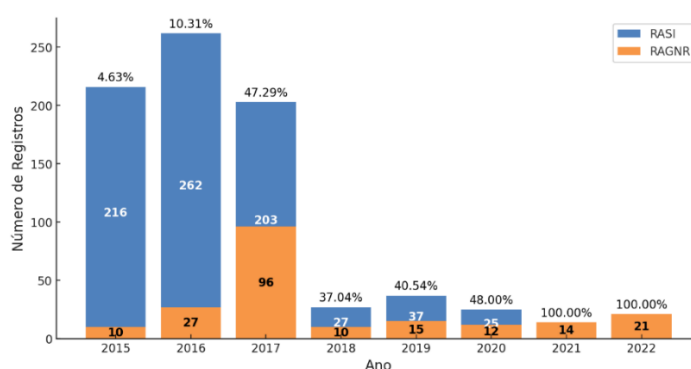


Figura n.º 5 - Comparação entre RASI e o RAGNR relativamente a furtos a ATM

Fonte: RASI 2015 a 2022 e RAGNR 2015 a 2022

2.4 Enquadramento jurídico

O furto a ATM em Portugal, em termos de classificação de legislação penal, integra a categoria de “Crimes contra o património”, tipificado como “furto qualificado”⁴⁹, nos termos do Art.º 204.º do Código Penal Português (CPP)⁵⁰.

⁴⁹ Este artigo prevê a qualificação do furto nos casos em a coisa móvel furtada se encontra “fechada em gaveta, cofre ou outro receptáculo equipados com fechadura ou outro dispositivo especialmente destinado à sua segurança” (d) do n.º 1 do Art.º 204.º do CPP). O mesmo artigo prevê a qualificação do furto caso haja introdução “(...) ilegítimamente em (...) estabelecimento comercial ou industrial ou espaço fechado (...)” (Art.º 204.º, n.º1, f) do CPP) ou “penetrando em (...) estabelecimento comercial ou industrial ou outro espaço fechado, por arrombamento, escalamento ou chaves falsas.” (e) do n.º 2 do Art.º 204.º do CPP). Dentro das condutas que qualificam o crime de furto de referir ainda “(...) trazendo, no momento do crime, arma aparente ou oculta” (f) do n.º 2 do Art.º 204.º do CPP).

⁵⁰ Cfr: Código Penal Português, aprovado pelo Decreto-Lei n.º 48/95, de 15 de março, com a última alteração introduzida pela Lei n.º 15/2024, de 29 de janeiro.

Segundo um estudo de caso realizado pela *Forward Payment Solutions, SA* (SIBS) para a *ATM Industry Association* (ATMIA), é ainda comum que os furtos a ATM estejam interligados com outras práticas criminais, nomeadamente no âmbito dos crimes de dano⁵¹ ou dano qualificado⁵², furto de viaturas, crime de “Incêndios, explosões e outras condutas especialmente perigosas”,⁵³ sobretudo nos casos em que o ataque é realizado com recurso a gás e explosivos (ATMIA, 2014a).

Em casos de grupos organizados, podem ainda estar em causa o crime por associação criminosa⁵⁴, para tal exige a congregação de um elemento organizativo, um elemento de estabilidade associativa e um elemento de finalidade criminosa. A tipificação como associação criminosa exige uma estrutura que lhe garante alguma estabilidade, perdura no tempo e evidencia um processo de formação de vontade coletiva e apresenta um sentimento comum de ligação a uma realidade autónoma (Acórdão do Tribunal da Relação do Porto⁵⁵).

Os ataques lógicos além dos crimes mencionados podem ainda ser tipificados ainda como “Sabotagem informática”⁵⁶ previsto na Lei do Cibercrime⁵⁷.

2.5. Fatores preponderantes para um furto a ATM

Fruto do número de furtos a ATM que afetavam cada vez mais países europeus, a Rede Europeia de Prevenção da Criminalidade⁵⁸ e a Europol desenvolveram um documento⁵⁹ designado na sua tradução oficial em português de “Prevenção de assaltos físicos nos terminais bancários: Desenvolvimento De Uma Abordagem Eficaz”⁶⁰.

A REPC & Europol (2019) destaca alguns fatores como preponderantes no sucesso do ataque físico a uma ATM: características da ATM, planeamento do furto e a experiência e conhecimentos (especialização) dos perpetradores.

⁵¹ Cfr. Art.º 212.º do Código Penal Português

⁵² Cfr. Art.º 213.º do Código Penal Português

⁵³ Cfr. Art.º 272.º do Código Penal Português

⁵⁴ Cfr. Art.º 299.º do Código Penal Português

⁵⁵ Acórdão do Tribunal da Relação do Porto, n.º 5148/20.2JAPRT-A. P1, de 10 de março de 2021. <https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/0f37c2312c5f51f3802586b6005a2f82?OpenDocument>

⁵⁶ Cfr. Art.º 5 da Lei do Cibercrime

⁵⁷ Lei do Cibercrime, aprovado pelo Lei n.º 109/2009, de 15 de setembro, com a última alteração introduzida pela Lei n.º 79/2021, de 24 de novembro.

⁵⁸ *European Crime Prevention Network – EUCPN*

⁵⁹ Este documento que resume as conclusões da conferência realizada por estas organizações, com o objetivo de debelar os furtos a ATM, e tem como finalidade aumentar a consciencialização sobre os furtos a ATM e introduzir eventuais medidas preventivas, em especial aos ataques físicos a ATM.

⁶⁰ Disponível em

https://www.Europol.europa.eu/sites/default/files/documents/preventing_physical_atm_attacks.pdf

A maioria das ATM mais vulneráveis estão localizados na parte exterior de um edifício, integrados nas paredes ou então instalado de forma autónoma/isolada no interior de um edifício. No segundo caso, os perpetradores tendem a privilegiar as ATM localizados em estabelecimentos comerciais, em detrimento das localizados em bancos, onde, habitualmente, existem um número maior de medidas de segurança. A localização da ATM tem um papel preponderante, influenciando diretamente o nível de risco e consequentemente atratividade para potenciais ataques.

O planeamento deste tipo de furtos pode estender-se ao longo de várias semanas, ou até mesmo meses, durante os quais reúnem o material e as ferramentas necessárias consoante o MO adotado. Antes de realizar o furto é comum que os perpetradores realizarem uma vigilância prévia tanto da ATM quanto das instalações onde ela está localizada (ATMIA, 2014a).

Embora o número de elementos varie, o mais comum é dois a três elementos, normalmente do sexo masculino (ATMIA, 2014a). Segundo o RAGNR para o ano de 2018, para a execução de um furto a ATM, depreende-se que cada ilícito necessite entre três a quatro indivíduos por ocorrência.

As viaturas assumem um papel determinante neste tipo de furtos, sendo utilizados tanto para a deslocação até local do furto como para a fuga subsequente, frequentemente em alta velocidade. É comum o furto ou em alguns casos o aluguer de automóveis de alta cilindrada, sendo recorrente optarem por veículos da marca Audi ou BMW, principalmente modelos de segmentos de maiores dimensões, como carrinhas. Em determinados locais, onde as medidas de segurança são mais elevadas, é comum estes grupos recorrerem ao arrombamento da porta através de uma viatura adicional, frequentemente viaturas todo o terreno 4x4 e máquinas de construção como escavadoras ou empilhadoras, previamente furtadas (ATMIA, 2014a).

No que respeita ao equipamento necessário, grande parte encontra-se disponível em estabelecimentos comerciais comuns, fator que reduz significativamente as barreiras para a prática deste tipo de furtos. Este facto dificulta o rastreamento da origem das ferramentas pelas FS. No entanto é comum os grupos que recorrem ao gás explosivo, comprarem, alugarem ou furtarem botijas de gás a fornecedores de equipamentos de soldagem e corte, ou então furtarem oficinas do ramo automóvel especificamente para a obtenção de botijas de gás e dos tubos utilizados para introduzir o gás no interior da ATM.

No caso dos explosivos sólidos pode exigir em alguns casos, furtos a instalações que armazenam esse tipo de material, no entanto a sua obtenção e dos respetivos detonadores necessários é geralmente mais difícil do que a obtenção de gás explosivo (ATMIA, 2014a).

Segundo a REPC & Europol (2019), os grupos que praticam este tipo de furtos a nível transnacional dispõem muitas vezes de pontos de contacto no país-alvo. Estes pontos de contacto são indivíduos residentes que asseguram o apoio logístico, como o alojamento, o fornecimento de viaturas e dos equipamentos necessários, bem como a identificação de potenciais alvos.

Estes grupos dedicam um esforço substancial à seleção criteriosa dos alvos, considerando variáveis como o horário de carregamento das ATM, o ambiente circundante, as especificações técnicas das ATM, os itinerários (possíveis rotas de fuga) e as medidas de segurança implementadas, nomeadamente os sistemas de videovigilância e os sensores de alarme.

Os autores deste tipo de ataques costumam monitorizar as equipas de transporte de valores que fazem o carregamento da ATM, ou então fazem a monitorização da própria ATM logo após o abastecimento de dinheiro. Em alguns casos, de forma a garantir o máximo lucro possível, acabam por inoperar a ATM para que não seja possível realizar qualquer levantamento. Para isso podem recorrer ao bloqueio do leitor de cartões para impedir movimentos, colocar um aviso falso na ATM informando que a ATM está fora de serviço. Além desta estratégia podem também desativar ou obstruir a imagem das câmaras de vigilância antes do ataque (ATMIA, 2014a).

Alguns destes grupos, de forma a aumentar as probabilidades de êxito, recorrem frequentemente a estratégias que dificultem a resposta das FS. As estratégias mais recorrentes são: a manipulação de sistemas de alarme e da iluminação pública, o bloqueio de vias de acesso ou então formas de impedir que as viaturas das FS se possam deslocar para a zona ou nas imediações da ATM.

A execução bem-sucedida deste tipo de furtos exige determinados conhecimentos técnicos consoante o MO utilizado. Alguns métodos, exigem um maior nível de conhecimentos técnicos, exemplo disso é o uso de gás ou explosivos sólidos que já pressupõem um domínio e conhecimento destes materiais.

Os grupos mais organizados e experientes conseguem executar um furto a uma ATM num curto espaço de tempo, reduzindo substancialmente os riscos a que estão sujeitos bem como reduzindo os danos colaterais. Por outro lado, os grupos menos organizados ou menos experientes, com carácter mais oportunista tendem a realizar tentativas que não são bem-

sucedidas, frequentemente causando danos significativos às infraestruturas envolventes. Em alguns dos casos, face às dificuldades em concretizar este tipo de furtos, estes grupos que não foram bem-sucedidos acabam por regressar a formas mais tradicionais de furtos.

Quando um ataque é abandonado, quer seja porque os atacantes foram detetados ou os explosivos utilizados não detonaram, podem existir indícios da tentativa de furto. O mais comum é danos nos *shutters* ou nos módulos de depósito (cortadas, perfuradas ou amassadas), marcas de queimaduras ou fuligem na ATM causadas por explosões parciais ou porventura danos no edifício, como portas ou fechaduras parcialmente destruídas (ATMIA, 2014a).

Apesar da taxa de sucesso deste tipo de furtos ser baixa, os danos causados, por exemplo às estruturas dos edifícios fruto do uso de explosivos são bastante significativos, resultando num ambiente de insegurança nos moradores (REPC & Europol, 2019).

2.6. Prevenção de furtos de ATM segundo o REPC e Europol

Segundo o “Prevenção de assaltos físicos nos terminais bancários: Desenvolvimento de uma abordagem eficaz” da REPC & Europol em conjunto com a Europol a estratégia de prevenção deve assentar em três etapas⁶¹: (1) avaliação da situação, com identificação dos principais riscos e vulnerabilidades das ATM; (2) desenvolvimento de uma abordagem preventiva, com base na análise de risco e na cooperação interinstitucional; e (3) implementação de medidas preventivas e operacionais, com vista à redução da probabilidade e da eficácia das ações criminosas.

A identificação de vulnerabilidades específicas nas ATMs constitui uma prática recorrente por parte de GCO, que tendem a selecionar alvos com características estruturais ou operacionais favoráveis à perpetração de furtos. Nesse sentido urge a necessidade da elaboração de uma avaliação da situação, através da elaboração da construção de um perfil de risco individualizado, abrangendo toda a cadeia de segurança monetária, desde o transporte, ao abastecimento e armazenamento de numerário nos terminais.

A construção de um perfil de risco individualizado para cada ATM deve considerar um conjunto de variáveis críticas, entre as quais se destacam (Quadro n.º 3):

⁶¹ Vide Anexo A

Quadro n.º 3 - Perfil de risco individualizado para ATM

Perfil de risco individualizado para ATM
Características da localização da ATM e do seu enquadramento territorial (zona urbana ou rural, densidade populacional, proximidade de postos ou esquadras das FS, presença de videovigilância, sistemas de reconhecimento automático de matrículas, entre outros);
Posição física da ATM • distinguindo-se entre ATMs situados dentro ou fora de edifícios, • localizados em bancos ou instalações remotas (como juntas de freguesia e estabelecimentos comerciais), • bem como a sua configuração estrutural (embutido, ancorado ou autónomo);
O tipo de ATM;
Respetivas funcionalidades de segurança;
Volume de numerário armazenado;
Histórico de incidentes e tipos de ataques registados , o que permite antecipar padrões de atuação e ajustar as respostas preventivas;
Medidas de segurança já implementadas , como sistemas inteligentes de neutralização de notas (IBNS), videovigilância, sensores de intrusão e sistemas de neblina, entre outros dispositivos dissuasores e de proteção.

Fonte: REPC & Europol (2019)

Após a avaliação da situação e a identificação das áreas de maior risco, bem como dos pontos fortes e fracos da segurança das ATM, deve ser delineada uma estratégia de intervenção, frequentemente assente na colaboração entre entidades públicas e privadas. Esta estratégia deverá incluir a implementação de contramedidas de natureza preventiva e operacional. As medidas preventivas devem visar a redução da intenção e da capacidade dos perpetradores para cometer o furto. Para tal, propõem-se três tipos de ações preventivas, fundamentadas nos princípios da prevenção situacional: a) redução da recompensa associada ao crime, b) aumento do risco para os perpetradores e c) aumento do esforço necessário para a concretização do furto.

A prevenção dos furtos a ATM estrutura-se dessa forma em três eixos essenciais (Quadro n.º 4):

Quadro n.º 4 - Prevenção contra furtos a ATM

Redução das recompensas	Visa diminuir o incentivo económico dos furtos, através de medidas como a limitação do numerário nas ATM, o esvaziamento noturno das ATMs mais vulneráveis e a utilização de sistemas inteligentes de neutralização de notas (IBNS), que inutilizam fisicamente o dinheiro furtado.
Aumento do risco	Foca-se na dissuasão, promovendo a instalação de sistemas de videovigilância discretos ou ocultos, a partilha eficaz de informações entre entidades públicas e privadas, a criação de bases de dados forenses e o reforço da cooperação transnacional.
Aumento do esforço	Implica tornar o ato criminoso mais difícil de executar, através da colocação das ATM em locais de elevada segurança, da utilização de estruturas reforçadas, de sistemas de alarme e de tecnologias de dissuasão como o sistema de neblina.

Fonte: REPC & Europol (2019)

Para além destas medidas diretamente aplicadas às ATM, a eficácia de uma estratégia preventiva depende igualmente da implementação de um conjunto de medidas paralelas⁶². Estas medidas desempenham um papel essencial na consolidação de uma abordagem preventiva integrada, permitindo ampliar o alcance das políticas de segurança, envolver a sociedade civil e criar um ecossistema institucional resiliente à ocorrência de furtos a ATM.

Entre estas medidas, destacam-se (Quadro n.º 5):

Quadro n.º 5 - Medidas paralelas na prevenção de furtos a ATM

Medidas paralelas na prevenção de furtos a ATM
Desenvolvimento de estratégias de comunicação pública , com campanhas informativas e dissuasoras que desincentivem a prática criminosa, aumentem a perceção do risco entre os potenciais ofensores e promovam uma cultura de segurança entre os cidadãos
Reforço da colaboração interinstitucional , envolvendo forças de segurança, autoridades locais, operadores bancários e empresas de transporte de valores, criando canais formais de partilha de informação e mecanismos operacionais conjuntos
Adoção de um enquadramento legislativo eficaz , que preveja normas obrigatórias de segurança para os operadores de ATMs, penas proporcionais e dissuasoras para os crimes cometidos e instrumentos legais para a aplicação de medidas preventivas;

Fonte: REPC & Europol (2019)

2.7 Prevenção de furtos de ATM em Portugal

Em 2011, sob coordenação do Secretário-geral do Sistema de Segurança Interna, foram estabelecidas três Equipas Mistas de Prevenção Criminal, incluindo uma dedicada à prevenção de furtos e roubos a ATM, composta por elementos das várias Forças e Serviços de Segurança, tais como a GNR, a Polícia de Segurança Pública (PSP), a Polícia Judiciária (PJ), o Serviço de Estrangeiros e Fronteiras (agora extinto⁶³) e o Serviço de Informações de Segurança, tendo sido implementadas diversas estratégias e ações de prevenção e combate a este fenómeno (SSI, 2012).

A trajetória de crescimento, identificada em 2016 e 2017, inclusive praticados, em regra, com recurso a armas de grande calibre e explosivos ou meios equiparados (Ministério Público, 2017) levou à adoção de medidas preventivas e repressivas, incluindo a definição de estratégias de curto, médio e longo prazo, o reforço do intercâmbio de informações e a criação de uma equipe conjunta de análise composta por magistrados do Ministério Público, representantes do Departamento Central Investigação e Ação Penal e das Procuradorias-gerais Distritais, e por elementos da GNR, PJ e da PSP. A implementação dessas ações resultou na redução significativa das ocorrências, coincidindo com a detenção de vários membros de grupos criminosos associados (SSI, 2018).

⁶² Vide Anexo A

⁶³ Cfr. Decreto-Lei n.º 41/2023 de 2 de junho

2.8 Implementação das ATM em Portugal

O Regime Jurídico da Segurança Privada⁶⁴, promoveu um aumento do número e da exigência⁶⁵ das medidas de segurança aplicáveis às entidades que operam neste setor. No seio destas alterações, o legislador concedeu particular atenção às ATMs em função da especial vulnerabilidade de que as mesmas se revestem, assim como do alarme social que causa os incidentes a eles associado.

A situação recorrente de ataque a este tipo de equipamentos, cujo efeito provoca danos avultados, não só nas ATM que foram alvo de furto ou da tentativa, bem como nas infraestruturas onde o mesmo se insere, e até mesmos nas imediações, provocando ainda o aumento do sentimento de insegurança nas populações, levou a um aumento dos requisitos técnicos, medidas de segurança e os procedimentos de avaliação da instalação visando reduzir significativamente a apetência para este tipo de crimes.

A instalação de equipamentos ATM⁶⁶ ficou sujeita a uma avaliação prévia das condições de segurança do local de instalação e ao cumprimento dos requisitos técnicos e medidas de segurança. As medidas e os requisitos mínimos de segurança de equipamentos ATM, são aplicados de acordo com a avaliação de segurança do local onde estiverem instaladas, do tipo de equipamento e dos riscos associados às operações de manutenção.

Os requisitos técnicos impostos⁶⁷ a estes equipamentos encontram-se elencadas no Quadro n.º 6.

⁶⁴ *Cfr.* Art.º 10 do Regime Jurídico da Segurança Privada, aprovado pela Lei n.º 34/2013, de 16 de maio, posteriormente alterado pela Lei n.º 46/2019, de 8 de julho.

⁶⁵ Com o objetivo de aumentar os níveis de segurança e da eficácia da prevenção criminal, introduzindo assim medidas de segurança específicas, por considerar que este setor está exposto a riscos especiais.

⁶⁶ As medidas são aplicáveis a todos os equipamentos, com instalação de caráter permanente, em território nacional, desde que localizadas fora das áreas de atendimento ao público das sociedades financeiras e instituições de crédito e que se mantenham acessíveis fora do respetivo horário de funcionamento. As medidas de segurança e requisitos técnicos das ATM cuja instalação tenha caráter temporário serão determinadas em resultado de avaliação de risco extraordinária e autónoma.

⁶⁷ Os quais são aprovados por despacho do membro do governo responsável pela área da administração interna, encontram-se elencados na Portaria n.º 273/2013, de 20 de agosto, alterada pela Portaria n.º 106/2015, de 13 de abril e mais recentemente pela Portaria n.º 292/2020, de 18 de dezembro.

Quadro n.º 6 - Requisitos técnicos mínimos de ATM

Na definição dos requisitos mínimos da ATM devem ser considerados, nomeadamente, os seguintes fatores (n.º 2 do art.º 103 da Portaria n.º 273/2013, de 20 de agosto, alterada pela Portaria n.º 292/2020, de 18 de dezembro): • A segurança dos utentes e do público em geral; • As ameaças relativas à ATM, às operações de manutenção e ao local físico de instalação; • As condições do local de instalação • A existência de outras medidas de segurança no local de instalação; • As medidas de segurança nas operações de transporte de valores; • Os montantes disponíveis na ATM.
Os requisitos mínimos de segurança da ATM devem contemplar (n.º 3 do art.º 103 da Portaria n.º 273/2013, de 20 de agosto, alterada pela Portaria n.º 292/2020, de 18 de dezembro): • O nível de proteção do cofre e fechaduras por referência às normas técnicas EN 1143-1 e UL 291 ATM; • Monitorização permanente dos sistemas de alarme; • Equipamento de alarme de instalação obrigatória ou recomendada; • Proteção por sistema de videovigilância por câmaras de vídeo; • Iluminação mínima da ATM; • Proteção dos utentes; • Sistemas de ancoragem da ATM ao solo; • Proteção das notas por IBSN; • Proteção contra ataques físicos (ram raid: ato de conduzir um carro, geralmente roubado, contra a janela frontal de um edifício/estabelecimento, para que o conteúdo deste possa ser roubado); • Georreferenciação da ATM; • Sinalética de segurança.

Fonte: Portaria n.º 273/2013, de 20 de agosto, alterada pela Portaria n.º 106/2015, de 13 de abril e pela Portaria n.º 292/2020, de 18 de dezembro

Com a publicação da Portaria n.º 273/2013, de 20 de agosto, por força do Art.º 10 da Lei n.º 34/2013 de 16 de maio, foi atribuída às FS a missão de assegurar e manter o levantamento das situações de risco relativas a operações de manutenção⁶⁸ das ATM e relativamente à avaliação de risco dos locais onde os mesmos se encontram instalados.

A mesma norma legal veio ainda exigir que a instalação de novas ATM ficasse sujeita a registo, condicionado ao cumprimento de requisitos técnicos mínimos que foram aprovados por Despacho da Secretária de Estado Adjunta e da Administração Interna de 24 de maio de 2017, na FS territorialmente competente e submetido a parecer da mesma.

A Ficha de Avaliação de risco avalia o risco da instalação de determinada ATM com base na caracterização do local de instalação, caracterização das condições de instalação, caracterização das condições para operações de manutenção, avaliação das condições para realização de atos ilícitos, tipologia da ATM; juízo ampliativo – probabilidade de ocorrência de ilícito na ATM. O culminar desta avaliação termina com a atribuição de um nível de risco.

⁶⁸ Realizadas pelas empresas de segurança privada titulares de alvará D.

PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO

CAPÍTULO III – METODOLOGIA, MÉTODOS E MATERIAIS

Uma investigação desenvolve-se através de um percurso progressivo que conduz o investigador de um estado inicial de desconhecimento à construção estruturada do conhecimento científico. Este processo implica conforme sustenta Bertaux (1997) três fases que traduzem diferentes níveis de maturação da investigação: a exploração, a análise e a síntese. Estas etapas serão aprofundadas ao longo do presente capítulo, na medida em que constituem a espinha dorsal deste trabalho de investigação.

3.1. Objetivos da investigação

Esta investigação tem como Objetivo Geral (O_G): “Analisar como pode a GNR direcionar a prevenção de crimes de furto a ATM”.

A fim de alcançar este objetivo geral, foram definido os seguintes objetivos específicos (O_E):

- O_{E1}: “Analisar o *Modus Operandi* de furtos a ATM, em Portugal, na área de jurisdição da GNR”.
- O_{E2}: “Compreender quais os padrões de interesse para a GNR para prevenir os furtos a ATM em Portugal”.

Definida a temática sobre a qual versa a investigação, impera a necessidade de desenvolver a Questão de partida (Q_P), que traduza o “(...) fenómeno ou assunto (...) que se pretende alcançar com a realização da pesquisa (...)” (Rodrigues, 2007, p. 26). A Q_P servirá essencialmente de guia ao longo das várias fases da investigação (Haro et al., 2016). Subordinado ao tema proposto a Q_P é:

- Q_P: “Como pode a GNR direcionar a prevenção a crimes de furto a ATM?”

Da Q_P emergem as questões derivadas (Q_D) alinhadas com os O_E da investigação, tratando-se de questões de cariz mais restrito, dispostas em setores de análise que estão circunscritos no domínio da Q_P (Rosado, 2017).

- Q_{D1}: “Quais os *Modi Operandi* que tem vindo a ser adotadas em Portugal Continental, na área de jurisdição da GNR?”
- Q_{D2}: “Quais os padrões de interesse para a GNR para prevenir os furtos a ATM em Portugal?”

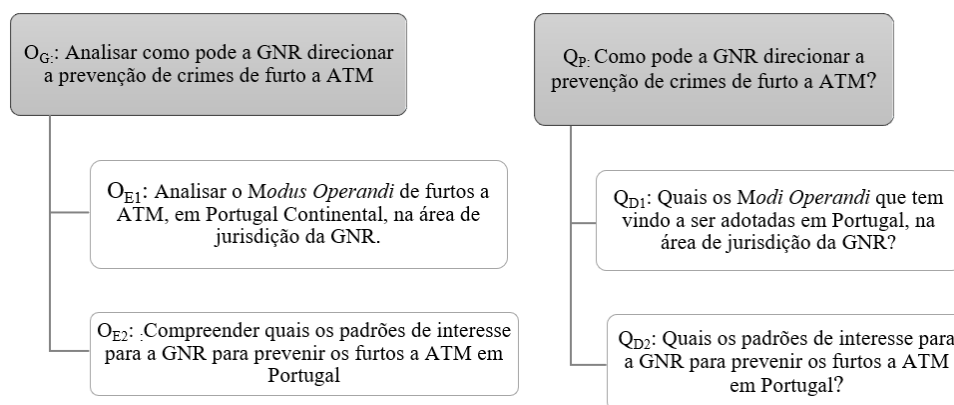


Figura n.º 6 - Relação entre os OE e as PD

3.2. Definição do desenho e da estratégia de investigação

Esta investigação seguiu uma abordagem mista, combinando elementos das abordagens qualitativa e quantitativa “(...) com o objetivo de alcançar uma compreensão mais ampla e aprofundada, e de reforçar a corroboração dos resultados (...)” (Johnson et al., 2007, p. 123). Os elementos da abordagem quantitativa prendem-se com o objetivo de observar e analisar o fenómeno em estudo de forma objetiva, através da recolha e tratamento de dados estatísticos. Essa análise é complementada através de elementos da abordagem qualitativa, por meio de entrevistas, permitindo aprofundar a compreensão dos resultados obtidos, identificar perceções e reforçar a interpretação dos dados quantitativos (Creswell, 2018).

Relativamente ao raciocínio que se afigurou mais adequado para esta investigação foi o raciocínio indutivo, que por sua vez remete-nos para o método indutivo “(...) que se baseia em análises de dados e de resultados sobre um fenómeno particular com o intuito de alcançar a generalização teórica (...)” (Rosado, 2017, p.118).

3.3. Técnicas e procedimentos de recolha de dados

A recolha de dados contemplou técnicas de recolha de dados documentais e não documentais (Santos et al., 2019). Na fase inicial da investigação, designada de revisão da literatura, com o propósito de desenvolver um quadro teórico-concetual, foram reunidos trabalhos científicos mais relevantes e atualizados sobre o tema em estudo (Haro et al., 2016). Nesta fase foram privilegiadas as designadas fontes primárias⁶⁹. A consulta decorreu essencialmente através de bases de dados e repositórios digitais⁷⁰. Face a temática e ao

⁶⁹ “(...) constituídas por textos originais, do próprio autor, sem qualquer interpretação de terceiros (...)” (Haro et al., 2016, p.49).

⁷⁰ “Scopus”, “Web of science”, “J-STOR”, “SciELO” e “EBSCO”, e ainda a consulta do “RCAAP”.

contexto do estudo além de artigos científicos considerou-se ainda relevante consultar legislação, maioritariamente nacional, estatísticas oficiais nacionais e europeias, bem como documentos internos da GNR e documentos de instituições e agências europeias na qual se destaca a Europol e a EAST.

Concluída a revisão da literatura, seguiu-se o designado trabalho de campo, e dado o modelo de investigação adotado, esta fase contemplou a análise de todas as ocorrências registadas na área da GNR relativas a furtos a ATM, complementada pela realização de entrevistas.

Na análise de todas as ocorrências registadas na área da GNR relativas a furtos a ATM, foram analisados os Autos de Notícia (AN) que foram elaborados pela GNR⁷¹, relativos a furtos a ATM, de 2016 a 2024, complementada por dados fornecidos pela Direção de Informações (DI) e pela Direção de Investigação Criminal (DIC) da GNR. Essa consulta foi realizada através do Sistema Integrado de Informações Operacionais Policiais (SIIOP) da GNR, que “(...) consiste num sistema baseado num repositório único, de informações, centralizado e alargado ao dispositivo que permite à Guarda o suporte à decisão/ação, baseado em informação alargada e em tempo real (...)” (NEP/GNR 2.20, p. 1).

De forma a complementar e consolidar os indicadores observados nos dados obtidos nas ocorrências registadas, e tendo em conta os objetivos desta investigação, foram ainda efetuadas nove entrevistas⁷². Entrevistas essas, semidiretivas, que se caracterizam como uma “(...) conversa mais ou menos orientada por guião previamente preparado (...)” (Cunha et al., 2012, p. 152), que permitiu efetuar uma recolha de dados mais aprofundada sobre a temática.

O planeamento das entrevistas dividiu-se em várias fases, numa primeira fase, ainda antes da realização das entrevistas foi necessário definir os objetivos das mesmas, de forma a poder escolher os entrevistados adequados e construir um guião face a esses objetivos (Vilelas, 2020). Apesar de se tratar de uma investigação centrada na prevenção criminal, era de todo relevante entrevistar elementos que estiverem ou estão, no exercício das suas funções, ligados à investigação ou na análise deste fenómeno. A escolha dos entrevistados não obedeceu a qualquer critério de amostragem, mas sim antes, a uma decisão que competiu

⁷¹ O estudo não incidiu nas Regiões Autónomas dos Açores e da Madeira, que contrariamente aos demais Comandos Territoriais da GNR, que correspondem aos dezoito distritos que compõem Portugal Continental, as atribuições cometidas à Guarda são essencialmente no âmbito da vigilância da costa e do mar territorial e da prevenção e investigação de infrações tributárias e aduaneiras, sem prejuízo de outras missões que lhes sejam especialmente cometidas (n.º 2 do art.º 37 da LOGNR).

⁷² *Vide* Apêndice C

ao investigador e que recaiu em características relativas ao perfil procurado. Essa escolha considerou o cargo ou função que desempenhou ou que desempenha, ao nível da especialização e o potencial colaborativo do entrevistado para os objetivos da investigação. Dessa forma, seguiu-se o método de amostragem não probabilística, sendo amostragem por especialistas (Haro et al., 2016).

Nesse sentido foram entrevistados⁷³ os Chefes da Secções de Informações e Investigação Criminal dos Comandos Territoriais de Lisboa, Porto e Setúbal, que correspondem aos distritos com maior incidência deste fenómeno em Portugal, segundo o RASI, característica que se verifica também na área da GNR no período analisado e da Secção de Investigação Criminal do Grupo de Intervenção de Operações Especiais da GNR. Pelo impacto nacional e dispersão territorial deste fenómeno foram também realizadas entrevistas a elementos da Direção de Investigação Criminal⁷⁴ da GNR e da Direção de Informações⁷⁵ da GNR. Apesar de se tratar de uma análise restrita a área de jurisdição da GNR considerou-se relevante o contributo das demais Forças e Serviços de Segurança com competência na matéria em Portugal, nomeadamente à PJ, através da Unidade Nacional Contraterrorismo e um elemento designado pela PSP.

3.4. Tratamento de dados

O tratamento dos dados quantitativos foi realizado com recurso ao *software IBM SPSS Statistics*, o qual possibilitou a análise de um conjunto de dados extraídos maioritariamente dos AN. Foram estabelecidos vários critérios⁷⁶ e parâmetros que possibilitaram a análise através de estatística descritiva dos dados.

A análise das entrevistas foi realizada com recurso ao *software MAXQDA*, o qual permitiu otimizar o tratamento dos dados qualitativos, centralizando e organizando a informação recolhida, através da codificação de dados, que possibilitou a transcrição das gravações das entrevistas e a marcação de segmentos de texto com códigos⁷⁷ temáticos, facilitando a categorização e posterior análise. Este processo viabilizou a elaboração de quadros de análise categorial, os quais organizam e sintetizam os principais temas identificados nas entrevistas, favorecendo a comparação e a identificação de padrões de resposta.

⁷³ Vide Apêndice C

⁷⁴ Chefe da Repartição de Análise de Informação Criminal e Chefe da Secção de Análise de Informação Criminal

⁷⁵ Chefe de Divisão

⁷⁶ Vide Apêndice A

⁷⁷ Vide Apêndice A

A categorização dos dados provenientes das entrevistas, recorreu-se à análise de conteúdo de natureza qualitativa, orientada por uma abordagem indutiva. Esta opção metodológica revela-se particularmente adequada ao propósito de explorar em profundidade as percepções e experiências dos participantes, evitando a imposição de categorias à priori. As categorias analíticas emergiram progressivamente através de um processo sistemático de codificação e interpretação, sustentado numa leitura atenta e numa comparação constante entre os dados recolhidos (Patton, 2002; Berg, 2001). A escolha das categorias prendeu-se com os objetivos de cada questão, que foram orientadas pela revisão de literatura, especialmente REPC & Europol, 2019: as duas primeiras relacionadas com indicadores de alerta, a terceira com as características do local, a quarta com as características da ATM e a quinta e última questão direcionada para a prevenção. As subcategorias, e uma vez que a abordagem seguida foi a indutiva, prenderam-se com a respostas às questões por parte dos entrevistados.

CAPÍTULO IV – APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

No presente capítulo apresentamos, analisamos e discutimos os dados que foram obtidos através da análise de todas as ocorrências que envolveram furtos a ATM, consumados ou na forma tentada, na área de jurisdição da GNR entre 2016 e 2024 assim como análise e discussão das entrevistas realizadas.

4.1. Apresentação e análise dos resultados quantitativos

Nesta fase, apresentam-se e analisam-se os resultados quantitativos obtidos, procurando identificar tendências e padrões relevantes para a investigação, os quais serão posteriormente confrontados com os resultados dos dados qualitativos e dos pressupostos teóricos, aprofundando a compreensão do fenómeno em estudo na discussão dos resultados.

4.1.1 Distribuição por Distrito e por Concelho

Entre os 18 distritos de Portugal, e ao longo dos oito anos analisados, segundo a Tabela n.º 4, os distritos do Porto e de Lisboa destacaram-se com o maior número de furtos, na forma tentada ou consumada, totalizando 43 e 42 ocorrências, respetivamente. Seguem-se os distritos de Aveiro e Setúbal, cada um, 30 ocorrências, e Leiria com 28. Já os distritos de Coimbra e Braga registaram, respetivamente, 18 e 17 ocorrências.

Importa salientar que, em todos estes distritos, cerca de metade das ocorrências tiveram lugar durante os anos de 2016 e 2017. Este biénio revelou-se particularmente expressivo no que respeita à incidência de furtos, destacando-se pelo número significativamente superior de casos em comparação com os anos subsequentes.

Tabela n.º 4 - Furtos ATM por Distrito de Portugal de 2016 a 2024

DISTRITO	2016	2017	2018	2019	2020	2021	2022	2023	2024	TOTAL
AVEIRO	1	11	-	2	1	4	3	7	1	30
BEJA	-	1	-	-	1	-	-	-	-	2
BRAGA	3	6	-	1	2	4	1	-	-	17
BRAGANÇA	-	-	-	-	-	-	-	1	-	1
CASTELO BRANCO	1	1	-	-	1	-	1	-	1	5
COIMBRA	4	7	-	-	1	-	3	-	3	18
ÉVORA	1	-	1	-	-	-	-	4	-	6
FARO	1	4	3	1	1	1	-	-	1	12
GUARDA	-	-	-	-	-	2	-	-	-	2
LEIRIA	13	13	-	-	-	-	1	-	1	28
LISBOA	8	24	2	1	3	1	-	1	2	42
PORTALEGRE	-	-	1	1	-	2	1	2	-	7
PORTO	11	13	4	3	4	1	3	3	1	43
SANTARÉM	-	6	-	-	-	2	2	2	-	12
SETÚBAL	8	1	-	6	2	-	1	1	2	30
VIANA DO CASTELO	-	-	-	-	1	-	-	-	2	3
VILA REAL	-	-	-	-	-	-	-	-	-	0
VISEU	1	0	-	-	-	-	4	-	2	7
TOTAL	52	96	11	15	17	17	20	21	16	265

O distrito do Porto, além de se destacar pelo maior número de ocorrências registadas, apresentou furtos em todos os anos do período analisado, evidenciando uma persistência significativa deste tipo de atividade criminosa. De modo análogo, o distrito de Lisboa registou ocorrências ao longo de quase todo o intervalo temporal analisado. Não obstante da ligeira redução do número de furtos face ao pico observado em 2017, manteve-se a continuidade desta prática delituosa em Lisboa.

No que concerne ao distrito de Aveiro, embora o volume de ocorrências seja inferior ao verificado nos distritos do Porto e de Lisboa, a regularidade dos furtos manteve-se ao longo do período considerado, destacando-se o ano de 2023, com sete registos. O distrito de Setúbal revela um padrão semelhante, caracterizado pela manutenção consistente deste tipo de criminalidade. Relativamente ao distrito de Leiria, ainda que ocupe a quinta posição em número de furtos, observa-se que 23 das 28 ocorrências se concentraram nos anos de 2016 e 2017.

Estes dados, tal como se verifica na Figura n.º 7, indicam uma concentração significativa deste fenómeno nos distritos do litoral, evidenciando que esta região é mais afetada por este tipo de ataques do que os distritos do interior.

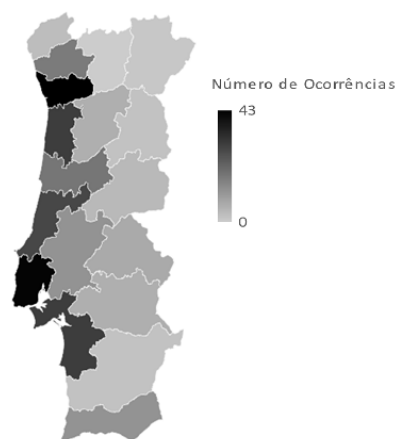


Figura n.º 7 - Mapa coroplético de furtos a ATM na área da GNR de 2016 a 2024

A um nível mais micro, alguns concelhos⁷⁸ destacam-se pelo número de furtos a ATM. O concelho de Sintra, no distrito de Lisboa, registou o maior número de ocorrências, com um total de 15 furtos. Seguiu-se Vila do Conde, no distrito do Porto, com 11 registos. Os concelhos de Almada e Palmela, ambos pertencentes ao distrito de Setúbal, contabilizaram sete e seis furtos, respetivamente. Já Paredes (Porto) e Barcelos (Braga) registaram também seis ocorrências cada.

4.1.2 Distribuição mensal e semanal

A distribuição mensal, apresentada na Figura n.º 8, varia entre um mínimo de 11 ocorrências em janeiro e um máximo de 37 em outubro. A média mensal de 22 ocorrências, coincide com a mediana, sugerindo uma distribuição relativamente simétrica. O desvio padrão, de aproximadamente 6,49 indica alguma variabilidade entre os meses, embora não muito acentuada. Importa referir que, nos últimos quatro meses do ano, a média mensal sobe ligeiramente para 28 ocorrências. No entanto, essa diferença não é suficientemente significativa para alterar a tendência geral, permitindo assim, concluir que o número de furtos apresenta um comportamento relativamente estável ao longo do ano.

⁷⁸ Vide Apêndice F

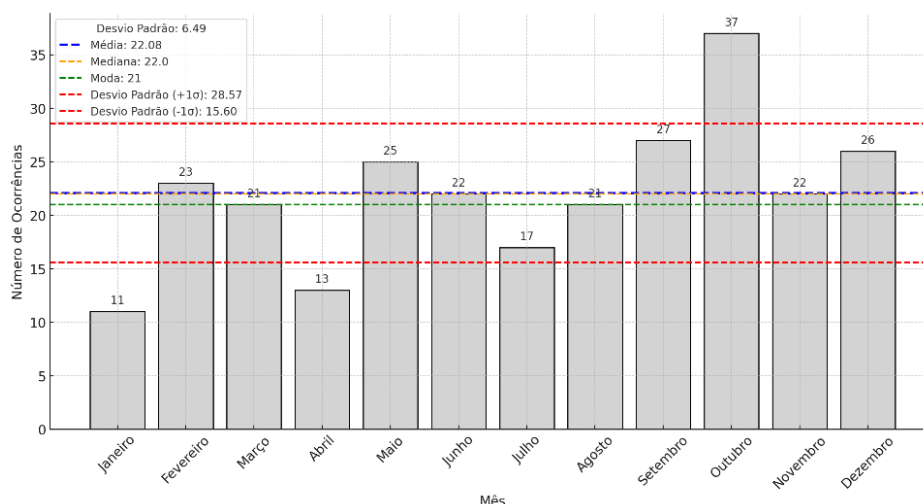


Figura n.º 8 - Número de furtos (tentativas e consumados) por mês de 2016 a 2024

A análise da distribuição semanal, apresentada na Figura n.º 9, releva uma tendência clara de aumento de furtos ao longo dos dias úteis, atingindo o pico à sexta-feira, com 54 furtos, o que representa 20,9% do total. No fim de semana, há uma quebra acentuada, sendo sábado e domingo os dias com menos registos. No total, 81,4% dos furtos (consumados ou tentados) em ATMs ocorreram em dias úteis, contra apenas 18,6% ao fim de semana.

O desvio padrão de 11,14 indica uma variabilidade considerável em torno da média de 36,86 furtos por dia da semana, refletindo alguma variação entre os dias, mas sem extremos muito acentuados. Apesar dos valores mais elevados à sexta-feira, os restantes dias úteis apresentam números relativamente próximos, apontando para uma distribuição estável de segunda a quinta. No entanto, a análise da dispersão confirma que há um crescimento gradual nas ocorrências ao longo da semana, seguido de uma queda acentuada no sábado e domingo.

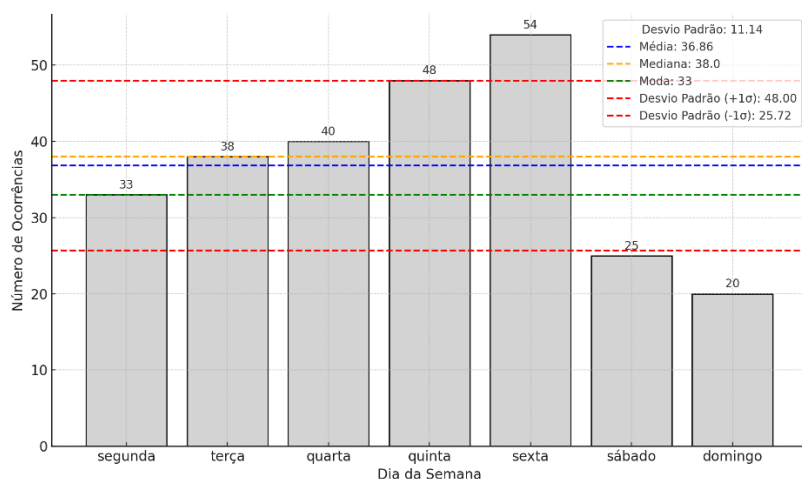


Figura n.º 9 - Número de furtos (tentativas e consumados) por dia da semana de 2016 a 2024

4.1.3 Análise da distribuição horária

A análise da distribuição horária, com base nas 233 ocorrências que apresentam indicação precisa da hora do furto, representando aproximadamente 87,9% do total de furtos, revela um padrão de incidência fortemente concentrado no período noturno, principalmente durante a madrugada, sobretudo entre as 03h00 e as 05h00, que somam 99 ocorrências. Dentro deste intervalo, o pico de furtos ocorreu às 04h00, com um total de 52 ocorrências, o que corresponde a aproximadamente 20% do universo das situações com hora definida. A partir das 06h00, observa-se um decréscimo acentuado da frequência dos furtos, sendo os registos em plena luz do dia manifestamente residuais, como é possível verificar pela Figura n.º 10.

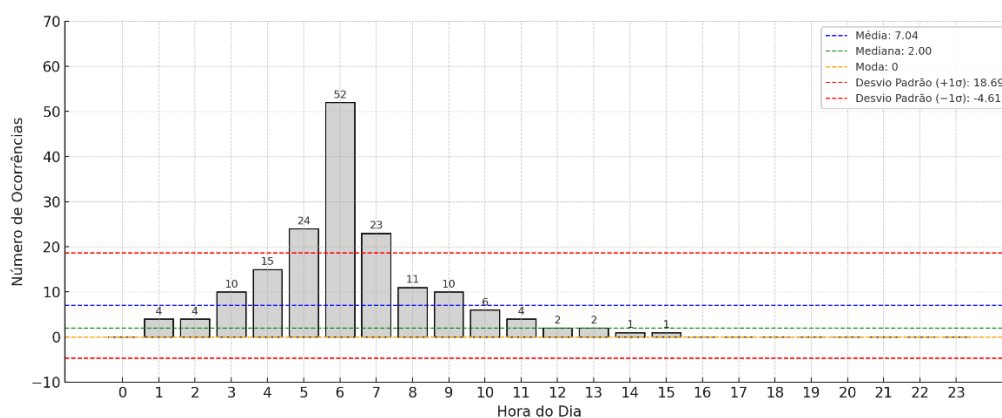


Figura n.º 10 - Número de furtos (tentativas e consumados) por hora de 2016 a 2024

Cumprido, contudo, considerar que uma proporção dos registos, cerca de 12,1%, correspondendo a 32 ocorrências, não apresenta uma hora de ocorrência rigorosamente determinada. Ainda assim, entre os 20 casos, tal como se verifica na Figura n.º 11, em que

se pode identificar uma janela temporal aproximada, constata-se que os intervalos mais frequentemente referidos continuam a situar-se no período da madrugada. Com base na tabela apresentada, é possível observar que o período com maior concentração de incidentes corresponde à janela entre 00H00 e 08H00, totalizando 13 ocorrências.

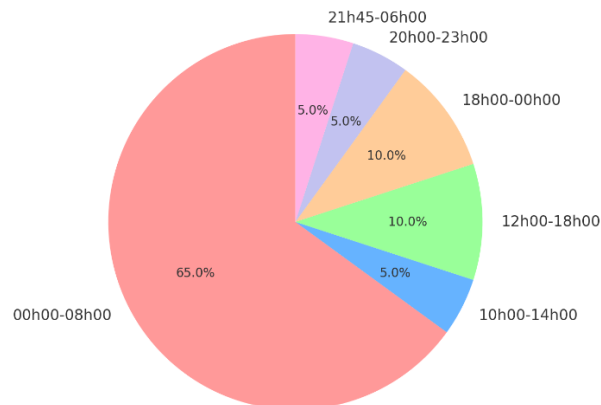


Figura n.º 11 - Janela temporal dos furtos sem hora definida de 2016 a 2024

4.1.4 *Modus Operandi*

Dos 265 furtos a ATM registados, é possível observar uma clara evidência no predomínio dos ataques físicos, como mostra a Figura n.º 12, com um total de 249 casos, correspondendo a 94% do total registado. Em contraste, os ataques lógicos contabilizam apenas 16 furtos, representando 6% do universo analisado.

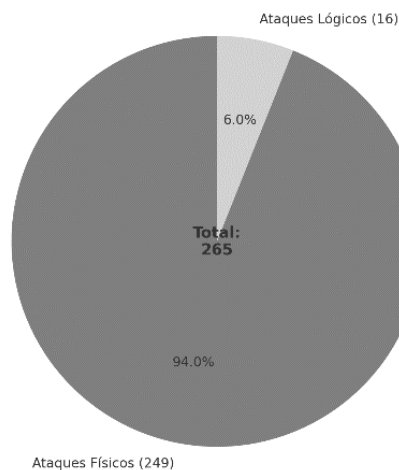


Figura n.º 12 - Comparação entre ataques físicos e lógicos de 2016 a 2024

4.1.4.1. *Modus Operandi* Ataques Físicos

Dos 249 ataques físicos, dentro das categorias dos ataques físicos estabelecidas pela EGAP, representadas na Figura n.º 13, praticamente 94% dos ataques físicos correspondem a ataques explosivos (48,8%) e a Furtos da ATM – no local (45,1%). Já os Furtos do ATM –

arrancamento (1,2%) e os ataques não especificados (4,9%) representam apenas sensivelmente 6%.

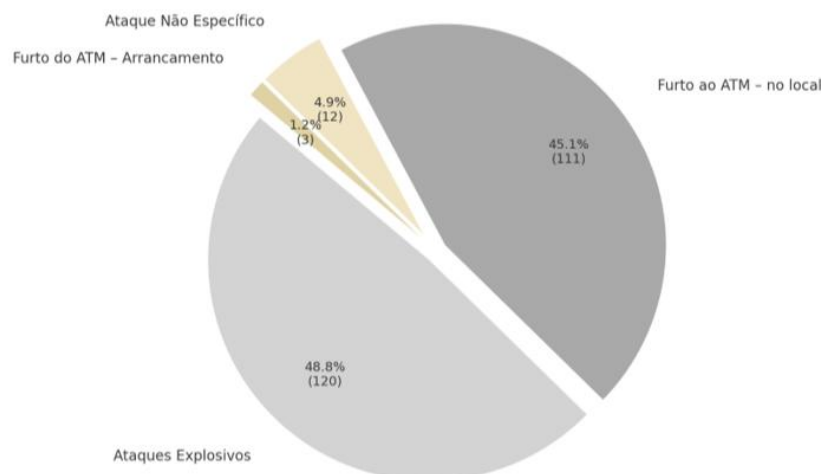


Figura n.º 13 - Modus Operandi Ataques Físicos de 2016 a 2024

Os ataques explosivos, com 120 registos, representam praticamente metade da totalidade dos ataques físicos registados (48,8%). A maioria desses ataques, cerca de 74% (96), foram realizados com recurso a explosivos gasosos (X1). Os explosivos sólidos (X2) são consideravelmente menos frequentes, apenas foram registados 9 casos (7,4%), incluindo três casos com recurso a uma granada. No entanto, em 18,9% dos ataques, não foi possível determinar o tipo de explosivo usado (Figura n.º 14).

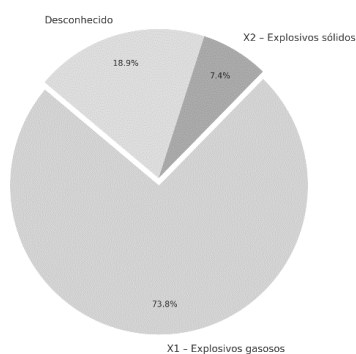


Figura n.º 14 – Comparação ataques explosivos de 2016 a 2024

Os Furtos da ATM – no local, com 111 registos, representando 45,1% dos ataques físicos, foram subdivididos em: através de perfuração (B2) com apenas uma ocorrência com recurso a um berbequim (0,4%), corte (B3) com 28 ocorrências (11,4%) com recurso a instrumentos de corte como rebarbadoras e alicates de corte, e arrombamento (B4), sendo este último o segundo MO mais frequente com 82 registos (32,5%), sendo realizados com recurso a pés de cabra, chaves de fendas, martelos e marretas.

Registaram-se ainda três casos de furto por extração física da ATM (Rip Out), correspondendo a 1,2%, e 12 ataques não especificados, equivalentes a 4,9%, que refletem limitações na identificação técnica do método utilizado.

Tabela n.º 5 – Ataques físicos a ATM por ano de 2016 a 2024

Ano	B2 – Perfuração	B3 – Corte	B4 – Arrombamento	X1 – Explosivos gasosos	X2 – Explosivos Sólidos	Desconhecido	Ataques não específicos	Furto do ATM – arrancamento	
2016	-	7	12	16	7	10	-	-	52
2017	-	3	17	69	-	7	-	-	96
2018	1	2	4	4	-	-	-	-	11
2019	-	5	8	1	1	-	-	-	15
2020	-	5	5	1	-	-	-	2	13
2021	-	3	6	-	-	-	8	-	17
2022	-	-	8	-	-	-	2	-	10
2023	-	1	15	1	1	1	-	-	19
2024	-	2	7	4	-	-	2	1	16
Total	1	28	82	96	9	18	12	3	249

Os furtos a ATM com explosivos gasosos (X1) totalizaram 96 ocorrências, com um pico em 2017, ano em que se registaram 69 casos, o que representa mais de dois terços do total desta tipologia. No entanto, após uma queda acentuada nos anos seguintes, este método de ataque voltou a surgir recentemente, com uma ocorrência em 2023 e quatro em 2024, indicando um ligeiro ressurgimento.

O recurso ao arrombamento (B4) apresenta uma representatividade constante ao longo do período analisado, com destaque para os anos de 2020 (14 ocorrências), 2022 (13 ocorrências) e 2023 (15 ocorrências). Os dados indicam que esta subcategoria tem mantido uma frequência elevada e recorrente.

A análise da percentagem de sucesso dos diferentes MO, nos ataques físicos, como se pode verificar na Tabela n.º 6, evidencia diferenças relevantes entre os diversos métodos utilizados. Destaca-se, em particular, a elevada eficácia dos ataques com explosivos gasosos (X1), que registaram uma taxa de sucesso de 67,7%. Valor significativamente superior ao das restantes tipologias. Já os explosivos sólidos (X2) demonstraram uma eficácia moderada, com 44,4% de sucesso.

Os ataques por corte (B3) apresentaram uma taxa de sucesso de 57,1%, também relativamente elevada, com 16 ataques consumados em 28. Em contrapartida, o arrombamento (B4), apesar de ser amplamente utilizado (80), revelou uma baixa taxa de sucesso, de apenas 17,5%. Os ataques por arrancamento da ATM não resultaram em qualquer consumação.

Tabela n.º 6 - Taxa de consumação furtos a ATM de 2016 a 2024

Tipos de Ataque	Subtipo	Nº de ataques	Consumado	Tentativa	Desconhecido	Percentagem de sucesso
Ataques explosivos	X1 – Explosivos gasosos	96	65	22	9	67,7%
	X2 – Explosivos Sólidos	9	4	4	1	44,4%
	Desconhecido	18	9	11	3	50%
Furto da ATM – arrancamento	-	3	-	-	3	0%
Furtos da ATM – no local	B2 – Perfuração	1	-	-	1	0%
	B3 – Corte	28	16	12	-	57,1%
	B4 – Arrombamento	82	14	62	6	17,5%
Ataques não específicos	-	12	0	12		0%
Total		249	108	123	23	

4.1.4.2 Modus Operandi Ataques Lógicos

Dentro dos ataques lógicos apenas foram registados 16 casos, maioritariamente através dos ataques designados de *Black Box*. O primeiro registo de ataque *Black Box* surgiu em 2020 com três registos, em 2021 não há registo de qualquer ataque, reaparecendo em 2022 com 10 registos, o valor mais elevado em todo o período analisado. No entanto, após este pico, verificou-se uma redução significativa em 2023 com apenas duas ocorrências e em 2024 não foi registada qualquer ocorrência (Tabela n.º 7). O ano de 2020 ficou também marcado pelo único ataque designado de *Jackpotting*.

Tabela n.º 7 - Ataques lógicos a ATM por ano de 2016 a 2024

Ano	Jackpotting	Black Box
2016	-	-
2017	-	-
2018	-	-
2019	-	-
2020	1	3
2021	-	-
2022	-	10
2023	-	2
2024	-	-
Total	1	15

4.1.5 Local da ATM

Relativamente à análise dos locais onde as ATM estão instaladas, verificou-se que os bancos surgem como o principal foco de incidência, totalizando 85 ocorrências, o que corresponde a 32,1% do total registado. Seguem-se as juntas de freguesia com 55 casos, que incluem ATM instaladas no seu interior como integradas na parede na parte exterior das instalações ou numa instalação anexa à mesma (20,8%). Em terceiro lugar surge as ATM instaladas na via pública com 37 ocorrências (14,0%). Estes três locais representam, em conjunto, aproximadamente dois terços das ocorrências.

De destacar ainda os hipermercados, supermercados e minimercados com 23 registos (8,7%), bem como os postos de abastecimento de combustível (17 ocorrências, 6,4%).

Também merecem referência os estabelecimentos comerciais (3,8%), os restaurantes, snack-bares e pastelarias (3,0%) e os clubes e associações (2,6%).

As demais categorias, entre as quais se incluem postos de turismo, unidades hoteleiras, antigas agências bancárias, estabelecimentos de ensino, edifícios habitacionais, serviços postais, entre outros registam uma incidência bastante residual, inferior ou igual a 0,8% cada.

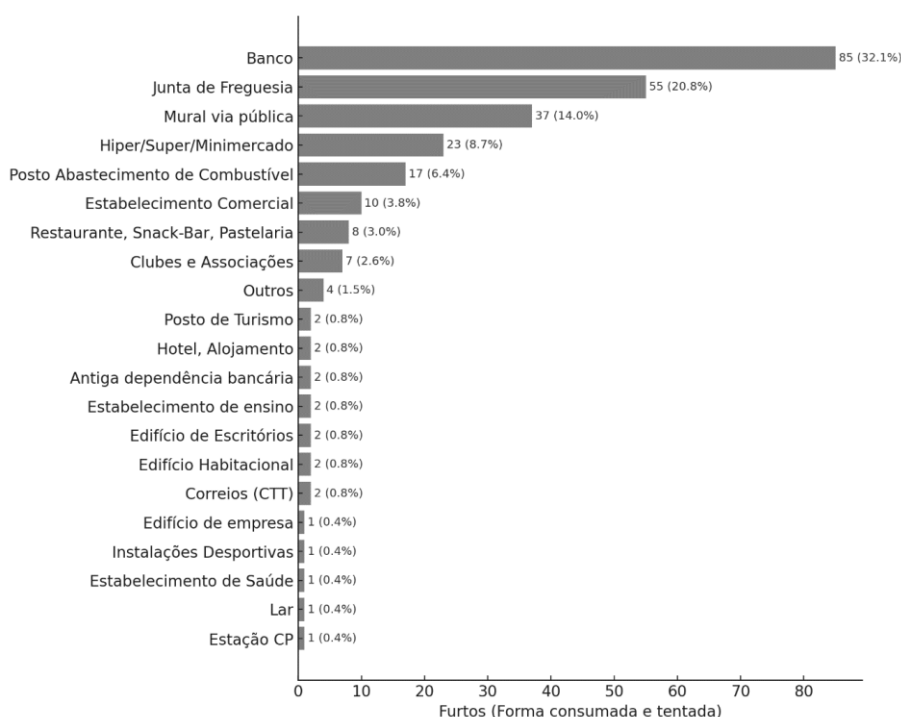


Figura n.º 15 - Tipo de local

Entre os bancos onde foram registados furtos aos seus ATM, a Caixa de Crédito Agrícola (CCA) registou o maior número de furtos a caixas automáticas multibanco (ATM), com um total de 42 ocorrências, correspondentes a 49,4% do total de furtos registados em bancos (Figura n.º 16).

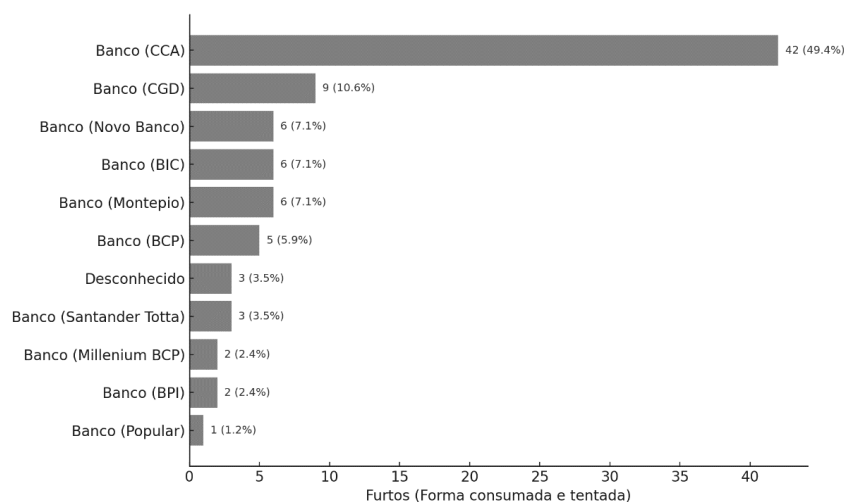


Figura n.º 16 - Furtos ATM por banco

4.1.6 Veículos e fuga

Em 81 ocorrências (das 265⁷⁹) foi identificado um possível veículo de fuga. Das 13 marcas registadas, as marcas alemãs BMW e Audi são as mais frequentemente utilizadas neste tipo de furtos, com 39,7% e 19,2% dos casos, respetivamente, totalizando cerca de 59%.

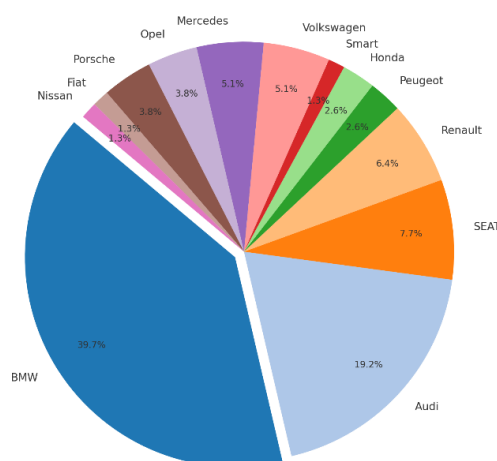


Figura n.º 17 - Marcas das viaturas suspeitas

4.1.7. Número de indivíduos

Nos dados disponíveis foi possível identificar o número de indivíduos suspeitos em 123 ocorrências (das 265⁸⁰). A média do número de suspeitos por furto é de aproximadamente 2,76, com um desvio padrão de cerca de 1,06, indicando uma baixa

⁷⁹ 30,57% do total das ocorrências

⁸⁰ 46,42% do total das ocorrências

dispersão (Figura n.º 18). A análise revela uma predominância de grupos compostos por dois a quatro elementos. Sendo que a moda foi de três (elementos), indicando que o número de suspeitos mais registado foi de três elementos. As ocorrências envolvendo apenas um ou dois suspeitos surgem com menor expressão. Já os registos com cinco suspeitos foram pouco frequentes.

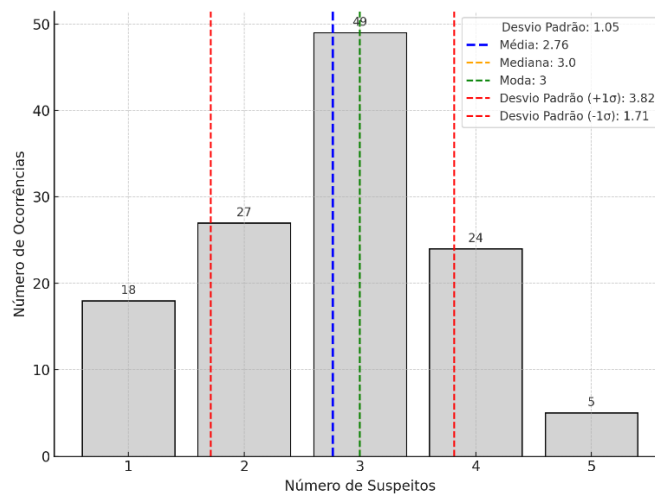


Figura n.º 18 - Número de indivíduos suspeitos

4.1.8. Sistemas de Videovigilância

A presença de sistemas de videovigilância foi registada em 135 ocorrências (cerca de 52% dos casos analisados), ao passo que em 76 ocorrências (29%) foi confirmada a ausência destes sistemas. No entanto em 54 ocorrências (aproximadamente 19%) a informação é desconhecida.

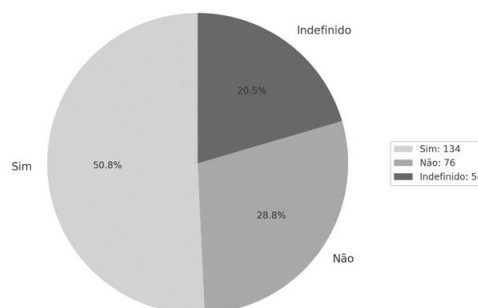


Figura n.º 19 - Sistemas de videovigilância

4.2 Apresentação e análise das entrevistas

A primeira questão “Na prevenção de furtos de/a ATM que indicadores de alerta identifica como relevantes?” procurou perceber que indicadores podem alertar para este fenómeno criminal. A análise dos indicadores de alerta associados à prática de furtos de e a ATM foi dividida em três grupos: avarias na ATM, viaturas e outros crimes associados (Quadro n.º 7).

No que concerne às avarias nas ATM, observa-se que este fator foi identificado por 44% dos entrevistados como um indicador relevante. Segundo quatro entrevistados, uma ATM fora de serviço pode ser fruto de ações de quem pretende atacar a ATM, com o objetivo de impedir a utilização (especialmente a realização de levantamentos de dinheiro) por parte dos utilizadores, potenciando assim o lucro do furto, ou então como refere o E7, em caso de anomalia a ATM é verificada e novamente carregada, ficando totalmente abastecida e vulnerável à ação dos perpetradores.

Relativamente ao uso de viaturas é referido por 33% dos entrevistados a utilização de automóveis de alta cilindrada (A.2.1). Alguns entrevistados mencionam algumas marcas específicas: BMW (33%), Audi (22%), Seat (11%) e Grupo Volkswagen⁸¹ (22%). A utilização de carrinhas (A.2.2) (22%) surge como uma opção estratégica, sobretudo quando os furtos implicam o transporte de ferramentas/ instrumentos volumosos ou da própria estrutura da ATM.

No domínio de outros crimes associados ou percursos, destaca-se o furto de veículos com uma representatividade de 44%, evidenciando a sua função instrumental na execução dos furtos de ATM. O furto de botijas de gás, nomeadamente de acetileno, aparece em 33% das entrevistas, remetendo para um tipo específico de método de ataque, através de explosão. Por sua vez, o furto de extintores, com 22% de menções, é entendido como um comportamento complementar, normalmente utilizado como elemento de distração ou de mitigação da resposta policial durante o furto.

⁸¹ Volkswagen, Audi, SEAT, Škoda, Bentley, Bugatti, Lamborghini, Porsche, Ducati; Scania, MAN, International e IC Bus

Quadro n.º 7 - Análise entrevistas: Indicadores de alerta

Categoria	Subcategoria	Código	E1	E2	E3	E4	E5	E6	E7	E8	E9	Resultado
Avarias na ATM	-	A.1	x				x		x		x	4/9(≈ 44%)
Viaturas	Alta cilindrada	A.2.1		x	x					x		3/9(≈ 33%)
	Carrinhas	A.2.2				x			x			2/9(≈ 22%)
Marcas de automóveis	BMW	A.3.1			x	x			x			3/9(≈ 33%)
	Audi	A.3.2			x				x			2/9(≈ 22%)
	Grupo Volkswagen	A.3.3				x			x			2/9(≈ 22%)
	SEAT	A.3.4			x							1/9(≈ 11%)
Outros crimes associados	Furto de veículos	A.4.1		x	x				x	x		4/9(≈ 44%)
	Furtos de botijas de gás (acetileno)	A.4.2				x			x	x		3/9(≈ 33%)
	Furto de Extintores	A.4.3							x	x		2/9(≈ 22%)

Na segunda questão: “De que forma o carregamento da ATM influencia o planeamento deste tipo de ataques?” teve como objetivo perceber qual a preponderância do carregamento para os perpetradores (Quadro n.º 8).

A influência do carregamento da ATM emerge como o indicador com maior grau de consenso, sendo mencionado por 78% dos entrevistados. Este resultado sugere que os grupos criminosos, especialmente os GCO, tendem a identificar os momentos de reabastecimento das ATM como oportunidades estratégicas para maximizar o retorno financeiro. Nas E2, E6 e E7 foi referido que estes grupos obtêm esta informação de forma “privilegiada” quer através de informadores que residem ou trabalham junto da caixa ATM ou então de funcionários das empresas responsáveis pelo carregamento.

Quadro n.º 8 - Análise entrevistas: Carregamento do ATM

Categoria	Subcategoria	Código	E1	E2	E3	E4	E5	E6	E7	E8	E9	Resultado
Carregamento do ATM	Tem influência no planeamento	A.5.1	x	x		x	x	x	x		x	7/9(≈ 78%)
	Depende	A.5.2								x		1/9(≈ 11%)
	Não influência o planeamento	A.5.3			x							1/9(≈ 11%)

A questão 3 “Que fatores do local onde a ATM está instalada podem influenciar a decisão em praticar furtos de/a ATM?”, procurou perceber de que forma o local, quer a infraestrutura onde está instalado e os arredores desse mesmo local podem influenciar este tipo de furtos (Quadro n.º 9).

Verifica-se que “Isolamento geográfico” (B.1.3) e “Pontos de fuga” (B.1.4) foram unanimemente (100%) identificados como características relevantes. Este resultado evidencia uma perceção comum entre os entrevistados de que os perpetradores têm em consideração estes dois fatores no momento da seleção do local onde pretende realizar o furto. O isolamento geográfico é apontado como um elemento que dificulta a resposta rápida das FS e reduz a presença de potenciais testemunhas. Paralelamente, a existência de pontos

de fuga, como autoestradas ou vias rápidas nas imediações, permite percorrer grandes distâncias em poucos minutos e dificultando a detenção dos suspeitos.

A subcategoria “Iluminação” (B.1.1) e “Fragilidade do local” (B.1.2) foram mencionadas ambas em cerca de 67% de resposta, refletindo que a maioria dos entrevistados reconhece estes fatores como facilitadores. A débil iluminação é vista como uma condição que reduz a vigilância natural e permite aos perpetradores agirem de forma mais dissimulada, dificultando a perceção por parte de eventuais testemunhas. Relativamente à fragilidade do local, os entrevistados referem-se essencialmente à infraestrutura física do espaço onde a ATM está instalado, apontando a falta de resistência estrutural como um fator crítico. Exemplos como portas fáceis de arrombar, fachadas em vidro ou instalações anexas a edifícios pouco robustos, como se verificou em algumas juntas de freguesia, foram mencionados. Estas condições oferecem um acesso rápido e direto ao interior, permitindo que os perpetradores atinjam o terminal multibanco com relativa facilidade.

Quadro n.º 9 - Análise entrevistas: Características do local

Categoria	Subcategoria	Código	E1	E2	E3	E4	E5	E6	E7	E8	E9	Resultado
Características do local	Iluminação	B.1.1	x	x		x		x		x	x	6/9(≈ 67%)
	Fragilidade do local	B.1.2		x	x	x	x	x	x			6/9(≈ 67%)
	Isolamento geográfico	B.1.3	x	x	x	x	x	x	x	x	x	9/9(100%)
	Pontos de fuga	B.1.4	x	x	x	x	x	x	x	x	X	9/9(100%)

A questão 4 “Com base nos *Modi Operandi* registados em Portugal, nos últimos anos, quais são as características da ATM que poderão ampliar a vulnerabilidade desta infraestrutura à prática de furtos?” tinha como objetivo identificar quais as características específicas das ATM, com base na experiência dos entrevistados, aumentam a sua vulnerabilidade a este tipo de furtos (Quadro n.º 10).

Os “Sistemas de Segurança” (C.2) foram mencionados por 78% dos entrevistados, como um fator importante. Este resultado evidencia a perceção generalizada de que a presença (ou ausência) de mecanismos de segurança influencia significativamente a vulnerabilidade do ATM. Os sistemas de alarme, videovigilância e proteção física são vistos como dissuasores da ação criminosa.

Relativamente à relevância do modelo da ATM na seleção dos seus alvos por parte dos perpetradores é quase unanime (89%) que “Tem influência” (C.3.1). Os entrevistados consideram que o modelo da ATM pode facilitar ou dificultar a ação dos perpetradores. Os E4, E7 e E9 destacam os modelos DV213/1413 da marca portuguesa De La Rue, como modelos preferenciais dos perpetradores, especialmente com ataques com gás. Nas E1, E2 e E6 foi referido que os modelos mais antigos são mais vulneráveis. Esta fragilidade é

associada ao facto de os modelos mais antigos não estarem sujeitos aos sistemas de segurança mais recentes e mais eficazes contra determinados tipos de ataque. Em contraste, os modelos mais recentes refletem a evolução da indústria na resposta a este tipo de criminalidade, sendo concebidos com materiais mais robustos e sistemas de proteção mais avançados.

O tipo de ATM segundo E7 e E8 está intimamente relacionado com o MO e categoria ou subcategoria de ataque. As ATMs instaladas de forma autónoma são mais suscetíveis a ataques do tipo ATM - no local, especialmente com recurso a corte ou arrombamento, devido à sua estrutura estar mais exposta. Por outro lado, as ATMs integradas na parede tendem a ser mais visados em ataques com explosivos gasosos.

A “Entidade gestora” (C.1) foi mencionada por dois dos entrevistados. Nas E7 e E4, destacaram que a CCA como o principal alvo dos perpetradores em comparação com outros bancos. Segundo os participantes, esta tendência está diretamente associada ao facto das ATM desta instituição serem regularmente carregados por funcionários do próprio banco. Este procedimento, é dos conhecimentos dos perpetradores levando-os a presumir que a ATM, em regra, está carregada.

Quadro n.º 10 - Análise entrevistas: Características da ATM

Categoria	Subcategoria	Sub-subcategoria	Código	E1	E2	E3	E4	E5	E6	E7	E8	E9	Resultado
Características da ATM	Entidade gestora	-	C.1				x			x			2/9(≈ 22%)
	Sistemas de Segurança	-	C.2	x	X	x	x	x	x			x	7/9(≈ 78%)
	Modelo	Tem influência na seleção dos alvos	C.3.1	x	x	x	x		x	x	x	x	8/9(≈ 78%)
		Não tem influência na seleção dos alvos	C.3.2										0/9(0%)

A questão 5 “Como pode a GNR prevenir a prática de crimes de furto de/a ATM?” teve como objetivo perceber junto dos entrevistados onde a GNR deve incidir os seus recursos na debelação de furtos a ATM (Quadro n.º 11).

Relativamente às medidas que a GNR deve adotar para reduzir este tipo de furtos, destaca-se com particular relevância a “Recolha e tratamento de informação” (D.3), assinalada por 89% dos entrevistados. Esta prática é referida como essencial para compreender a dinâmica dos furtos a ATMs. Os entrevistados defendem a necessidade da recolha e tratamento de informação com objetivo de identificar padrões de atuação dos grupos criminosos, como horários, MO, tipos de equipamentos visados ou localização preferencial, permitindo alocar os recursos, principalmente as patrulhas, para as zonas de maior risco.

Essa necessidade de prever possíveis alvos está ligada ao facto de que 56% dos entrevistados (E1, E2, E3, E8 e E9) terem a perceção que os grupos responsáveis por esse tipo de ataques planeam os seus ataques, realizando reconhecimento prévio dos locais e seleção das ATM.

Dentro das estratégias de patrulhamento, o “Patrulhamento – locais de risco” (D.5.1), foi mencionada por 78% dos entrevistados. Esta estratégia está centrada na orientação do patrulhamento para zonas previamente identificadas como mais suscetíveis à ocorrência deste tipo de crimes. Menos rereferida, apenas por 33% dos entrevistados, o “Patrulhamento - comportamentos suspeitos” (D.5.2), os entrevistados referiem a importância de alertar e capacitar os militares da GNR, para a identificação de comportamentos considerados atípicos ou suspeitos nas imediações das ATMs.

A “Cooperação” (D.4), referida por 78% dos entrevistados, surge como um dos pilares fundamentais para uma prevenção eficaz. Face à sofisticação e mobilidade dos grupos criminosos, os entrevistados destacam a importância de um trabalho articulado entre as FS, as instituições financeiras, em especial a Forward Payment Solutions (SIBS), entidade gestora de uma parte bastante considerável da rede Multibanco em Portugal, e outras entidades ou parceiros relevantes.

A “Ficha de avaliação de risco” (D.2) foi mencionada por dois entrevistados sublinhando a necessidade do cumprimento rigoroso desta ficha na prevenção de furtos a ATM. Também referida por 22% dos entrevistados, surge a importância de envolver a comunidade local na prevenção, nomeadamente através do alerta e da denúncia de comportamentos suspeitos junto das ATMs (“Sensibilizar a população” (D.1).

Quadro n.º 11 - Análise entrevistas: Prevenção de furto de ATM

Categoria	Subcategoria	Sub-subcategoria	Código	E1	E2	E3	E4	E5	E6	E7	E8	E9	Resultado
Prevenção	Sensibilizar a população	-	D.1		x							x	2/9(≈ 22%)
	Ficha de avaliação do risco	-	D.2					x		x			2/9(≈ 22%)
	Recolha e tratamento de informação	-	D.3	x	x	x	x	x	x		x	x	8/9(≈ 89%)
	Cooperação	-	D.4	x	x			x	x	x	x	x	7/9(≈ 78%)
	Patrulhamento	Locais de risco	D.5.1	x		x		x	x	x	x	x	7/9(≈ 78%)
		Comportamentos suspeitos	D.5.2	x	x							x	3/9(≈ 33%)

4.3 Discussão dos resultados

Tal como se verifica no panorama europeu, descrito nos relatórios da EAST, também em Portugal se observa um claro predomínio dos ataques físicos face aos ataques lógicos. Entre 2016 e 2024, na área de responsabilidade da GNR, 94% dos registos corresponderam

a ataques físicos, enquanto apenas 6% se referiram a ataques lógicos. Dentro dos ataques físicos, dois métodos destacam-se de forma expressiva: os ataques com explosivos e o furto da ATM - no local, que em conjunto representam 94% dos ataques físicos, ou seja, cerca de 88% do total de ocorrências registadas no período analisado.

Praticamente metade dos ataques físicos a ATMs envolveram o uso de explosivos gasosos, apresentando uma taxa de consumação de 67,7%, ou seja, em mais de dois terços dos casos o objetivo do furto foi efetivamente alcançado. A elevada taxa de sucesso, quando comparada a outros MO, aliada à complexidade técnica envolvida, sugere a atuação de grupos criminosos altamente especializados, com domínio de conhecimentos técnicos, acesso a materiais específicos e capacidade de planeamento, organização e execução rápida. Conforme apontam a REPC & Europol (2019), fatores como o planeamento detalhado do furto e a experiência e conhecimentos (especialização) dos perpetradores são determinantes para o êxito destas ações criminosas.

Por outro lado, os furtos das ATM – no local, especialmente por arrombamento, um dos mais usuais MO em Portugal, apresentam uma percentagem de consumação bastante reduzida, podendo estar associada a grupos menos organizados ou menos experientes, com caráter mais oportunista que tendem a realizar tentativas que não são bem-sucedidas (REPC & Europol, 2019).

Ao nível dos ataques lógicos, é possível observar que os primeiros casos registados na área da GNR ocorreram em 2020, precisamente o ano em que, segundo o relatório da EAST, se verificou o maior número de ataques deste tipo na Europa. Contudo, estes ataques, que exige conhecimentos técnicos específicos, continuam a ser esporádicos e sazonais em Portugal.

De acordo com o REPC & Europol (2019), os grupos envolvidos em furtos a ATM dedicam um esforço substancial à seleção criteriosa dos alvos, analisando variáveis como o horário do carregamento de numerário, o ambiente envolvente, as características técnicas dos equipamentos, os itinerários de fuga e as medidas de segurança implementadas, nomeadamente sistemas de videovigilância e sensores de alarme. Esta preocupação dada ao planeamento é igualmente referida pela ATMIA (2014a) e por cinco dos nove entrevistados, que confirmam que, na maioria dos casos, os furtos a ATM são cuidadosamente planeados.

Entre os fatores mais determinantes, destaca-se o carregamento das ATM, identificado pelo REPC & Europol (2019) e pela quase totalidade dos entrevistados como um elemento crítico na definição do momento do furto.

A localização das ATM surge também como uma variável essencial, influenciando diretamente o nível de risco associado e, consequentemente, a atratividade. Esta escolha não ocorre de forma aleatória, sendo condicionada por fatores físicos e contextuais que favorecem a execução do furto e dificultam a atuação das FS. A proximidade a vias rápidas e autoestradas referida por todos os entrevistados, é estrategicamente valorizada pelos perpetradores, ao permitir uma fuga célere e eficaz (ATMIA, 2014a).

Todos os entrevistados identificaram como fatores críticos o isolamento das ATM e as condições de fuga, refletindo a percepção de que a ausência de vigilância no entorno imediato potencia a concretização do furto. Paralelamente é destacada de forma unânime a importância da proximidade a infraestruturas rodoviárias como condição essencial para garantir uma fuga rápida e segura.

A análise da distribuição espacial dos furtos ocorridos na área de jurisdição da GNR de 2016 a 2024, demonstra uma forte concentração nos distritos do litoral, com especial incidência no Porto e em Lisboa, seguidos por Aveiro, Setúbal e Leiria. Esta concentração pode ser explicada por fatores como a maior densidade populacional, a elevada presença de ATM e uma rede rodoviária bem desenvolvida, que facilita tanto o acesso como a fuga dos locais.

No plano temporal, verifica-se uma distribuição mensal relativamente homogênea, com variações pouco significativas. No entanto, a análise semanal revela uma assimetria expressiva: 81,4% das ocorrências registam-se durante os dias úteis, com uma progressão ascendente entre segunda e sexta-feira, culminando com um pico de furtos à sexta-feira. Em termos horários, os furtos concentram-se entre as 02h00 e as 05h00 da manhã, com o pico de incidência às 04h00. Estes dados são consistentes com a literatura existente, que assinala o período noturno como especialmente propício à ocorrência de determinados crimes, especialmente crimes mais violentos, devido à reduzida circulação de pessoas e à menor presença das FS (Thomas et al., 2024; Sánchez-Delgado, 2024).

A fragilidade do local de instalação foi referida por seis dos nove entrevistados, estabelecendo assim uma convergência com análise quantitativa. Em diversos casos analisados, as ATM encontravam-se instalados em anexos ou integrados nas paredes exteriores de edifícios, como os das juntas de freguesia ou em algumas localidades com menor densidade populacional, o que lhes conferia reduzida resistência física contra furtos.

O REPC & Europol (2019) identifica como particularmente vulneráveis as ATM instalados no exterior de edifícios, integradas nas paredes, ou instaladas de forma autónoma no interior de estabelecimentos comerciais. Os perpetradores tendem a privilegiar este tipo

de equipamento em detrimento das ATM instalados em bancos, onde, em regra, se verifica a presença de um maior número de medidas de segurança. A localização da ATM assume, assim, um papel central na avaliação do risco e na definição da atratividade do alvo.

Apesar de 32,1% das ocorrências se verificarem em bancos, especialmente na CCA, que representa praticamente metade deste valor, valor que à primeira vista poderá parecer contraditório com as tendências da literatura, os restantes 67,9% ocorreram noutra tipo de locais, confirmando a preferência por alvos com menores níveis de proteção física.

As juntas de freguesia destacam-se como o segundo tipo de local mais visado (20,8%), o que é particularmente relevante, considerando tratar-se de infraestruturas frequentemente situadas em áreas de baixa densidade populacional e com reduzida presença humana fora do horário de expediente. As condições estruturais frágeis, como portas em vidro, paredes pouco resistentes e acessos de fácil arrombamento, foram identificadas como fatores críticos por cerca de 67% dos entrevistados.

As ATM integradas em murais exteriores em via pública representam 14% do total de ocorrências. Estas ATM, habitualmente sem proteção física envolvente, revelam-se especialmente vulneráveis durante o período noturno. Outros tipos de locais relevantes são os hiper/super/minimercados (8,7%) e os postos de abastecimento de combustível (6,4%). Uma das principais vulnerabilidades destes locais pretende-se com os horários regulares destes estabelecimentos.

No que diz respeito às características das ATM, a literatura e os entrevistados referem a importância de considerar simultaneamente a localização e a tipologia construtiva dos equipamentos. O estudo da TrendMicro & Europol (2017) evidencia que os ataques lógicos são muitas vezes desenvolvidos com base em vulnerabilidades específicas de determinados fabricantes, componentes físicos ou versões de software.

A distinção entre ATM integradas na parede e ATM autónomos foi salientada pelos entrevistados E7 e E8, que sublinham a existência de vulnerabilidades distintas, consoante o MO utilizado. As ATM integradas são mais suscetíveis a ataques com explosivos. Já as ATM autónomas, geralmente localizados em estabelecimentos comerciais, são frequentemente alvo de arrombamento ou remoção total, beneficiando da menor resistência física, no entanto não há nenhuma evidencia da literatura que confirme estas afirmações, nem foi possível fazer essa análise através dos dados quantitativos.

Relativamente às medidas de dissuasão, 78% dos entrevistados associaram a presença de sistemas de segurança (como videovigilância e alarmes) à mitigação deste tipo de furtos, em consonância com as recomendações do REPC & Europol (2019). No entanto, a

constatação de que mais de metade dos furtos ocorreram em locais onde existia videovigilância reforça a ideia de que, estes sistemas não são, por si só, um fator de dissuasão suficiente.

Por fim, foi referido por parte considerável dos entrevistados, que o modelo da ATM influencia diretamente a seleção do alvo. Alguns entrevistados mencionaram o modelo “De La Rue: DV213/1413” e, de forma genérica, os “modelos mais antigos”. Embora a ausência de dados quantitativos impossibilite a confirmação da maior vulnerabilidade destes modelos, a sua recorrência nas respostas justifica a sua inclusão prioritária nas análises de risco e nas estratégias de mitigação.

No que diz respeito às viaturas utilizadas, fator igualmente relevante no planeamento e preparação de um furto a ATM, a literatura aponta para utilização, principalmente de viaturas furtadas, criteriosamente selecionadas para a evasão do local do furto (ATMIA, 2014a). Esta tendência é confirmada pela análise das entrevistas onde quatro dos entrevistados referem o furto de viaturas com um indicador de alerta. A literatura aponta para a utilização recorrente de veículos de alta cilindrada e elevado desempenho, com destaque para as marcas BMW e Audi, especialmente modelos de maiores dimensões como carrinhas (ATMIA, 2014a). A análise dos furtos a ATM registadas permitiu observar que 39,7% dos veículos identificados pertencem à marca BMW e 19,2% à Audi. Estas mesmas marcas são ainda referidas por 33% dos participantes, tendo sido ainda feita referida a marca SEAT e ainda o grupo Volkswagen. A SEAT representa 7,7% dos veículos identificados, logo atrás da BMW e Audi. De destacar que cumulativamente a Audi, SEAT, Volkswagen, Porsche, todas elas pertencentes ao grupo Volkswagen representam 35,9% dos veículos identificados, como é possível observar na Figura n.º 20. O recurso a modelos de maiores dimensões, como carrinhas, mencionada na literatura como uma prática comum, foi igualmente referida por dois entrevistados, no entanto os dados quantitativos disponíveis não permitiram realizar esta análise.

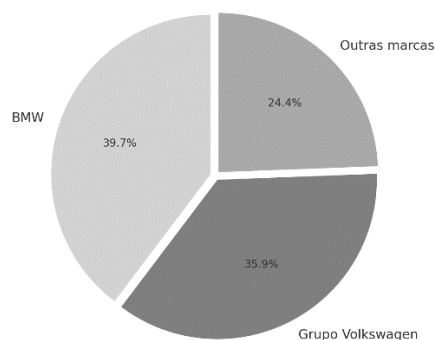


Figura n.º 20 - Comparação marcas/grupos de viaturas

No que respeita ao número de elementos, existe um consenso entre o que a literatura refere e a análise dos furtos registados. O relatório do RAGNR (2018) estima que a realização de um furto requer entre três a quatro indivíduos. A ATMIA (2014a) vai de encontro com esta estimativa, apontando que os grupos atuam geralmente em duplas ou trios, compostos quase exclusivamente por homens. A análise efetuada reforça esta tendência, com a maioria das ocorrências em que foi possível identificar o número de suspeitos a situar-se entre dois e quatro indivíduos, sendo que cerca de metade dos registos referem a presença de três indivíduos.

Outro potencial indicador é ATMs fora de serviço. A inoperacionalidade prévia das ATM é apontada pela ATMIA (2014a) como um possível indicador de ataque iminente, sendo esta prática identificada por quatro dos nove entrevistados, que reforça a importância de monitorizar alterações anómalas no funcionamento das ATM, que podem ter sido previamente realizadas pelos futuros perpetradores destes ataques, com o objetivo de maximizar o valor furtado.

O ATMIA (2014a) identificou o furto de garrafas de gás acetileno, especialmente em serralharias e oficinais de automóveis, como possível indício antecessor, particular no furto com explosão através de gás. Este potencial crime antecedente é igualmente mencionado por três entrevistados, o que reforça o seu papel como potencial indicador da preparação para um ataque com o recurso a explosivos gasosos.

Relativamente às estratégias para a prevenção deste fenómeno, comparando as recomendações da REPC & Europol com os resultados das entrevistas realizadas é possível observar diversas convergências. Uma das convergências mais evidentes refere-se à recolha e tratamento sistemático da informação, apontada como prioritária por 89% dos entrevistados. Esta prática está em consonância com a primeira etapa da estratégia delineada pela REPC & Europol, que defende a necessidade de uma avaliação aprofundada da situação,

assente na análise de padrões criminais, histórico de incidentes e fatores de risco associados às ATMs.

Os sistemas de segurança das ATMs, mencionados pela maioria dos entrevistados (78%), desempenham um papel central na prevenção deste tipo de furto, de acordo com o REPC & Europol. Estes sistemas inserem-se em três pilares: a diminuição da recompensa, através do mecanismo de tintage das notas (IBNS); o aumento do risco, com a utilização de sistemas de videovigilância; e o aumento do esforço, por meio de mecanismos que dificultam o acesso ao cofre ou à caixa de segurança da ATM (REPC & Europol L, 2019).

A cooperação interinstitucional, entre FS, bancos e outros organismos, em especial a SIBS, é essencial para garantir uma atuação coordenada e eficaz, tanto na prevenção como na resposta a incidentes mencionada por 78% dos entrevistados, é igualmente destacada nas medidas paralelas que compõem as recomendações da REPC & Europol (2019) e apontada pelo RASI de 2017 como uma das principais causas para a queda do número de furtos a ATM em Portugal.

Apesar de pouco mencionada pelos entrevistados a ficha de avaliação de risco, uma das principais se não a principal estratégia implementada em Portugal para debelar os furtos a ATM, está diretamente relacionada com dois dos três pilares da prevenção delineada pela REPC & Europol, o aumento do esforço e a diminuição da recompensa. Esta avaliação avalia entre outros: medidas de segurança a que a ATM está sujeita, as condições do local da instalação e os montantes disponíveis. Diferente desta avaliação é a construção de um perfil de risco individualizado para cada ATM proposto pela REPC & Europol (2019). Apesar de se tratarem de avaliações distintas, a primeira focada no processo de instalação e a segunda relativa a ATMs já instaladas, estas estratégias, embora diferentes, são complementares.

Relativamente ao patrulhamento realizado pelas FS, e no caso em concreto a GNR, 78% dos entrevistados referem a necessidade de o patrulhamento ser orientado para locais de risco. Estratégia essa que está alinhada com o pilar do aumento do risco definida pela prevenção situacional da REPC & Europol, que preconiza o reforço da presença das FS, especialmente em locais e horários de maior risco. Análise do histórico de furtos a ATM, na área da GNR, entre 2016 a 2024 e análise das entrevistas realizadas, possibilitou o reconhecimento de alguns locais mais propícios a este tipo de furtos, tais como locais mais isolados ou com bons pontos de fuga, ATMs instalados em locais que dispõem de um número mais reduzido sistemas de segurança, ou então modelos de ATM mais vulneráveis. No plano temporal, a incidência concentrou-se nos dias úteis, especialmente à sexta-feira, sobretudo durante a madrugada (entre as 02h00 e as 05h00 da manhã).

A sensibilização da população, referida por 22% dos entrevistados, está associada à promoção da denúncia de comportamentos suspeitos por parte dos cidadãos, o que contribui para a deteção precoce de possíveis ameaças, que constitui um dos objetivos, dentro do pilar do aumento do esforço da estratégia de prevenção estabelecida pela REPC & Europol.

CONCLUSÕES E RECOMENDAÇÕES

A investigação desenvolvida teve como propósito central compreender como a GNR pode direcionar a prevenção para debelar os furtos a ATM. Neste sentido, a análise desenvolvida permitiu, de forma sustentada, responder às perguntas derivadas previamente formuladas, para então se culminar na resposta à pergunta de partida.

Resposta à **QD1**: Quais os MO que tem vindo a ser adotadas em Portugal Continental, na área de jurisdição da GNR?

No que diz respeito aos MO, há predomínio claros dos ataques físicos, especialmente ataques com recurso a explosivos e Furto da ATM – no local. A categoria mais comum é o recurso a ataques explosivos, especialmente com recurso a explosivos gasosos, método que apresentou uma elevada taxa de consumação (aproximadamente 67,7%). Esta taxa de consumação evidencia que estes indivíduos ou grupos de indivíduos possuem conhecimentos, organização e experiência necessário para realizar este tipo de furtos.

A perigosidade deste tipo de ataque é agravada pelo seu potencial destrutivo, uma vez que os danos não se limitam à própria ATM, estendendo-se frequentemente às estruturas envolventes, nomeadamente aos edifícios onde os equipamentos se encontram instalados. Tendo em conta que muitos destes edifícios são de carácter habitacional, os ataques contribuem de forma significativa para o aumento do sentimento de insegurança nas zonas afetadas. Assim, este MO exige uma atenção reforçada por parte das FS e das demais entidades com competências na prevenção e combate a este fenómeno criminal.

O furto da ATM - no local constitui a segunda categoria mais prevalente entre os ataques físicos. Este consiste na tentativa de acesso ao cofre ou à caixa de segurança da ATM no próprio local de instalação, recorrendo a ferramentas como rebarbadoras, alicates, pés de cabra e marretas. Entre as subcategorias identificadas, destacam-se os métodos de corte e arrombamento. Embora o arrombamento seja uma técnica amplamente utilizada, apresenta uma baixa taxa de sucesso (17,5%), contrastando com o corte, que, apesar de menos frequente, regista uma taxa de consumação superior (57,1%). Este contraste evidencia que a frequência de uso de um determinado MO nem sempre está correlacionada com a sua eficácia.

Por outro lado, os ataques lógicos têm ocorrido de forma esporádica e sazonal. Apesar de menos comuns, estes ataques são particularmente dirigidos a determinados fabricantes, modelos ou versões de *software*, o que denota um grau de especialização técnica por parte

dos perpetradores. O designado ataque *Black Box* constitui o principal método lógico identificado, com maior incidência em 2022. No entanto, à semelhança do que se verifica na Europa, este tipo de ataque começa a ser muito residual, quase inexistente.

Resposta à Q12: Compreender quais os padrões de interesse para a GNR para prevenir os crimes contra ATM em Portugal?

Em regra, especialmente quando falamos em grupos organizados, estes furtos são cuidadosamente planeados. A grande maioria dos furtos envolve uma escolha criteriosa (vulnerabilidade, isolamento geográfico e itinerários para a fuga) do alvo. Em regra, há um prévio reconhecimento e estudo do local e do ambiente circundante, nomeadamente os itinerários de fuga, e controlo/estudo dos carregamentos de numerário nas ATM, assim como as especificações técnicas das ATM, e as medidas de segurança implementadas. Os perpetradores tendem a selecionar ATMs situadas nas proximidades de vias com bons acessos, especialmente autoestradas ou vias rápidas, e em zonas relativamente isoladas, com o objetivo de garantir uma fuga rápida, reduzindo substancialmente a probabilidade de intervenção policial durante a execução do furto.

A composição e atuação destes grupos seguem um padrão consistente: atuam em grupos três a quatro indivíduos, geralmente do sexo masculino, muitas vezes ligados a redes organizadas de crimes contra o património.

Antes da execução do furto ao ATM, é frequente a prática de crimes preparatórios. No caso dos ataques com explosivos gasosos é recorrente o furto de botijas de gás acetileno especialmente em serralharias ou em oficinas de automóveis. Comum a todos os MO é o furto de viaturas de alta cilindrada e de preferência modelos de maiores dimensões, espacialmente da marca BMW e grupo Volkswagen, em especial a Audi e SEAT.

Um dos indicadores de um possível ataque é ATMs fora de serviço. Determinados grupos para maximizarem os seus lucros acabam por previamente inoperacionalizar as ATMs, por exemplo, obstruindo as entradas para os cartões ou saída do dinheiro.

Geograficamente, verificou-se uma concentração espacial dos furtos nos distritos do litoral do país, especialmente Porto, Lisboa, Aveiro, Setúbal e Leiria, coincidente com áreas de maior densidade populacional e, fundamentalmente, com melhor acessibilidade rodoviária. No plano temporal, a incidência concentra-se marcadamente nos dias úteis (81,4% dos casos), com um pico às sextas-feiras (20,9%), e sobretudo durante a madrugada (58,5% das ocorrências entre as 02h00 e as 05h00 da manhã).

Outro dado relevante, pese embora cerca de 32% dos furtos tenham ocorrido em ATM instaladas em bancos, a maioria (cerca de 68%) teve lugar fora dos bancos,

nomeadamente em locais mais isolados com menor vigilância e por sua vez mais vulneráveis. Os locais mais visados foram as ATM instaladas em bancos, juntas de freguesia e ATM instaladas em murais na à via pública. Com menor incidência mais ainda com alguma relevância surgem os Hiper e supermercados e os postos de abastecimento de combustível e os clubes e associações, localizados em zonas mais isoladas. Dentro dos bancos, face aquilo que foi o histórico de furtos, a CCA representa praticamente metade dos furtos registados, destacando-se consideravelmente dos restantes bancos.

Com base em toda a investigação realizada e após respondidas as Q_D, importa nesta fase responder ao Q_P: Como pode a GNR direcionar a prevenção a crimes de furto a ATM?

A análise realizada permite concluir que este tipo de criminalidade apresenta um elevado grau de complexidade, estando, na maioria dos casos, associada à atuação de GCO que operam de forma organizada e planeada. Esta complexidade exige das FS uma resposta assente numa abordagem multidisciplinar, através de estratégias intimamente relacionadas com a prevenção situacional (aumento do risco, aumento do esforço e a redução de recompensas).

Para esse efeito, destaca-se a importância da construção de um perfil de risco individualizado para cada ATM, onde devem ser considerados determinados fatores que contribuem para o aumento da vulnerabilidade de determinada ATM.

Entre os aspetos mais relevantes incluem-se as características da localização e do enquadramento territorial, a posição física, o tipo de ATM, volume do dinheiro armazenado, medidas de segurança implementadas e histórico de incidentes e tipos de ataques registados.

A caracterização da localização e o enquadramento territorial inclui critérios como a densidade populacional, como por exemplo se está inserido em zonas urbanas ou rurais, a proximidade de postos ou esquadras das FS e a presença de sistemas de segurança, como videovigilância.

Avaliação da posição física da ATM, prende-se com a distinção entre ATMs instaladas dentro ou fora de edifícios, em bancos ou em locais como juntas de freguesia, estabelecimentos comerciais ou então instalados na via pública. Prende-se ainda com o seu tipo de instalação, integrado na parede ou instalado de forma autónoma (regra geral no interior de um edifício). No tipo de ATM é importante dar especial relevância a determinadas ATMs, entre elas: ATM com fácil acesso a sua parte de trás, a modelos mais antigos que em regra estão sujeitos a um número mais reduzido de medidas de segurança e nos casos de furtos com recurso a explosivos gasosos dar particular atenção aos modelos DV213/1413 da

marca da De La Rue. Adicionalmente devem ser analisadas os sistemas de segurança instalados, o volume de numerário armazenado.

Torna-se essencial a recolha e o tratamento sistemático de informação, com vista à identificação de padrões e à definição de estratégias preventivas eficazes. Estabelecer o histórico de incidentes e tipos de ataques registados, possibilitará antecipar padrões de atuação e ajustar as respostas preventivas.

A análise realizada revela uma concentração deste tipo de furtos nos distritos do litoral, especialmente Porto, Lisboa, Setúbal e Aveiro com especial incidência nos concelhos de Sintra, Vila do Conde, Almada, Palmela, Paredes e Barcelos. Esta distribuição geográfica reforça a importância da afetação de recursos e medidas preventivas orientadas para os territórios de maior risco.

A maioria dos furtos ocorreram em dias úteis, especialmente à sexta-feira. O período com maior incidência foi durante a noite, sobretudo entre as 02h00 e as 05h00, com especial incidência por volta das 04h00, sendo que em plena luz do dia o número de furtos é muito residual, quase insignificante.

Os locais mais visados foram os ATM instalados em bancos (especialmente no CCA), juntas de freguesia e ATM integrados na parede com acesso direto à via pública. Com menor incidência mais ainda com alguma relevância surgem os Hiper e supermercados e os postos de abastecimento de combustível. Os clubes e associações, localizados em zonas mais isoladas são também suscetíveis deste tipo de ataques.

Tais padrões exigem uma gestão estratégica do patrulhamento, que deve privilegiar os locais e horários mais críticos, com atenção especial às ATM isoladas, em zonas com fraca iluminação, com bons itinerários para a fuga do local, e as que apresentem vulnerabilidades estruturais ou ausência de medidas de dissuasão eficazes, quer no local onde está instalado quer da própria ATM.

É igualmente essencial, dar continuidade à correta elaboração da Ficha de Avaliação de Risco (diferente do perfil de risco individualizado para ATM), que avalia o risco da instalação de determinada ATM com base na caracterização do local de instalação, caracterização das condições de instalação, caracterização das condições para operações de manutenção, avaliação das condições e a probabilidade para realização de atos ilícitos e a tipologia da ATM.

É imperativo reforçar a sensibilização dos militares para a identificação de sinais e comportamentos potencialmente suspeitos, que possam funcionar como precursores da atividade criminosa. Entre os indicadores mais comuns associados aos MO especialmente

dos GCO, destaca-se o furto de viaturas de alta cilindrada, com particular incidência nas marcas BMW e nas pertencentes ao Grupo Volkswagen, nomeadamente Audi e Seat, especialmente as versões carrinhas. Outro sinal de alarme relevante é a existência de ATM fora de serviço, situação que pode indiciar uma tentativa iminente de furto, prática recorrente entre os GCO como forma de maximizar os lucros.

Durante as ações de patrulhamento, os militares devem prestar especial atenção à presença de viaturas de características referidas, especialmente em horários e contextos de maior risco, bem como à movimentação de grupos compostos por dois a quatro indivíduos nas proximidades das ATMs. A posse de ferramentas como rebarbadoras, alicates, serras de corte, chaves de fenda, botijas de gás (acetileno), tubos, baterias e extintores, deve igualmente ser interpretada como um potencial indício da preparação de um furto.

Outro elemento essencial na prevenção é a cooperação interinstitucional, promovendo a articulação entre FS, bancos e outras entidades. A partilha atempada de informação, o cruzamento de dados e a construção de perfis de risco, potenciam uma resposta integrada e eficaz, alinhada com as orientações da REPC em conjunto com a Europol.

Destaca-se ainda o papel da sensibilização da população como ferramenta de reforço da segurança. Os cidadãos devem ser incentivados a comunicar comportamentos suspeitos junto das ATMs. Simultaneamente, é importante que a GNR utilize de forma estratégica os meios de comunicação social, com o intuito de promover uma perceção social de elevado risco para os potenciais infratores. Esta perceção poderá ser incitada através da divulgação de operações policiais que resultaram em detenções e apreensões, contribuindo assim para um efeito dissuasor.

Tal como em qualquer investigação, este estudo apresenta algumas limitações que importa assinalar. A principal prende-se com a indisponibilidade de dados considerados sensíveis. Por motivos de confidencialidade, não foi possível aceder a informação detalhada sobre os modelos de ATM frequentemente mais visados, por parte da SIBS.

Adicionalmente, os dados disponíveis não permitiram analisar os modelos de ATM furtados nem distinguir entre ATMs integrados em estruturas fixas (como paredes) e os instalados de forma autónoma. Esta limitação impossibilitou a análise da relação entre o tipo de instalação e o MO adotado nos furtos, restringindo a capacidade de identificar padrões operacionais e vulnerabilidades específicas.

Face a estas limitações, recomenda-se que futuras investigações aprofundem a perspetiva dos próprios perpetradores, através da realização de entrevistas com indivíduos condenados por este tipo de crime. Esta abordagem qualitativa poderá fornecer informações

cruciais sobre as motivações, os critérios de seleção dos alvos e as percepções sobre os sistemas de segurança, contribuindo para o desenvolvimento de estratégias de prevenção mais ajustadas e eficazes.

REFERÊNCIAS BIBLIOGRÁFICAS E OUTRAS FONTES

- Academia Militar. (2025). Curso de Ciências Militares na especialidade de segurança. <http://academiamilitar.pt/curso-de-ciencias-militares-na-especialidade-de-seguranca.html>
- Allum, F. (2025). Researching organized crime: A novel approach combining inductive and storyline paradigms. *International Journal of Qualitative Methods*, 24, 1–12. <https://doi.org/10.1177/16094069241307588>
- Almeida, F. E. G. e, Logsdon, L., Ceccato, V., Paula, D. C. J. de, Santos, J. M., & Portela, A. (2023). Análise temporal de roubos e furtos a residência em Cuiabá, Brasil. *Revista Brasileira de Segurança Pública*, 17(1), 208–231. <https://doi.org/10.31060/rbsp.2023.v17.n1.1456>
- Alperstedt, G., Hoffmann, M., & Sá, V. (2022). Mecanismos públicos de coordenação e *wicked problems*: estudo de um arranjo interorganizacional voltado ao combate do crime organizado em Santa Catarina. *Revista de Direito da Cidade*, 14(2). <https://doi.org/10.12957/rdc.2022.56064>
- ATMIA. (2014a). *Preventing gas and explosive attacks – Version 2*. ATM Industry Association
- ATMIA. (2014b). *ATM software security best practices guide (Version 3)*. ATM Industry Association
- Berg, B. L. (2001). *Qualitative research methods for the social sciences* (4.^a ed.). Allyn & Bacon.
- Bertaux, D. (1997). *Les récits de vie: Perspective ethnosociologique*. Paris: Nathan.
- Brantingham, P. J., & Brantingham, P. L. (1991). *Environmental criminology* (2.^a ed.). Waveland Press.
- Brantingham, P. J., Brantingham, P. L., & Andresen, M. A. (2017). The geometry of crime and crime pattern theory. *CrimRxiv*. <https://www.crimrxiv.com/pub/b3vnxots>
- Camoleze, C. D. E. (2022). SEVERINO, Antônio Joaquim. *Metodologia do trabalho científico* (23^a ed.). *Revista de Educação da Unina*, 3(3). <https://doi.org/10.51399/reunina.v3i3.177>
- Clark, R. E. (1983). Reconsidering research on learning from media. *Review of Educational Research*, 53(4), 445–459. <http://dx.doi.org/10.3102/00346543053004445>
- Clarke, R. V. (1992). *Situational crime prevention: Successful case studies*. Harrow and Heston.

- Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine
- Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In M. J. Smith & D. B. Cornish (Eds.), *Theory for practice in situational crime prevention (Crime Prevention Studies, Vol. 16*, pp. 111–124). Criminal Justice Press.
- Corrado, R. R., DeLisi, M., & Katz, C. M. (2017). How individual and contextual factors affect antisocial and delinquent behaviors: A comparison between young offenders, adolescents at risk of social exclusion, and a community sample. *Frontiers in Psychology, 8*, 1825. <https://doi.org/10.3389/fpsyg.2017.01825>
- Cozens, P., Saville, G., & Hillier, D. (2005). *Crime prevention through environmental design (CPTED): a review and modern bibliography*. Property Management. 23(5), 328–356. <https://doi.org/10.1108/02637470510631483>
- Crawford, A., & Evans, K. (2012). Crime prevention and community safety. In *The Oxford Handbook of Criminology* (pp. 769–805). <https://doi.org/10.1093/he/9780199590278.003.0026>
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5.^a ed.). Thousand Oaks, CA: SAGE Publications.
- Cunha, M., Rego, A., Cunha, R., Cardoso, C., Marques, C., & Gomes, J. (2012). *Manual de Gestão de Pessoal e do Capital Humano* (2^a ed.). Edições Sílabo.
- Despacho Ministério Público (MP): Procuradoria-Geral da República 06-12-2017. (2017). SIMP
- Elias, L. (2022). Ciências Policiais e Segurança Interna, Desafios e Prospetiva. 2^a Edição revista e atualizada. Lisboa: ISCPSI.
- European Association for Secure Transactions [EAST]. (2023). *ATM physical attacks rise in Europe*. European Association for Secure Transactions. <https://www.association-secure-transactions.eu/atm-physical-attacks-rise-in-europe/>
- European Association for Secure Transactions [EAST]. (2025). *EAST membership*. <https://www.association-secure-transactions.eu/east-membership/>

- European Association for Secure Transactions [EAST]. (2025). *Terminal physical attack definitions & terminology*. <https://www.association-secure-transactions.eu/industry-information/terminal-physical-attack-definitions-terminology/>
- European Association for Secure Transactions [EAST]. (2023). *Terminal physical attack definitions & terminology (ATM & ATS)* (Versão 1.2). <https://www.association-secure-transactions.eu/wp-content/uploads/EAST-Terminal-Physical-Attack-Definitions-Terminology-ATM-ATS.pdf>
- Europol. (2020). *Serious and organised crime threat assessment (SOCTA)*. European Union Agency for Law Enforcement Cooperation.
- Europol. (2021). *Guidance and recommendations regarding logical attacks on ATMs: Mitigating the risk, setting up lines of defence, identifying and responding to logical attacks*. European Cybercrime Centre (EC3)
- Europol. (2025). *About Europol*. <https://www.Europol.europa.eu/about-Europol>
- Felson, M. (1998). *Crime and everyday life* (2.^a ed.). Pine Forge Press.
- Felson, M. (2006). *Crime and nature*. Sage. <https://doi.org/10.4135/9781452204260>
- Fraile, M., Ford, M., Gadyatskaya, O., Kumar, R., Stoelinga, M., & Trujillo-Rasua, R. (2016). Using attack-defense trees to analyze threats and countermeasures in an ATM: A case study. In J. Horkoff et al. (Eds.), *PoEM 2016: Practice of Enterprise Modeling* (pp. 326–334). Springer. https://doi.org/10.1007/978-3-319-48393-1_24
- Guarda Nacional Republicana [GNR] (2011). Norma de Execução Permanente/GNR 2.20, de 12 de dezembro. Lisboa: Comando Operacional
- Guarda Nacional Republicana. (2020a). *Estratégia da GNR 2025*. Lisboa: GNR.
- Haro, F. A., Serafim, J., Cobra, J., Faria, L., Roque, M. I., Ramos, M., Carvalho, P., & Costa, R. (2016). *Investigação em ciências sociais: Guia prático do estudante*. Pactor.
- Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety*, 15(1), 65–79. <https://doi.org/10.1057/cpcs.2012.14>
- Interpol. (2019). *Organised crime: Trends and responses*. International Criminal Police Organization.

- Interpol. (2025). *What is INTERPOL?*. <https://www.interpol.int/Who-we-are/What-is-INTERPOL2>
- Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). *Toward a definition of mixed methods research. Journal of Mixed Methods Research, 1*(2), 112–133. <https://doi.org/10.1177/1558689806298224>
- Kuhn, A., & Agra, C. (2010). *Somos todos criminosos? Pequena introdução à criminologia e ao direito das sanções*. Casa das Letras.
- Lynch, M. J., Stretesky, P. B., & Long, M. A. (2018). Situational crime prevention and the ecological regulation of green crime: A review and discussion. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 178–196. <https://doi.org/10.1177/0002716218789080>
- Muggah, R., & Diniz, G. (2013). Digitally enhanced violence prevention in the Americas. *Stability: International Journal of Security & Development, 2*(3), 57, 1–23. <http://dx.doi.org/10.5334/sta.c>
- Nagin, D. S., & Paternoster, R. (2024). Enduring individual differences and rational choice theories of crime. *Law & Society Review*. <https://doi.org/10.1017/lsr.2024.25>
- NCR Corporation. (2018). *ATM security: Explaining attack vectors, defense strategies and solutions*. NCR Corporation.
- Patton, M. Q. (2002). *Qualitative evaluation and research methods* (3.^a ed.). SAGE Publications.
- PORDATA. (2024). *Caixas automáticas Multibanco*. Fundação Francisco Manuel dos Santos. <https://www.pordata.pt/pt/estatisticas/economia/rendimento-e-poupanca/caixas-automaticas-multibanco>
- Radosteva, Y. V. (2020). To the issue of situational crime prevention. *Atlantis Press*. <https://doi.org/10.2991/assehr.k.200321.088>
- Rebocho, M. (2009). *The hunter and the hunted: A comparative study of the hunting behavior of rapists and child molesters* [Tese de doutoramento, Universidade do Minho]. Universidade do Minho.

- Rede Europeia de Prevenção do Crime & Agência da União Europeia para a Cooperação Policial . (2019). *Prevenção de assaltos físicos nos terminais bancários: Desenvolvimento de uma abordagem eficaz*.
- REPC & Europol. (2019). *Prevenção de assaltos físicos nos terminais bancários: Desenvolvimento de uma abordagem eficaz*. Agência da União Europeia para a Cooperação Policial & Rede Europeia de Prevenção do Crime.
- Rodrigues, C. W. (2007). *Metodologia científica II*. Paracambi.
- Rosado, D. P. (2017). *Elementos essenciais de sociologia geral*. Gradiva.
- Sánchez-Delgado, H. (2024). Explicando la delincuencia en Barcelona: ¿Desorganización social u oportunidades del turismo? *Revista Española de Investigación Criminológica*, 21(1), e861. <https://doi.org/10.46381/reic.v21i1.861>
- Santos, L. A. B. dos, Lima, J. M. M. do V., Garcia, F. M. G. P. P., Monteiro, F. T., Silva, N. M. P. da, Silva, J. C. do V. F., Santos, R. J. R. P. dos, Afonso, C. F. N. L. D., & Piedade, J. C. L. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.^a ed.). Instituto Universitário Militar – Centro de Investigação e Desenvolvimento.
- Scott, M. S. (2006). *Robbery at automated teller machines* (Problem-Specific Guides Series No. 8). U.S. Department of Justice, Office of Community Oriented Policing Services.
- Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating system concepts* (10th ed.). Wiley.
- Silva, T. G. (2023). *Furtos em residências: No submundo do crime* (1.^a ed.). Pactor.
- Skoudis, E., & Zeltser, L. (2021). *Malware: Fighting malicious code*. Addison-Wesley.
- Stallings, W. (2018). *Computer organization and architecture: Designing for performance* (11th ed.). Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson Education.
- Thomas, C., Jeong, J., & Wolff, K. T. (2024). *Testing Routine Activity Theory: Behavioural Pathways Linking Temperature to Crime*. *British Journal of Criminology*. <https://doi.org/10.1093/bjc/azae091>
- Tonry, M., & Farrington, D. P. (1995). *Building a safer society: Strategic approaches to crime prevention* (Vol. 19). University of Chicago Press.

TrendMicro & Europol (2017). *Cashing in on ATM malware: A comprehensive look at various attack types*. Trend Micro Forward-Looking Threat Research (FTR) Team & Europol European Cybercrime Centre (EC3).

Tribunal da Relação do Porto. (2021, 10 de março). *Acórdão n.º 5148/20.2JAPRT-A.PI*. <https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/0f37c2312c5f51f3802586b6005a2f82?OpenDocument>

Valente, M. M. G. (2022). O hexágono da prevenção criminal - A recolocação das medidas de polícia numa possível reconstrução das fronteiras da prevenção e repressão criminal. In I Congresso Internacional JusCrim: Prevenção, policiamento e segurança — Implicações nos direitos humanos (p. 91). Atlas.

Vilelas, J. (2020). *Investigação: O processo de construção do conhecimento* (3ª ed.). Edições Sílabo.

Wyatt, T., van Uhm, D., & Nurse, A. (2020). Differentiating criminal networks in the illegal wildlife trade: Organized, corporate and disorganized crime. *Trends in Organized Crime*, 23(4), 350–366. <https://doi.org/10.1007/s12117-020-09385-9>

Legislação:

Assembleia da República. (1995). *Decreto-Lei n.º 48/95, de 15 de março*. Diário da República, 1.ª série-A, n.º 63.

Assembleia da República. (2007). *Lei n.º 63/2007, de 6 de novembro*. Diário da República, 1.ª série, n.º 213.

Assembleia da República. (2009). *Lei n.º 5/2009, de 29 de janeiro*. Diário da República, 1.ª série, n.º 20, p. 602. Assembleia da República. (2021). *Lei n.º 79/2021, de 24 de novembro*. Diário da República, 1.ª série, n.º 228, 9–38.

Assembleia da República. (2013). *Lei n.º 34/2013, de 16 de maio*. Diário da República, 1.ª série, n.º 94.

Assembleia da República. (2013). *Lei n.º 34/2013, de 16 de maio*. Diário da República, 1.ª série, n.º 94.

Assembleia da República. (2019). *Lei n.º 46/2019, de 8 de julho*. Diário da República, 1.ª série, n.º 128.

Assembleia da República. (2023). *Decreto-Lei n.º 41/2023, de 2 de junho*. Diário da República, 1.ª série, n.º 107, pp. 20–106.

Conselho da União Europeia. (2008). *Decisão-Quadro 2008/841/JAI do Conselho relativa à luta contra a criminalidade organizada*. Jornal Oficial da União Europeia, L 300, 42–45. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008F0841>

Conselho da União Europeia. (2009). *Decisão 2009/902/JAI do Conselho, de 30 de novembro de 2009, que cria uma Rede Europeia de Prevenção da Criminalidade (REPC) e revoga a Decisão 2001/427/JAI*. Jornal Oficial da União Europeia, L 321, 44–46.

Ministério da Administração Interna. (2013). *Portaria n.º 273/2013, de 20 de agosto*. Diário da República, 1.ª série, n.º 159.

Ministério da Administração Interna. (2015). *Portaria n.º 106/2015, de 13 de abril*. Diário da República, 1.ª série, n.º 71.

Ministério da Administração Interna. (2020). *Portaria n.º 292/2020, de 18 de dezembro*. Diário da República, 1.ª série, n.º 245, pp. 23–113.

Organização das Nações Unidas. (2000). *Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional*.

Presidência da República. (2004). *Decreto do Presidente da República n.º 19/2004, de 2 de abril*. Diário da República, 1.ª série-A, n.º 79, p. 2080.

Relatórios:

Europol (2017). Serious and Organised Crime Threat Assessment (SOCTA). Europol

Europol (2021). Serious and Organised Crime Threat Assessment (SOCTA). Europol

Europol (2025). Serious and Organised Crime Threat Assessment (SOCTA). Europol

Guarda Nacional Republicana (2013). Relatório de Atividades 2012. Lisboa: GNR

Guarda Nacional Republicana (2014). Relatório de Atividades 2013. Lisboa: GNR

Guarda Nacional Republicana (2015). Relatório de Atividades 2014. Lisboa: GNR

Guarda Nacional Republicana (2016). Relatório de Atividades 2015. Lisboa: GNR

Guarda Nacional Republicana (2017). Relatório de Atividades 2016. Lisboa: GNR

Guarda Nacional Republicana (2018). Relatório de Atividades 2017. Lisboa: GNR

Guarda Nacional Republicana (2019). Relatório de Atividades 2018. Lisboa: GNR

Guarda Nacional Republicana (2020b). Relatório de Atividades 2019. Lisboa: GNR

Guarda Nacional Republicana (2021). Relatório de Atividades 2020. Lisboa: GNR

Guarda Nacional Republicana (2022). Relatório de Atividades 2021. Lisboa: GNR

Guarda Nacional Republicana (2023). Relatório de Atividades 2022. Lisboa: GNR

Sistema de Segurança Interna (2013). Relatório Anual de Segurança Interna - Ano 2012. Lisboa: SSI.

Sistema de Segurança Interna (2018). Relatório Anual de Segurança Interna - Ano 2017. Lisboa: SSI.

Sistema de Segurança Interna (2019). Relatório Anual de Segurança Interna - Ano 2018. Lisboa: SSI.

Sistema de Segurança Interna (2020). Relatório Anual de Segurança Interna - Ano 2019. Lisboa: SSI.

Sistema de Segurança Interna (2021). Relatório Anual de Segurança Interna - Ano 2020. Lisboa: SSI.

Sistema de Segurança Interna (2022). Relatório Anual de Segurança Interna - Ano 2021. Lisboa: SSI.

Sistema de Segurança Interna (2023). Relatório Anual de Segurança Interna - Ano 2022. Lisboa: SSI.

APÊNDICES

APÊNDICE A – TABELA ANÁLISE DOS DADOS QUANTITATIVOS

Ano	2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023 e 2024
Mês	Janeiro, fevereiro, março, abril, maio, junho, julho, agosto, setembro, outubro, novembro e dezembro.
Dias da Semana	Segunda-feira, Terça-feira, Quarta-feira, Quinta-feira, Sexta-feira, Sábado e Domingo
Hora	00h, 01h, 02h, 03h, 04h, 05h, 06h, 07h, 08h, 09h, 10h, 11h, 12h, 13h, 14h, 15h, 16h, 17h, 18h, 19h, 20h, 21h, 22h e 23h.
Distritos	Aveiro, Beja, Braga, Bragança, Castelo Branco, Coimbra, Évora, Faro, Guarda, Leiria, Lisboa, Portalegre, Porto, Santarém, Setúbal, Viana do Castelo, Vila Real e Viseu.
Concelhos	Santa Maria Da Feira, Oliveira De Azeméis, Águeda, Ílhavo, Albergaria-A-Velha, Aveiro, Santa Maria De Lamas, Castelo De Paiva, Espinho, Mealhada, Ovar, Vale De Cambra, Aljustrel, Beja, Barcelos, Guimarães, Vila Nova De Famalicão, Braga, Esposende, Amares, Macedo De Cavaleiros, Castelo Branco, Covilhã, Sertã, Coimbra, Condeixa-A-Nova, Figueira Da Foz, Cantanhede, Lousã, Miranda Do Corvo, Montemor-O-Velho, Oliveira Do Hospital, Penacova, Tábua, Vila Nova De Poiares, Albufeira, Aljezur, Loulé, Faro, Lagos, Silves, Guarda, Vila Real De Santo António, Alcobaça, Porto De Mós, Caldas Da Rainha, Leiria, Peniche, Alvaiázere, Ansião, Pombal, Óbidos, Batalha, Bombarral, Marinha Grande, Sintra, Azambuja, Vila Franca De Xira, Alenquer, Loures, Lourinhã, Torres Vedras, Mafra, Arruda Dos Vinhos, Cadaval, Cascais, Campo Maior, Alter Do Chão, Elvas, Fronteira, Nisa, Ponte De Sor, Vila Do Conde, Paredes, Vila Nova De Gaia, Gondomar, Penafiel, Santo Tirso, Amarante, Maia, Baião, Felgueiras, Lousada, Matosinhos, Mindelo, Paços De Ferreira, Póvoa Do Varzim, Trofa, Abrantes, Cartaxo, Rio Maior, Torres Novas, Chamusca, Ferreira Do Zêzere, Samora Correia, Santarém, Almada, Palmela, Alcochete, Moita, Sesimbra, Santiago Do Cacém, Setúbal, Alcácer Do Sal, Seixal, Caminha, Melgaço, Vila Nova Da Cerveira, Viseu, Carregal Do Sal, Mortágua, Nelas, Tondela, Évora, Montemor-O-Novo, Mourão, Reguengos De Monsaraz, Vila Viçosa.
Tipo de ATM	Antiga dependência bancária, Banco, Banco (Montepio), Banco (BCP), Banco (BIC), Banco (BPI), Banco (CCA), Banco (CGD), Banco (Millennium BCP), Banco (Novo Banco), Banco (Popular), Banco (Santander Totta), Clubes e Associações, Correios (CTT), Edifício de empresa, Edifício Habitacional, Edifício Público, Edifício Municipal, Estabelecimento de ensino, Instalações Desportivas, Estabelecimento Comercial, Estação CP, Hiper/Super/Minimercado, Hotel, Alojamento, Junta de Freguesia, Lar, Mural via pública, Outros, Posto Abastecimento de Combustível, Restaurante, Snack-Bar, Pastelaria, Edifício de Escritórios, Estabelecimento de Saúde, Papelaria, Posto de Turismo.
<i>Modus Operandi</i> (Ataques físicos)	Ataques explosivos (X1 – Explosivos gasosos e X2 – Explosivos Sólidos), Furtos do ATM – arrancamento, (Furtos do ATM – no local: B1 – Corte com Maçarico, B2 – Perfuração, B3 – Corte, B4 – Arrombamento), Ataques não específicos
<i>Modus Operandi</i> (Ataques lógicos)	Black Box e Jackpotting
Sistemas de Videovigilância	Sim, Não e Desconhecido
Nº de suspeitos	1, 2, 3, 4, 5 e desconhecido
Veículo de Fuga	BMW, Audi, SEAT, Renault, Peugeot, Honda, Smart, Volkswagen, Mercedes, Opel, Porsche, Nissan e Fiat.

APÊNDICE B – GUIÃO DE ENTREVISTA

Guião de Entrevista



**ACADEMIA MILITAR
DIRECÇÃO DE ENSINO**

Mestrado Integrado em Ciências Militares, na Especialidade de Segurança (GNR)

TRABALHO DE INVESTIGAÇÃO APLICADA

**Prevenção Criminal: Estudo de caso a furtos a terminais de
multibanco**

AUTOR: Aspirante GNR INFANTARIA Licínio André Capela do Rêgo

ORIENTADOR: Major de Infantaria Doutorada da GNR Adriana Filipa Martins Gameiro

Lisboa, 02 de abril de 2024

CARTA DE APRESENTAÇÃO

O presente inquérito por entrevista surge no âmbito da realização do Trabalho de Investigação Aplicada (TIA) inerente à frequência do Mestrado Integrado em Ciências Militares – Segurança, ministrado na Academia Militar. O TIA subordinado ao tema ***“Prevenção Criminal: Estudo de caso a furtos a terminais de multibanco”*** tem como principal finalidade compreender e analisar este fenómeno, com vista à definição de estratégias de prevenção mais eficazes, ajustadas à realidade operacional da GNR e às especificidades onde estes crimes ocorrem com maior incidência.

Nesse sentido, com o propósito de obter informações relevantes e válidas relativamente às matérias supracitadas, solicito a Vossa Excelência que me conceda uma entrevista sobre o tema em apreço, considerando que o seu contributo é fundamental para atingir os objetivos propostos para a presente investigação.

Grato desde já pela sua disponibilidade e atenção.

Atenciosamente,

Licínio André Capela do Rêgo
Aspirante de Infantaria da Guarda Nacional Republicana

PROTOCOLO DE CONSENTIMENTO INFORMADO

O presente protocolo é estabelecido entre Licínio André Capela do Rêgo, aluno da AM a realizar a investigação com o tema: Prevenção Criminal: Estudo de caso a furtos a terminais multibanco, e o participante:

_____,
através do método de inquérito por entrevista.

O investigador e o orientador científico comprometem-se a:

- a) Conduzir a investigação de acordo com os parâmetros de qualidade preconizados pela comunidade científica da especialidade;
- b) Discutir e negociar outros aspetos específicos de cada caso relativos à confidencialidade da informação, se solicitado pelo participante;
- c) Impedir qualquer divulgação de informação referente aos participantes, exteriormente à equipa de investigação, sem o consentimento prévio de todos os envolvidos;
- d) Entregar uma síntese descritiva dos resultados aos participantes, através de correio eletrónico;
- e) Manter os participantes a par do trabalho que está a ser desenvolvido, nomeadamente no que concerne à análise dos dados, sempre que os mesmos o solicitem;
- f) Prestar aos participantes no processo todos os esclarecimentos solicitados no decorrer da investigação;
- g) Cumprir o Código Deontológico da *American Psychological Association* (APA 7ª Edição) na realização da investigação;
- h) Eliminar todas as gravações áudio após o decorrer da investigação e a defesa pública da tese.

Os participantes comprometem-se a:

- a) Prestar informações sobre a sua experiência no caso em estudo e sobre a sua experiência profissional;
- b) Ser entrevistado num momento acordado entre o investigador e o participante;
- c) Autorizar a gravação áudio da entrevista, a pedido do investigador;
- d) Decidir mencionar ou omitir a sua participação no projeto nos contextos profissionais em que considere conveniente fazê-lo;
- e) Permitir a publicação do resultado do estudo, com omissão da sua identidade, nomeadamente nas seguintes situações:
 - I. Tese de Mestrado a apresentar à Academia Militar;
 - II. Comunicações em congressos científicos-profissionais;
 - III. Publicações científicas em revistas e/ou em livros da especialidade.

Assinaturas:

—

(Participante)

(Investigador)

Local e Data:

IDENTIFICAÇÃO DO ENTREVISTADO

Nome:	Hora (Início/Fim):
U/E/O:	Data:
Função/Posto:	Local:

ENTREVISTA

As respostas de Sua Excelência são fundamentais para atingir os objetivos da investigação, pelo que se solicita que as mesmas sejam o mais completas possível. As suas respostas irão servir única e exclusivamente como objeto de estudo para a investigação, pelo que lhe é solicitada autorização para efetuar gravação e posterior análise e transcrição das respostas. Se for sua intenção, as mesmas ser-lhe-ão facultadas, juntamente com o trabalho final, assim que o mesmo seja aprovado.

Indicadores de Alerta	1. Na prevenção de furtos de/a ATM que indicadores de alerta identifica como relevantes?
	2. De que forma o carregamento da ATM influencia o planeamento deste tipo de ataques?
Características do local	3. Que fatores do local onde a ATM está instalada podem influenciar a decisão em praticar furtos de/a ATM?
Características da ATM	4. Com base nos <i>Modi Operandi</i> registados em Portugal, nos últimos anos, quais são as características do ATM que poderão ampliar a vulnerabilidade desta infraestrutura à prática de furtos?
Prevenção Criminal	5. Como pode a GNR prevenir a prática de crimes de furto de/a ATM?

Obrigado pela disponibilidade e colaboração.

Licínio Rêgo

Aspirante de Infantaria da GNR

APÊNDICE C - CARACTERIZAÇÃO DOS ENTREVISTADOS

Função	Unidade / Órgão	Formato	Data
Chefe da Secção de Informações e Investigação Criminal	Comando Territorial de Lisboa	Presencial	12/04/2025
Chefe da Secção de Informações e Investigação Criminal	Comando Territorial de Porto	Escrita	10/04/2025
Chefe da Secção de Informações e Investigação Criminal	Comando Territorial de Setúbal	Microsoft Teams	11/04/2025
Chefe da Secção de Investigação Criminal	Grupo de Intervenção de Operações Especiais (GIOE) da GNR	Presencial	10/04/2025
Chefe da Repartição de Análise de Informação Criminal	Direção de Investigação Criminal (DIC) da GNR	Escrita	15/04/2025
Chefe da Seção de Análise de Informação Criminal	Direção de Investigação Criminal (DIC) da GNR	Presencial	02/05/2025
Chefe de Divisão	Direção de Informações (DI) da GNR	Escrita	01/05/2025
Comandante Distrital de Setúbal	Comando Distrital de Setúbal da PSP	Presencial	24/04/2025
Coordenador da 2ª Secção Regional do Combate da Banditismo	Unidade Nacional Contraterrorismo (UNCT) da PJ	Presencial	08/04/2025

APÊNDICE D - CODIFICAÇÃO DAS ENTREVISTAS

Categoria	Bloco	Questão da Entrevista	Subcategoria	Sub-Subcategoria	Código
Indicadores de alerta	A	1.Na prevenção de furtos de/a ATM que indicadores de alerta identifica como relevantes?	Avárias na ATM		A.1
			Viaturas	Alta cilindrada	A.2.1
				Carrinhas	A.2.2
			Marcas de automóveis	BMW	A.3.1
				Audi	A.3.2
				Grupo Volkswagen	A.3.3
				SEAT	A.3.4
			Outros crimes associados	Furto de veículos	A.4.1
				Furtos de botijas de gás (acetileno)	A.4.2
				Furto de Extintores	A.4.3
		2.De que forma o carregamento da ATM influencia o planeamento deste tipo de ataques?	Carregamento do ATM	Tem influência no planeamento	A.5.1
				Depende	A.5.2
				Não influencia o planeamento	A.5.3
Características do local	B	3.Que fatores do local onde a ATM está instalada podem influenciar a decisão em praticar furtos de/a ATM?	Iluminação	-	B.1.1
			Fragilidade do local	-	B.1.2
			Isolamento geográfico	-	B.1.3
			Pontos de fuga	-	B.1.4
Características da ATM	C	4.Com base nos <i>Modi Operandi</i> registados em Portugal, nos últimos anos, quais são as características da ATM que poderão ampliar a vulnerabilidade desta infraestrutura à prática de furtos?	Entidade gestora	-	C.1
			Sistemas de Segurança	-	C.2
			Modelo	Tem influência na seleção dos alvos	C.3.1
				Não tem influência na seleção dos alvos	C.3.2
Prevenção	D	5.Como pode a GNR prevenir a prática de crimes de furto de/a ATM?	Sensibilizar a população	-	D.1
			Ficha de avaliação do risco	-	D.2
			Recolha e tratamento de informação	-	D.3
			Cooperação	-	D.4
			Patrulhamento	Locais de risco	D.5.1
				Comportamentos suspeitos	D.5.2

APÊNDICE E - NÚMERO DE FURTOS POR DISTRITO E ANO (PORTUGAL CONTINENTAL)

Aveiro	Ílhavo	5
	Oliveira De Azeméis, Águeda	4
	Albergaria-A-Velha, Aveiro e Santa Maria De Lamas	2
	Castelo De Paiva, Espinho, Mealhada, Ovar e Vale De Cambra	1
Beja	Aljustrel e Beja	1
Braga	Barcelos	6
	Guimarães e Vila Nova De Famalicão	3
	Braga e Esposende	2
	Amares	1
Bragança	Macedo De Cavaleiros	1
Castelo Branco	Castelo Branco	3
	Covilhã e Sertã	1
Coimbra	Coimbra, Condeixa-A-Nova e Figueira Da Foz	3
	Cantanhede	2
	Lousã, Miranda Do Corvo, Montemor-O-Velho, Oliveira Do Hospital, Penacova, Tábua e Vila Nova De Poiares	1
Faro	Albufeira	5
	Aljezur e Loulé	2
	Faro, Lagos, Vila Real de Santo António e Silves	1
Guarda	Guarda	1
Leiria	Alcobaça e Porto de Mós	4
	Caldas Da Rainha, Leiria e Peniche	3
	Alvaiázere, Ansião, Pombal e Óbidos	2
	Batalha, Bombarral e Marinha Grande	1
Lisboa	Sintra	15
	Azambuja e Vila Franca De Xira	5
	Alenquer, Loures, Lourinhã, Torres Vedras	3
	Mafra	2
	Arruda Dos Vinhos, Cadaval e Cascais	1
Portalegre	Campo Maior	2
	Alter Do Chão, Elvas, Fronteira, Nisa e Ponte De Sor	1
Porto	Vila Do Conde	11
	Paredes	6
	Vila Nova De Gaia	5
	Gondomar, Penafiel e Santo Tirso	3
	Amarante e Maia	2
	Baião, Felgueiras, Lousada, Matosinhos, Mindelo, Paços De Ferreira, Póvoa Do Varzim e Trofa	1
Santarém	Abrantes, Cartaxo, Rio Maior e Torres Novas	2
	Chamusca, Ferreira Do Zêzere, Samora Correia e Santarém	1
Setúbal	Almada	7
	Palmela	6
	Alcochete	4
	Moita e Sesimbra	3
	Alcácer Do Sal, Santiago Do Cacém e Setúbal	2
	Seixal	1
Viana Do Castelo	Caminha e Melgaço	1
	Vila Nova Da Cerveira	1
Viseu	Viseu	2
	Carregal Do Sal, Mortágua, Nelas, Tondela e Nelas	1
Évora	Évora	2
	Montemor-O-Novo, Mourão, Reguengos De Monsaraz e Vila Viçosa	1

APÊNDICE F- NÚMERO DE FURTOS POR DISTRITO E ANO (PORTUGAL CONTINENTAL)

1. Na prevenção de furtos de/a ATM que indicadores de alerta identifica como relevantes?	
E1	(...) poderemos levar em consideração os comportamentos atípicos nas proximidades dos locais onde as ATM se encontram instaladas (pessoas/viaturas) (...) Identificação de objetos ou dispositivos estranhos colocados na ATM; sinais de tentativa de arrombamento; danos nos sistemas de CCTV do local; avarias recorrentes ou interrupção das comunicações da ATM; histórico de furtos anteriores; entre outros.
E2	(...) veículos suspeitos nas imediações, particularmente em horários atípicos, como durante a madrugada ou fins de semana, (...) viaturas, geralmente de grande cilindrada, podem apresentar matrículas adulteradas (Falsas) ou ocultadas, e são frequentemente associadas a outros crimes, como furtos de veículo (...) atuação de indivíduos em comportamento de vigilância ou reconhecimento prévio. Normalmente, os assaltantes visitam o local com dias ou semanas de antecedência para analisar os horários de menor movimento, os trajetos de fuga e o tempo médio de resposta das forças de segurança. A presença repetida e não justificada de pessoas nas proximidades de ATM deve ser considerada suspeita, especialmente em áreas remotas e pouco populosas. A ocorrência de crimes associados (...) furtos de veículos de um determinado grupo automóvel, ocorrem frequentemente dias ou até semanas antes do ataque. Adicionalmente, pode ocorrer sabotagens ao sistema de videovigilância e/ou sistema de iluminação nas imediações (...)
E3	(...) primeiro ataque identificar o Modus Operandi utilizado (tipo de ferramentas utilizadas) (...) e dessa forma aumentar a troca de informação criminal entre os diversos OPC, e ajustar o patrulhamento com divulgação da informação relativo ao Modus Operandi ao dispositivo, para que quando abordam uma caixa ATM possam identificar o tipo de ataque (...)
E4	(...) furto de viaturas ligeiras na sua maioria carrinhas, preferencialmente do Grupo VW e BMW (...) Furtos a oficinas com subtração de botijas de hidrocarboneto da classe dos alcinos (...)
E5	(...) Sucessivas avarias: pode estar a ser alvo de intervenção e alteração do layout e estrutura (...)
E6	(...) fatores ambientais ou geográficos são os mais relevantes, concretamente o local físico onde o ATM está instalado e maior ou menor isolamento da zona. (...) instalado num Posto de Abastecimento de Combustível numa estrada mais isolada, e que não funciona 24h, se existe CCTV no local, se a iluminação pública é boa, se está localizado numa zona de baixa presença policial ou baixa circulação noturna, se o edifício onde está inserido o ATM é robusto ou não, se tem alarme, a distância ao Posto Policial mais próximo, se a localização do ATM se insere numa zona fronteira entre Pter/Dter ou com a PSP, entre outros aspetos (...) ser tido em consideração a própria construção do local onde o ATM está e a sua conceção, nomeadamente se o ATM está ancorado ao solo, se está protegido por barreiras ou quaisquer outros mecanismos de aceleração negativa para viaturas, se possível o estacionamento de viaturas junto à ATM (...).
E7	(...) Furtos de garrafas de gás acetileno e oxigénio, normalmente ocorridos em serralharias, empresas metalúrgicas ou em depósitos de fornecedores. Furtos de extintores, que também são um sinal associado. (...) Furtos de automóveis, especialmente veículos de gama alta e, preferencialmente, modelos tipo tourer (carrinhas), como Volkswagen Passat, Audi A4 e A6, BMW, sobretudo 520. Estes veículos são usados para o transporte dos equipamentos ou para facilitar a fuga. (...) estado operacional das máquinas: Máquinas fora de serviço ou colocadas fora de serviço intencionalmente (...). A máquina é reparada e volta a ser carregada. Muitas vezes, introduzem um pauzinho, um palito, ou outros objetos pequenos que bloqueiam algum mecanismo interno da máquina.
E8	(...) os furtos de bilhas de gás, sim (...) o furto de extintores, sim, que é a sua utilização para encobrir fugas no caso de perseguição policial, e os roubos, sobretudo de viaturas de alta cilindrada, porque é aquela preocupação que ele tem para depois fazer uma fuga rápida (...)
E9	(...) Localizações mais isoladas, essencialmente fora de instituições bancárias farão dessa ATM um maior alvo potencial (...) Presença de dispositivos estranhos (...) Movimentação suspeita: Indivíduos permanecendo próximo ao ATM por longos períodos sem realizar transações ou demonstrando comportamento de vigilância (...)

2. De que forma o carregamento do ATM influencia o planeamento deste tipo de ataques?	
E1	os furtos levados a efeito por grupos organizados são meticulosamente planeados, sendo o estudo dos horários/datas de carregamento uma das suas prioridades, uma vez que os proventos da execução efetiva do furto serão amplamente influenciados se o mesmo ocorrer após o carregamento da ATM.
E2	(...) carregamento de um ATM constitui um dos aspetos mais críticos no planeamento de furtos. Os autores de crimes estão cientes de que, após o reabastecimento, os terminais atingem o seu ponto máximo de liquidez, o que se traduz num aumento significativo do retorno financeiro de um eventual ataque. Por conseguinte, diversos grupos monitorizam os horários e frequências de carregamento com antecedência (...) sugere que os atacantes obtiveram informações prévias ou monitorizaram diretamente o processo de carregamento, enfatizando a importância da confidencialidade e de medidas dissuasivas.
E3	O dia do carregamento não é tão influenciador do ataque ao ATM (...)
E4	(...) os suspeitos, e de acordo com o nível de organização destes, levam-nos a acreditar que recolhem esse tipo de informação de modo privilegiado (...)
E5	(...) É o momento de maior fragilidade e também de maior proveito do valor a furtar. (...)
E6	(...) quem pretende perpetrar um ilícito deste âmbito (...) efetua um estudo prévio e reconhecimento do local e destas rotinas, e saberá quando é que o mesmo está carregado, muitas vezes por via de informadores ou ex-funcionários para saber os dias/horas de abastecimento (...) O carregamento do ATM é um dos fatores mais críticos no planeamento de furtos e outro tipo de ataques e influencia diretamente a motivação, oportunidade e modus operandi dos criminosos (...)
E7	(...) caixas de crédito agrícola (...) são os próprios funcionários que fazem o carregamento. Quando? Ou de manhã, quando chegam e percebem que a máquina precisa de dinheiro, ou ao fim do dia, para garantir que, durante a noite, há capital disponível. O que é que isso provoca? Se repararem, tem havido muitos assaltos a bancos CCA à hora do fecho, precisamente quando os funcionários estão a carregar a máquina. Isto significa que eles sabem que essas máquinas, apesar de terem menos dinheiro, têm sempre algum dinheiro disponível (...)
E8	(...) depende do investimento que fez, depende dos custos que tens, do risco que corre (...) Há muitas situações em que se faz reconhecimento para ver quando é que os ATMs são carregados ou não, isso, normalmente, é demasiado investido e risco. Ter alguém a fazer vigilância a um ATM durante o dia, para tentar perceber quando é que ele é carregado ou não, é um custo elevado, em termos de horas de trabalho. Agora, também não podemos descartar outros cenários, de poder haver algum tipo de informação de “baixos custos”. Ou seja, alguém que tenha essa informação, que trabalhe nesse serviço, e que possa dar essa dica. Ou seja, alguém que mora ou que trabalhe perto do sítio onde está o ATM e que possa dar esse tipo de informação. (...)
E9	(...) Se o carregamento ocorrer em horários fixos, os criminosos podem planejar ataques com base nesses momentos, aproveitando a movimentação de dinheiro (...) ATMs recém-carregados têm maior quantidade de dinheiro disponível, tomando-os alvos mais atrativos.

3. Que fatores do local onde o ATM está instalado podem influenciar a decisão em praticar furtos de/a ATM?	
E1	Os fatores são diversos, e devem ser levados em consideração na avaliação de risco efetuada para efeitos de instalação de novos ATM, nomeadamente as características do local, a iluminação, o acesso direto através da via pública, os fluxos de circulação de pessoas e veículos, a existência de circuitos de CCTV, entre outros.
E2	A localização do ATM constitui um dos fatores mais relevantes na decisão de um indivíduo com propósitos criminosos. Os ATM localizados em áreas rurais ou com baixa densidade populacional apresentam um risco acrescido, dada a reduzida presença de testemunhas e a potencial demora na resposta das forças de segurança. Estes locais frequentemente apresentam uma vigilância reduzida, tanto em termos de presença humana como de sistemas eletrónicos de vigilância. A facilidade de fuga após a prática de um crime constitui outro aspeto importante. A proximidade a vias rápidas, como autoestradas ou estradas nacionais, permite aos autores de crimes deslocarem-se para outros locais em poucos

	minutos, antes da chegada das patrulhas da GNR. A existência de vias secundárias e caminhos rurais com falta de iluminação facilita igualmente a ocultação da viatura e a evasão dos suspeitos. A infraestrutura que acolhe o ATM também influencia a sua vulnerabilidade. Por exemplo, ATMs colocados em postos de combustível, centros comerciais com horário limitado ou em estruturas independentes (sem ligação direta a um edifício sólido) são mais fáceis de remover ou destruir. A solidez do edifício e os materiais utilizados na sua construção determinam o tempo necessário para arrombar ou remover a máquina. A luminosidade e a presença de videovigilância são igualmente fatores a ter em conta. A falta de iluminação ou a inoperacionalidade das câmaras de vigilância, bem como a sua má qualidade, contribuem para um ambiente favorável à prática de atividades delituosas. A ausência de iluminação pública e de sistemas de alarme visíveis é uma constante em locais onde os ataques são mais bem-sucedidos.
E3	(...) procuram caixas ATM isoladas ou com uma estrutura simples (juntas de freguesia ou associações culturais) de fácil acesso onde o nível de equipamentos de alerta (CCTV e Alarmes e diminuto ou inexistente, o ideal para os autores é o modelo de ATM associado a uma localização isolada. Os Autores procedem à recolha prévia de informação dos locais alvo (aquando da utilização do método por explosão, escolhem as caixas ATM situadas em locais onde exista contigüamente, janelas, portas ou separadores de vidro que quebrem com a explosão, porquanto tal lhes facilitar o acesso às gavetas do dinheiro pela retaguarda do multibanco), bem como os itinerários de acesso e fuga; Efetuam furto de veículos, sobretudo de gama alta (Audi, BMW, Mercedes e Seat) e utilizam estes veículos para realizarem o ilícito (com espaço temporal de várias semanas ou meses entre o furto do veículo e o de ATM, ou em alguns casos, no próprio dia/noite);
E4	(...) escolha dos suspeitos se direcionou a localizações maioritariamente em zonas discretas, pouco iluminadas, mas próximas de boas zonas de acesso (fuga) (...) edifícios que permitissem acesso mais facilitado do ponto de vista da engenharia. Acresce referir que em relação a estabelecimentos bancários, direcionaram a sua escolha, maioritariamente à Caixa de Crédito Agrícola.
E5	Fraca videovigilância, local ermo e de fácil escapatória, bem como material fraco ou de fácil arrombamento, onde o ATM está instalado. (...)
E6	(...) isolamento e a diminuta visibilidade do local, que potencia estes ilícitos, a instalação do ATM em zonas industriais, parques de estacionamento, zonas rurais ou lojas encerradas fora de horas são especialmente atrativos, a iluminação pública deficiente ou inexistente, a não existência de CCTV ou alarme no edifício onde o ATM está instalado, o local permitir o acesso, até ao ATM, por parte de viaturas e estar próximo de grandes eixos rodoviários e/ou múltiplas vias de fuga e a própria conceção física do imóvel onde o ATM está instalado, se, por exemplo, se a fachada é frágil, e se não tem elementos de proteção passiva, como pilares, grades, muros ou reforços estruturais.
E7	(...) as juntas de freguesia são um alvo frequente. (...) a máquina serve uma freguesia inteira e está instalada num pequeno anexo à junta de freguesia, num pequeno barraco, com entrada por trás, o que facilita o furto. A máquina é colocada num pequeno anexo improvisado (...) Além disso, também são comuns os ataques a recintos desportivos. Normalmente, estes espaços ficam ligeiramente fora dos centros urbanos e têm uma máquina mais isolada, sem grande vigilância. Outros locais muito apetecíveis são antigos balcões desativados e ATM instalados em paredes de vidro, em imobiliárias, agências de seguros, super e mini-mercados e, até, cabeleireiros. Normalmente, estes locais são escolhidos porque, durante a noite, têm pouca vigilância. Estão afastados dos postos da polícia, da GNR, ou das esquadras da PSP, e são, portanto, alvos fáceis.
E8	(...) um local mais isolado, menos policiado, menos iluminado (...) locais que tenham boas vias de fuga (...) também temos a questão da frequência dos carregamentos e o volume dos carregamentos, que será diferente. A frequência e o volume de carregamento, por exemplo, nas juntas de freguesia ao longo de zonas como o Algueirão-Mem Martins ou o Margem do Bispo, são, com certeza, bem menores do que num ATM na Alta de Lisboa ou em zonas mais centrais de Lisboa, onde há muito mais movimento. Portanto, nesses locais, terá montantes maiores, a frequência de carregamento será maior, e a probabilidade de apanhar o ATM quase vazio é mais baixa. Apesar do risco ser mais elevado, face à possibilidade de retorno, aí entram as vias de fuga como fator decisivo.
E9	ATMs situados em locais pouco iluminados, isolados ou com baixa circulação de pessoas são mais propensos a serem alvo de furtos, devido à menor probabilidade de testemunhas (...) Áreas de fácil acesso e fuga, como perto de estradas ou locais com pouca vigilância, oferecem maior conveniência para criminosos.

4. Com base nos modi operandi registados em Portugal, nos últimos anos, quais são as características do ATM que poderão ampliar a vulnerabilidade desta infraestrutura à prática de furtos?	
E1	(...) as ATM mais vulneráveis serão as que não dispõem de mecanismos de segurança mais avançados, nomeadamente no que concerne às características da estrutura da máquina e, em especial, aos sistemas de tintagem de notas.
E2	O tipo de ATM constitui uma variável determinante. Máquinas de modelo mais antigo, desprovidas de reforços estruturais e de sistemas de alarme integrados, apresentam uma maior facilidade de violação. Adicionalmente, os ATM independentes, localizados fora das agências bancárias e não integrados em infraestruturas seguras, como caixas muradas ou com portas reforçadas, apresentam um nível de vulnerabilidade acrescido. A marca e o modelo do equipamento também influenciam o grau de segurança. Alguns modelos mais recentes estão equipados com mecanismos de autodefesa, como sistemas de tinta indelével que mancham as notas em caso de arrombamento ou sensores de vibração que alertam para tentativas de ataque. Porém, é importante notar que os modelos mais antigos podem não dispor de tais proteções, tornando-se assim alvos preferenciais para ações delituosas (...) Equipamentos com versões desatualizadas ou com falhas técnicas tomam-se inevitavelmente mais suscetíveis (...)
E3	(...) Tendo em conta as situações registadas anteriormente, não é excluída a probabilidade de todas as máquinas ATM serem vulneráveis a este tipo de MO, no entanto, os modelos mais atacados através do método de "Explosão", em território nacional tem sido a máquina de modelo "DeLaRue DV1413", esta é mais "pretensa" ao furto, pois o rebentamento leva à imediata queda da caixa forte (onde se encontra acessível o dinheiro), levando a um menor tempo na concretização do furto (+/- 2 min.).
E4	(...) A escolha incidiu sobretudo nas Máquinas ATM da marca - De la Rua 14-13. (...)
E5	Estar embutida em paredes de madeira ou vidro junto à via pública (montanha de lojas, por exemplo), bem como em locais de fácil acesso, junto a uma simples porta, facilmente pode ser carregada, arrebatada ou estroncada
E6	(...) tratar de um modelo mais antigo, e como tal com menos características de segurança, com o invólucro e gaveta das notas facilmente violável, e que permitirá introdução de objetos (...) ou injeção de gás.
E7	(...) ataques físicos através de corte, temos duas situações. Por norma, máquinas portáteis. As máquinas portáteis são alvo, muitas vezes, de furto com máquinas de corte, com rebarbador (...) em arrombamento já com recurso a maçarico, um instrumento de corte através do maçarico, já estamos a falar das máquinas multibanco que estão encastradas e em que é possível ter acesso ao interior. Ao interior, portanto, à parte de trás. (...) Bem, todas as máquinas são propícias para o arrombamento com gás ou com combustível. Só há dois ou três modelos em que o uso da mistura gasosa ou dos explosivos sólidos tem sucesso. São as máquinas da família DV1413 (...) Nas 1413, essas sim, essas sim, é mais fácil e eram, eu creio que a partir de determinada altura 95% das máquinas alvo de explosão com gás ou com explosivo sólido eram todas dessa marca (...)
E8	(...) ataques com gás, eu diria que, em regra, são para os ATMs "on-the-wall" (...) se corre bem, mantém-se ou porque há um conhecimento melhor por alguma razão, o que já implica alguns conhecimentos técnicos dessa volumetria e da banda de explosividade do gás usado ou então é feita uma experiência prática num modelo específico. Normalmente, é o tempo, medem o tempo que estão a bombear gás e, com aquele tempo, sabem que funciona naquele modelo de ATM. Então fazem sempre no mesmo modelo, da mesma forma, para garantir que continua a funcionar. Ou seja, para ganhar, não se mexe, não se inventa, não se varia, para manter o sucesso (...)
E9	(...) Máquinas mais antigas como os modelos da linha DV213, eram passíveis de ser cortadas e arrombadas devido ao seu sistema de fecho do cofre (...)

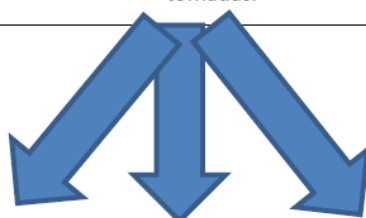
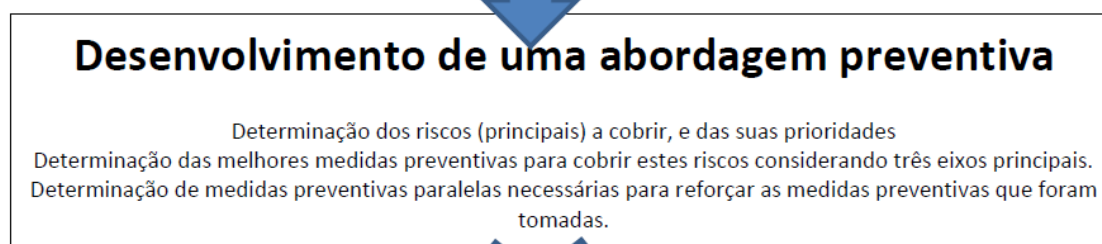
6. Como pode a GNR prevenir a prática de crimes de furto de/a ATM?	
E1	(...) o papel crucial da análise do fenómeno pelas estruturas de informações e investigação criminal, que permitem uma melhor orientação do dispositivo nas atividades preventivas levadas a efeito pelas Unidades. Com base nesta dimensão analítica, é possível alocar os recursos (patrulhamento) para as zonas de risco mais elevado, de forma mais tempestiva. Acresce ainda uma colaboração e comunicação, constantes, com as instituições bancárias, que ao longos dos últimos anos tem permitido uma resposta mais eficiente face a este tipo de fenómeno criminal.
E2	(...) da implementação de operações de investigação criminal orientadas pela análise criminal, especialmente na capacidade de detetar padrões e conseguir chegar ao grupo de autores (...) uma melhor articulação com entidades bancárias e gestoras de ATM, promovendo o intercâmbio de

	informações em tempo real. Protocolos de comunicação direta, partilha de imagens de videovigilância e notificações automáticas de carregamentos ou incidentes são fundamentais para uma resposta mais eficaz e preventiva. (...) o reforço do treino das patrulhas para reconhecer sinais de preparação para crimes de furto pode permitir uma intervenção antes da consumação do crime (...) sensibilização da população e o incentivo à denúncia de comportamentos suspeitos são elementos cruciais.
E3	(...) Plano de Interceção e abordagem por Comando Territorial, onde constem a localização dos ATM potenciais alvos (georreferenciação) e possíveis itinerários de acesso e fuga, que aquando dos ilícitos e aliados ao comando e controlo efetuado pelas Salas de Situação dos Comandos Territoriais, permita efetuar o posicionamento estratégico das patrulhas, coordenando os meios disponíveis, e assim, conseguir destas uma pronta atuação, melhor recolha de informação e possível interceção dos meliantes (...) Formação / informação dos militares das patrulhas, no tocante à operacionalização do Plano de Interceção e abordagem, salientando a importância da observação e apontamento dos pormenores mais relevantes, da perigosidade que estes meliantes representam e da posterior recolha do máximo de informação, junto das diversas entidades envolvidas (a título da futura análise e tratamento da informação criminal)(...) Após o levantamento de todas as caixas ATM na sua ZA de atuação, os PTER devem incidir o patrulhamento diário (noturno) pelos locais onde existem ATM.
E4	A maior dificuldade no acompanhamento desta prática criminal, prende-se com a forma desajustada e deficiente como o crime é registado em sistema SIOP-P, pois a mesma problemática criminal surge inscrita de várias formas (tipo de crime). Por outro lado, ainda no que concerne ao registo em sistema, os objetos não são criados ou apresentam deficiências da descrição (...) importa proceder-se à atualização dos MO direcionados a esta temática criminal, com vista a potenciar ações mais preditivas.
E5	Efetuar uma rigorosa avaliação de segurança aos locais onde as entidades bancárias pretendem instalar os ATM (...), exigindo as condições legais para a sua instalação (...) Coordenação com as entidades bancárias, de manutenção das máquinas e dos locais onde as máquinas se encontram instaladas (...) Reforço do policiamento preventivo em locais mais sombrios, ermos ou propícios aos furtos (...) Recolha de informações policiais e de investigação criminal, que permitam a predição de eventuais crimes (...) manter estreita relação e colaboração com (...) OPC.
E6	(...) quem se dedica a este tipo de ilícitos possui um nível de organização, mobilidade, recursos, motivação e sofisticação (...) implementadas medidas integradas em toda a ZA da GNR, que alie obrigatoriamente o patrulhamento de elevada visibilidade e ostensivo junto dos ATM mais vulneráveis, nos períodos mais críticos (03h00/05h00) (...) recolha de informações (...) e troca de informações permanente com os restantes OPC's, bem como com a SIBS (...), deverão as Entidades Bancárias instaladoras dos ATM ser sensibilizadas e alertadas para a implementação e reforço de medidas de segurança passiva, complementares à atuação dos OPC.
E7	(...) Em termos formais, pode assegurar o cumprimento de uma primeira portaria que surgiu (...) É fundamental perceber se a máquina está de facto ancorada ao chão, com bucha química e todos os elementos de fixação adequados, e se o local onde está instalada oferece alguma resistência física, por exemplo, se é um espaço com vidro, se as paredes são de vidro, entre outros aspetos (...) é importante ter um bom relacionamento com as entidades bancárias e perceber se existe uma rotina de carregamento das máquinas (...) é essencial identificar quais são as máquinas mais vulneráveis, seja pela distância ao posto da GNR, seja por serem mais antigas e, por isso, mais suscetíveis a ataques (...) que se encontram em locais mais isolados, como juntas de freguesia, campos de futebol, ou espaços desportivos (...) fazer um levantamento da videovigilância existente no local (...) temos verificado sempre, é que os autores destes furtos são indivíduos que moram em áreas urbanas sob controlo da Polícia de Segurança Pública, (...) É preciso haver aqui uma certa relação (...)
E8	(...) não tenho dúvidas de que estes tipos de grupos têm também vigilância da área para evitar correr riscos. E, sim, temos essa perceção nos grupos que já apanhámos (...) única forma que vejo é através daquilo que falámos anteriormente: dos crimes percursores e dos sinais de alerta que possam indicar a preparação de algum tipo de crime. Também ajudaria se houvesse uma boa disseminação de informação (...) Uma das formas seria melhorar a identificação deste tipo de crimes percursores e permitir que fossem feitos alertas a nível nacional para a possibilidade de ocorrência destes crimes. Assim, poderíamos direcionar e sensibilizar melhor os nossos meios de patrulha para essas zonas. Tendo esta informação, os nossos polícias conhecem bem as suas áreas e, assim, e tem logo a perceção de quais seriam os ATM mais vulneráveis, associados a características de maior isolamento ou melhores vias de fuga. (...)
E9	Poderá reforçar o seu patrulhamento em zonas de maior risco, atendendo à localização das máquinas e pouco mais. Não se trata de um crime inopinado, mas sim algo preparado e estudado pelos seus autores. Estes, estudam a localização da máquina, a localização do Posto, a rota das patrulhas e usam de forma comum falsas ocorrências para afastarem a patrulha da zona da máquina, se atendermos ao método de explosão por gás, basta entre 1 a 2 minutos para terem acesso ao dinheiro, dando-lhes de forma confortável bastante tempo para estarem longe antes da resposta policial (...) Instalação de câmaras de segurança em locais estratégicos e patrulhamento regular em áreas vulneráveis (...) Campanhas de sensibilização para alertar a população sobre comportamentos suspeitos e medidas de segurança (...) Utilização de sistemas de alarme e dispositivos antifurto nos ATMs. (sistemas de tintagem de notas/colagem de notas) (...) Colaboração com instituições financeiras (...) Investigação e intel: Identificar padrões de crimes e grupos organizados para antecipar e prevenir ataques.

ANEXO

ANEXO A – RECOMENDAÇÕES PARA UMA ABORDAGEM PREVENTIVA: RESUMO

Desenvolvimento de uma resposta eficaz para a prevenção de assaltos físicos a terminais bancários



Medidas preventivas que podem ser tomadas para		
Diminuição da recompensa	Aumentar o risco	Aumento do esforço
– Diminuição do montante de dinheiro. - o Esvaziamento do terminal bancário à noite. - o Aumento do número/frequência dos reabastecimentos. – Destruição do saque. - o Sistemas inteligentes de neutralização de notas bancárias. - o Marcadores infravermelhos na tinta dos sistemas de neutralização para detetar notas manchadas pelos recetores de notas. - o Sob desenvolvimento: cola.	– Partilha de informações através fronteiras para: - o deteção precoce ou em tempo real de um assalto a um terminal bancário, - o reforçamento da abordagem operacional, - o condenação dos recidivistas, - o intercâmbio de dados forenses a nível europeu. – Dispositivos de escuta e circuito fechado de televisão. – Punição consequente e reabilitação do delinquente.	– Fornecimento de um ambiente resistente ao crime. - o Modificação da localização dos terminais de alto risco. - o Medidas de segurança: obstáculos físicos, supervisão, etc. – Reforço dos terminais com portas rolantes, resistentes aos explosivos de gás ou sólidos, etc. – Medidas arquiteturais como por exemplo máquinas de acesso traseiro – Sistemas de neblina de segurança.

Medidas paralelas para reforçar a abordagem preventiva

- Legislação eficaz, inclusive medidas de prevenção contra assaltos físicos a terminais bancários, sentenças consequentes, etc.
- Estratégia eficaz nos meios de comunicação para dissuadir os perpetradores.
- Colaboração aumentada entre todos os intervenientes (públicos, particulares, polícia) na luta contra os assaltos físicos.
- Redução do risco de danos colaterais a socorristas ou civis (por exemplo, os que vivem nas proximidades e os transeuntes).
- Prevenção social evitando que os jovens sejam recrutados para (este tipo de) crime.

Figura n.º 21 - Recomendações para uma abordagem preventiva: resumo

Fonte: (REPC & Europol, 2019, p.24)