UTILIZAÇÃO FRAUDULENTA DA APLICAÇÃO MB WAY

Nota Prática nº 20/2020

14 de maio de 2020

NOTA PRÁTICA nº 20/2020
14 de maio de 2020

UTILIZAÇÃO FRAUDULENTA DA APLICAÇÃO MB WAY

Esta Nota Prática tem como propósito ser um auxiliar dos magistrados do Ministério Público na compreensão dos fenómenos criminais resultantes da utilização fraudulenta da aplicação MB WAY. Descreve, embora de forma genérica, as diversas situações de facto detetadas e procura contribuir para a respetiva integração jurídico-criminal. Aponta linhas de investigação do caso concreto: sugere diligências de obtenção de prova para a forma mais comum dos casos (a que ocorre com mais frequência) e refere diligências mais alargadas para casos mais complexos.

A Nota foi elaborada após uma ampla partilha de experiências e contributos de magistrados do Ministério Público titulares de investigações envolvendo este fenómeno (em especial, pontos de contacto da Rede Cibercrime e outros magistrados dos DIAP), visando partilhar boas práticas que possam promover a intervenção eficaz e coordenada do Ministério Público.

ÍNDICE

A. O FENÓMENO

1. O Ministério Público tem crescentemente recebido denúncias por práticas fraudulentas relacionadas com a aplicação de pagamentos MB WAY. Em suma, o que tem sido recorrentemente denunciado é o engano fraudulento provocado a muitas vítimas, por criminosos que, por esta via, pretendem obter ilícita e indevidamente valores monetários, por vezes de montante elevado.

2. O MB WAY é uma aplicação destinada primordialmente ao pagamento de quantias com origem e destino em duas contas bancárias diferentes, sobre as quais tenham sido emitidos cartões bancários, utilizando para o efeito os números telefónicos dos titulares dos respetivos cartões (de origem e de destino da quantia em causa). Na aplicação MB WAY, a movimentação de quantias efetua-se mediante a autenticação por via do número de telefone do titular do cartão e de um PIN, definido pelo próprio, aquando da adesão ao serviço.

B. AS PRÁTICAS CRIMINOSAS

3. As situações criminosas que têm ocorrido processam-se genericamente da seguinte forma:

- o agente dos factos escolhe as suas vítimas em plataformas de venda *online*[1], procurando aí identificar pessoas que tenham disponibilizado objetos para venda;
- depois, contacta telefonicamente tais pessoas, manifestando a vontade firme de comprar esses objetos e dispondo-se a pagar os mesmos de imediato, mesmo sem os ver e sem ter qualquer garantia de que os mesmos satisfaçam o seu interesse;
- manifesta o intuito de pagar os mesmos por via da aplicação MB WAY;
- em regra, caso a vítima seja conhecedora deste processo de pagamento, o agente dos factos desliga logo a chamada, não voltando a estabelecer qualquer contacto;
- porém, caso a vítima não conheça a aplicação MB WAY, o agente dos factos desenvolve um processo ardiloso, tendo em vista ter acesso à conta bancária daquela.

4. Nos inúmeros casos concretos que têm sido denunciados, este tipo de atuação varia nos seus pormenores, consoante o agente dos factos criminosos e as circunstâncias do momento.

5. Em muitos dos casos, o agente dos factos convence a vítima de que, para poder pagar-lhe (o que manifesta que fará de imediato), esta tem que deslocar-se a uma caixa Multibanco. Se a vítima aceita fazê-lo, uma vez aí, dá-lhe instruções para aderir ao serviço MB WAY, por via do menu disponível na aplicação informática do Multibanco. Dá-lhe ainda instruções para que, no campo onde deve inserir-se um número de telemóvel, insira o número do telefone do agente do crime, e que insira ainda um PIN indicado pelo mesmo.
Ou seja, na prática, além de convencer a vítima a aderir ao serviço MB WAY, o agente dos factos convence-a ainda a que associe a aplicação ao número de telemóvel dele, fixando um código PIN igualmente por ele definido.

6. Nalguns casos, o agente do crime dá instruções à vítima para que esta associe o seu próprio número de telefone (memorizando-o, para o utilizar mais tarde). Nestas situações, quando a vítima

[1] Por exemplo, entre outras, https://www.coisas.com/, https://www.olx.pt/, ou https://www.custojusto.pt/.

recebe por SMS o código de autenticação do serviço MB WAY, o agente do crime pede que o mesmo lhe seja fornecido – para assim poder utilizá-lo mais tarde, para ativar o serviço.

7. Em qualquer dos casos, na posse do número de telemóvel da vítima e do PIN, o agente do crime consegue aceder ao cartão bancário e à conta bancária daquela. Por isso pode, desde logo, consultar o seu saldo bancário.
Além disso, por via do serviço MB WAY, pode ordenar movimentos bancários a partir da conta da vítima (transferências para outros cartões ou contas bancárias), ou pagamentos de compras. Pode ainda efetuar levantamentos em numerário em caixas Multibanco (este é, aliás, um dos casos mais frequentes).

8. Em variantes igualmente denunciadas, os agentes do crime abordam mesmo vítimas que tenham já efetivamente instalada a aplicação MB WAY. Nalgumas situações, indicam à vítima pretender efetuar o pagamento por via da funcionalidade "*enviar dinheiro*". Porém, na verdade usam a funcionalidade "*pedir dinheiro*", remetendo o pedido à vítima. Esta, recebendo um pedido de dinheiro, inadvertidamente aciona o mesmo, sem se aperceber que, ao invés de receber, vai pagar dinheiro.
Em alternativa a este método, nalguns casos, o agente do crime utiliza a funcionalidade de adicionar uma descrição aos "*pedidos de dinheiro*", com o propósito de que a mesma seja interpretada como uma mensagem da própria aplicação. Tal mensagem incita, de forma enganosa, a que se confirme a funcionalidade de "*pedido de dinheiro*", por forma a que a vítima, instintiva e irrefletidamente ordene o "*envio de dinheiro*".

C. AS VÍTIMAS

9. Em geral, estas situações criminosas resultam da falta de conhecimento e da credulidade dos utilizadores, designadamente de alguns dos que disponibilizam produtos para venda *online*. Por este motivo, têm sido apresentadas queixas por vítimas de todo o país, de forma dispersa e sem conexão entre elas, uma vez que a abordagem que a elas é feita tem por base anúncios na Internet. Por esta razão, entre as diversas vítimas não costuma existir qualquer tipo de relação.

10. Porém, a prática tem revelado que, do lado dos agentes do crime, há alguma concentração: existem múltiplos agentes, com diferentes formas de atuar, mas cada um deles abordou já um grande número de vítimas. Poderá portanto ocorrer, em muitas situações, conexão processual, a qual é relevante em termos processuais penais.
Poderá haver razões para a junção de vários dos processos instaurados em diferentes comarcas do país. Por razões de eficácia, um dos critérios usados para tal junção pode ser o do local onde estão instaladas as caixas ATM onde se processaram os levantamentos, porque será provavelmente o local onde os agentes do crime repetirão múltiplos atos criminosos.

D. ENQUADRAMENTO JURÍDICO

11. Como se referiu acima, foram identificadas práticas criminosas diferenciadas, levadas a cabo por diferentes agentes, isolados e desconhecidos uns dos outros. Por isso, embora todos tenham o mesmo propósito (defraudar vítimas em seu favor), o padrão de cada atuação, no caso concreto,

varia. Por esse motivo, o enquadramento jurídico dos factos tem se ser ajustado à variante de cada caso concreto.

12. Em termos abstratos (não podendo nunca prescindir-se do enquadramento dos factos específicos do caso concreto), na generalidade das situações pode ocorrer a prática de seguintes tipos de ilícito:

- burla (previsto no artigo 217º do Código Penal);
- acesso ilegítimo (previsto no artigo 6º da Lei do Cibercrime);
- falsidade informática (previsto no artigo 3º da Lei do Cibercrime) e
- burla informática (previsto no Artigo 221º da Lei do Cibercrime).

D. 1. A BURLA

13. Como acima se descreveu, todo o processo criminoso tem início numa abordagem fraudulenta do agente do crime à vítima. Esta, é contactada pelo agente do crime, que a ludibria no sentido de a convencer a instalar a aplicação MB WAY e de lhe facultar o PIN MB WAY, que vai permitir ao agente do crime aceder ao cartão Multibanco e à conta bancária da vítima.
Trata-se de um processo ardiloso, com o intuito de permitir ao agente do crime aceder a proveito económico indevido. Sem prejuízo de a análise específica do caso concreto conduzir a diferente enquadramento, este comportamento pode vir a consubstanciar o crime de burla, previsto no artigo 217º, nº 1, do Código Penal[2].

14. A análise de um número significativo de casos concretos denunciados ao Ministério Público e aos órgãos de polícia criminal permitiu indiciar que em muitos deles, emboras as vítimas sejam desconhecidas umas das outras, o agente do crime pode ter sido o mesmo. As primeiras análises policiais sugerem mesmo que poderá haver grupos de agentes do crime que se têm dedicado a estes factos com regularidade, auferindo proveitos que lhes permitem viver dos mesmos. Nestes casos, poderá ocorrer, dependendo da análise do caso concreto, o crime de burla qualificada, previsto no artigo 218º[3].

15. Foram já denunciadas situações em que os proventos ilegitimamente obtidos pelo agente do crime são de valor elevado e, mesmo, consideravelmente elevado. É certo que estes valores não resultam imediatamente desta abordagem inicial, mas são conseguidos em consequência de todos este processo fraudulento, a que correspondem vários tipos de ilícito.
Por isso, se assim ocorrer – e sempre dependendo de ponderação no caso concreto –, o crime em causa pode ser de burla qualificada, como previsto no artigo 218º, nºs 1 ou 2[4].

---

[2] *Artigo 217º (Burla)*
1 – Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, por meio de erro ou engano sobre factos que astuciosamente provocou, determinar outrem à prática de atos que lhe causem, ou causem a outra pessoa, prejuízo patrimonial é punido com pena de prisão até três anos ou com pena de multa. (...)

[3] *Artigo 218º (Burla qualificada) (...)*
2 – A pena é a de prisão de dois a oito anos se: (...)
b) O agente fizer da burla modo de vida; (...)

[4] *Artigo 218º (Burla qualificada)*
1 – Quem praticar o facto previsto no nº 1 do artigo anterior é punido, se o prejuízo patrimonial for de valor elevado, com pena de prisão até cinco anos ou com pena de multa até 600 dias.
2 – A pena é a de prisão de dois a oito anos se:
a) O prejuízo patrimonial for de valor consideravelmente elevado; (...)

16. Têm sido comunicadas informalmente ao Ministério Público situações em que os burlões abordam as vítimas sem sucesso, porque estas estão informadas sobre este tipo de comportamentos delituosos. Noutros casos, no decurso do processo, apura-se que o agente do crime tentou ludibriar outras pessoas, para além do queixoso – pessoas essas que não apresentaram queixa formal. Portanto, em relação a estas vítimas, ocorreu um crime de burla simples, na forma tentada (artigo 217º, nº 1, e artigo 22º, ambos Código Penal). Embora tais factos sejam puníveis, nos termos do artigo 217º, nº 2 do Código Penal, nestas situações o procedimento criminal depende de queixa (como se dispõe no nº 3 do mesmo artigo 217º).
Todavia, quanto a situações em que um cidadão foi objeto de uma tentativa de burla deste tipo, sem se ter queixado, esta circunstância não deverá determinar, no caso concreto e nessa parte, o imediato arquivamento do processo. Com efeito, sendo conhecido o perfil deste tipo de criminalidade, importará antes de mais apurar se, no caso concreto, o agente do crime não terá incorrido na prática de mais crimes, situando-se pois a sua atuação na área da burla qualificada (artigo 218º do Código Penal), cujo procedimento não depende de queixa.

D.2. O ACESSO ILEGÍTIMO

17. O resultado mais imediato do processo delituoso que se descreveu é a possibilidade que o agente do crime tem de aceder à conta bancária da vítima, por via do seu cartão Multibanco. Com efeito, através da aplicação MB WAY, o agente do crime pode consultar saldos e movimentos da conta da vítima.
O sistema Multibanco é, nos termos da alínea a) do artigo 2º da Lei do Cibercrime[5], um *sistema informático*. Portanto, aceder a uma qualquer parte do sistema Multibanco (por exemplo, a uma conta bancária acessível por via do Multibanco) é suscetível de fazer incorrer o seu autor, sem prejuízo de diferente enquadramento em face das circunstâncias do caso concreto, no crime de acesso ilegítimo (artigo 6º da Lei do Cibercrime).

18. Assim, desde logo, o agente do crime tem "entrada" no *sistema informático*, preenchendo-se portanto o tipo de ilícito do nº 1 do artigo 6º da Lei do Cibercrime[6].
Porém, além disso, o agente do crime usa nessa ação o PIN MB WAY, código de acesso ao sistema, o qual existe para evitar que tal sistema seja acedido por quem não detiver legitimamente esse código. Este PIN tem a função de uma *password*, sendo portanto uma credencial de acesso ao MB

---

[5] *Artigo 2º (Definições)*
Para efeitos da presente lei, considera-se:
a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção; (...)

[6] *Artigo 6º (Acesso ilegítimo)*
1 – Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. (...)
3 – A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.
4 – A pena é de prisão de 1 a 5 anos quando:
a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. (...)

WAY. Por essa razão, ao usar indevidamente e de forma não autorizada este PIN MB WAY, o agente do crime pode preencher a previsão do nº 3 do artigo 6º da Lei do Cibercrime.

19. Acresce que ao "entrar" no sistema Multibanco, através do MB WAY, o agente do crime tem perante si, e pode ficar a conhecer, dados da conta bancária da vítima. Esta informação está resguardada pelo segredo bancário, nos termos do artigo 78º, nº 2, do Decreto-Lei nº 298/92, de 31 de dezembro. Portanto, aceder a ela pode fazer incorrer o agente do crime na forma agravada de crime de acesso ilegítimo, prevista no nº 4, alínea a) do artigo 6º da Lei do Cibercrime.

D.3. A FALSIDADE INFORMÁTICA

20. Descreveu-se acima que, após o acesso ao sistema bancário, por via do MB WAY, o agente do crime pode nele emitir ordens (bancárias) de pagamento, de transferência, ou de levantamento de valores. Na emissão dessas ordens, o agente do crime usa as credenciais de acesso da vítima, porque foi com as mesmas que acedeu ao sistema.
As ordens bancárias que o agente do crime emite, operacionalizadas por instruções no sistema MB WAY, são por ele registadas, em formato digital, como documentos informáticos (bancários). De tais documentos consta que as ordens foram emitidas pela vítima, legítima titular das credenciais que o agente do crime utilizou. Porém, isso não corresponde à realidade. Por outro lado, tais ordens são "executadas" pelo sistema, porque de acordo com as regras de funcionamento deste, foram emitidas por quem tinha a *legitimidade* (credenciais) para as emitir.
Ou seja, por via das credenciais da vítima, o agente de crime produziu documentos bancários que pretende que sejam tratados pelo MB WAY como se proviessem daquela vítima. Pretende ainda que em consequência da emissão de tais documentos resulte a realização de operações bancárias.

21. Como já diversas vezes se sublinhou, o padrão genérico de comportamento de agentes deste tipo de crime que se descreveu não dispensa a análise específica do caso concreto. Porém, se a atuação corresponder ao que acaba de referir-se, o agente do crime pode incorrer na prática do crime de falsidade informática, previsto no nº 1 do Artigo 3º da Lei do Cibercrime[7].

22. Numa perspetiva indiciária, no momento do início da investigação, não sendo ainda completamente conhecidos todos os detalhes da factualidade praticada, este crime, de falsidade informática, pode perfilar-se como o mais grave daqueles que possam vir a imputar-se ao agente do crime, uma vez que é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias. E se assim for, o lugar da prática deste crime pode ser determinante, em termos operativos, na determinação do local onde deve o processo ser investigado.
Com efeito, indiciando-se vários crimes, porventura praticados em várias comarcas, nos termos do artigo 28º, alínea a) do Código de Processo Penal, é competente para conhecer de todos eles "o tribunal competente para conhecer do crime a que couber pena mais grave".

[7] *Artigo 3º (Falsidade informática)*
1 – Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias. (...)

D. 4. A BURLA INFORMÁTICA

23. Além do crime de falsidade informática, previsto no nº 1 do Artigo 3º da Lei do Cibercrime, que acima se descreveu, pode ocorrer, em concurso com aquele, o crime de burla informática, previsto e punido pelo Artigo 221º, nº 1, do Código Penal.
A verificação deste tipo de crime depende, naturalmente, da análise específica do caso concreto. E poderá ocorrer concurso real com o crime de falsidade informática, já que os bens jurídicos protegidos por ambos os crimes são distintos (na falsidade, a fiabilidade que merecem os documentos informáticos e na burla informática a integridade dos sistemas de computadores e, simultaneamente, o património).

24. Com efeito, consumada a falsidade que acima se descreveu, quando utiliza ulteriormente a aplicação MB WAY, como se se tratasse da vítima, o agente do crime *usa*, ou *manipula* dados informáticos em seu proveito económico, o que vai ao encontro do tipo de ilícito previsto no artigo 221º, nº 1, do Código Penal[8].

E. A INVESTIGAÇÃO DO CASO CONCRETO

E.1. A ABORDAGEM DA VÍTIMA

25. Aquando do recebimento da queixa, deve ser recomendado à vítima que contacte de imediato o respetivo banco, bem como os restantes procedimentos preventivos descritos no Alerta Cibercrime emitido a este respeito[9]. Caso o pretenda, a vítima pode também efetuar contacto com a SIBS, gestora da rede Multibanco e do serviço MB WAY, para o número de telefone 217918780. Estes contactos com o banco e/ou com a SIBS, visando designadamente o cancelamento do cartão Multibanco, destinam-se a prevenir danos mais alargados.

A vítima deve ser **ouvida logo que possível**, a seguir à queixa.

26. Mas estes contactos da vítima podem também auxiliar a investigação, tornando-a mais expedita – a vítima deve ser ouvida em declarações logo que possível. É que a vítima pode, se assim o entender, direta e espontaneamente solicitar ao banco (para depois juntar ao inquérito), muitos documentos relevantes: cópia da ficha de abertura da sua conta, com os dados identificativos da mesma, os dados de identificação do cartão abusivamente usado, o extrato da conta nas datas dos movimentos fraudulentos, com discriminação dos movimentos do cartão abusivamente usado, informação sobre eventuais locais de levantamentos ou a identificação das contas de destino, no caso de transferências bancárias.

Solicitar à vítima/queixoso que peça ao banco emissor do cartão a identificação:
- da conta, do cartão e das operações do cartão na rede Multibanco
- das caixas ATM onde possa ter havido levantamentos
- das contas de destino de transferências bancárias que tenha havido

[8] *Artigo 221º (Burla informática e nas comunicações)*
1 – Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até três anos ou com pena de multa.

[9] Alerta Cibercrime de 7 de abril de 2020, disponível online aqui: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/alerta_mbway_2020_04_07.pdf.

Se estes documentos e informações não forem fornecidos pela vítima, tais elementos poderão ser solicitados ao banco, por despacho do Ministério Público, nos termos do artigo 79º, nº 2, alínea e) do Decreto-Lei nº 298/92 de 31 de Dezembro.

27. Na abordagem inicial, deve também ser perguntado à vítima se permite o acesso ao seu telemóvel, para que dele possam ser extraídos os registos das comunicações havidas com o agente do crime: eventuais registos de telefonemas efetuados e recebidos, eventuais mensagens de SMS, de *WhatsApp*, de correio eletrónico ou outras.

Solicitar à vítima/queixoso que preserve e faculte os registos das suas comunicações com o agente do crime

A obtenção de cópia desses registos, se consentida, pode ser feita por qualquer método: pode ser feita uma cópia com métodos tecnológicos forenses, ou pode, mais simplesmente, ser feita uma cópia fotográfica dos registos, que depois será junta ao processo, por auto. Esta informação, logo que junta ao inquérito, tem o valor de prova documental.

28. Já se insistiu, reforçadas vezes, no caráter deste tipo de criminalidade, marcado pela enorme multiplicação dos casos denunciados e pela total dispersão das vítimas pelo território nacional. A dispersão das vítimas traduz-se uma total dispersão do local onde são apresentadas as queixas. No decurso da investigação possivelmente estas queixas serão remetidas para outra circunscrição judicial, onde o agente do crime possa estar já a ser investigado, por factos idênticos contra outras vítimas.

Também este contexto recomenda a inquirição da vítima logo que possível, no local onde a queixa for apresentada (ou no serviço do Ministério Público onde é recebida) uma vez que a ulterior remessa do processo para outra circunscrição tornará esta inquirição logisticamente mais difícil.

Por outro lado, a multiplicação do número de vítimas, as quais virão, putativamente, a ser indicadas como testemunhas numa futura acusação, recomenda a inquirição por magistrado do Ministério Público, sempre que se reúnam condições para tal, atenta a diferença probatória de tal depoimento.

E. 2. OPC COMPETENTE

29. Deixou-se acima clarificado que as atuações ilícitas praticadas neste contexto têm variações entre elas, podendo vir a consubstanciar diferentes tipos de crimes, consoante as circunstâncias do caso concreto.

Delegação de competência: indiciando-se crimes de acesso ilegítimo ou de falsidade informática, a investigação é da competência Polícia Judiciária

Se a análise do caso concreto apontar para a verificação de crimes de acesso ilegítimo e de falsidade informática (Artigos 6º e 3º da Lei do Cibercrime), a delegação de competência para a investigação, que o Ministério Público venha a efetuar, deve ter em conta o teor do Artigo 7º, nº 3, alínea l) da Lei nº 49/2008, de 27 de agosto[10]. De acordo com este dispositivo, a investigação de crimes "*informáticos e praticados com recurso a tecnologia informática*" é da competência reservada da Polícia Judiciária.

[10] *Artigo 7º (Competência da Polícia Judiciária em matéria de investigação criminal) (...)*
3 - É ainda da competência reservada da Polícia Judiciária a investigação dos seguintes crimes, sem prejuízo do disposto no artigo seguinte:
l) Informáticos e praticados com recurso a tecnologia informática; (...)

E. 3. A PLATAFORMA MB WAY

30. Como acima se disse, a APP MB WAY é uma aplicação informática que permite a utilização do serviço MB WAY. Este, usando o serviço Multibanco, permite fazer compras *online* e em lojas físicas, gerar cartões virtuais MB NET, enviar e pedir dinheiro e ainda utilizar e levantar dinheiro diretamente através do próprio *smartphone*.
Pode aderir ao serviço MB WAY qualquer pessoa que seja titular de um cartão Multibanco (e portanto de uma conta bancária). As compras, transferências de verbas ou pagamentos processados por via do MB WAY são movimentos bancários, processados por via da rede Multibanco, como se fossem processados através do cartão a que a aplicação está associada.
Por isso, se um terceiro (o agente do crime) associar o seu número de telemóvel ao cartão Multibanco de uma vítima, aquele passa a poder usar completamente este cartão.

31. Portanto, a investigação tem, em primeira linha, que identificar os números de telemóvel utilizados pelo agente do crime, em associação ao cartão da vítima. Do mesmo modo, tem que identificar os movimentos MB WAY, com as referências de data e hora, bem como o tipo de operação e local onde foi realizado.
Tendo em conta o perfil desta atividade criminógena, repetidas vezes praticado pelo mesmo agente do crime, contra vítimas desconhecidas umas das outras, importará também saber se o número de telemóvel identificado já tinha estado associado a outras contas MB WAY, de outras vítimas.

32. A aplicação MB WAY é gerida pela SIBS (anteriormente "*Sociedade Interbancária de Serviços*" e atualmente "*SIBS Forward Payment Solutions*"), a mesma entidade que gere a rede Multibanco. Esta entidade gere, de forma transversal, o funcionamento da aplicação MB WAY, quanto a todas as instituições bancárias aderentes a este serviço. As informações registadas e detidas pelas SIBS a este respeito, embora abrangidas por sigilo bancário, poderão ser solicitadas a esta instituição, por despacho do Ministério Público, nos termos do artigo 79º, nº 2, alínea e) do Decreto-Lei nº 298/92 de 31 de Dezembro.

33. A SIBS pode informar o inquérito, designadamente, da informação respeitante aos concretos movimentos fraudulentos realizados por via do MB WAY: os locais, data e hora de tais movimentos, os montantes dos levantamentos (se tiver havido levantamentos em numerário), a concreta máquina ATM onde foi processado o levantamento; em caso de transferência, o número de telemóvel associado à conta beneficiária, bem como o IBAN (*International Bank Account Number*) da mesma.

34. Com o pedido de informações, deve ser fornecida à SIBS informação que permita identificar o número do cartão da vítima e o IBAN que corresponde à conta sobre o qual o mesmo foi emitido, bem como o número de telefone da vítima e aquele que possa ter sido usado pelo agente do crime na fraude.

Solicitar à MB WAY (SIBS) a identificação dos movimentos fraudulentos realizados por via do MB WAY:
- local, data e hora dos movimentos
- montantes dos levantamentos (em numerário) e a máquina ATM onde foi efetuado
- em caso de transferência, o número de telemóvel associado à conta beneficiária, bem como o IBAN da mesma

Tendo em vista o estabelecimento de comunicação eficaz, tal pedido deve ser efetuado por via do formulário que se junta como Anexo I, o qual deve ser dirigido, por correio eletrónico, para o seguinte endereço: investigations.fraud@sibs.com. A expedição de tal mensagem tem que ser efetuada a partir de um endereço oficial dos domínios @mpublico.org.pt, @tribunais.org.pt ou @pgr.pt.

A comunicação com a SIBS é feita por via um **formulário**, remetido por email para **investigations.fraud@sibs.com**

35. O pedido à SIBS, efetuado da forma que acima se descreveu, por via do formulário junto no Anexo I, deverá ser feito em todos os inquéritos em que se denunciem casos deste tipo.
Porém, em casos com maiores ou mais específicas exigências, poderá além disso ser efetuado um pedido mais alargado, solicitando informações mais completas. Tal pedido endereçado igualmente por email, para o mesmo endereço (investigations.fraud@sibs.com) poderá requerer da parte da SIBS mais diligências (e sobretudo mais demoradas), na preparação da resposta. A SIBS dispõe da informação mais alargada que aquela que acima se referiu, a qual pode ser solicitada caso se torne necessária, no caso concreto. Descreve-se essa informação no Anexo II.

E. 4. O RECEBIMENTO DA QUEIXA

No primeiro despacho, o Ministério Público deve logo verificar se acompanham a queixa alguns elementos de prova necessários – os elementos em falta devem solicitar-se logo

36. O tipo de criminalidade a que se refere esta nota prática é perpetrado à distância, sem contacto físico entre a vítima e o agente dos factos, sendo todo o relacionamento entre eles efetuado por via de redes de comunicações. Por isso, os elementos de prova essenciais à investigação deste tipo de casos estão registados em suporte digital. Muitos destes dados são voláteis: são preservados por um lapso muito curto de tempo, sendo depois apagados. Portanto, uma rápida recolha de prova é essencial ao sucesso da investigação.

37. Após o recebimento da queixa, deve de imediato verificar-se se acompanham a mesma algumas informações que, não sendo obtidas de forma expedita, mais tarde não será já possível obter. Assim acontecerá com informações respeitantes à forma como o agente dos factos abordou a vítima, ou referentes às comunicações eletrónicas efetuadas, ou ainda informações registas nas instituições bancárias.

E. 5. OS ANÚNCIOS *ONLINE*

38. Adiantou-se acima que, de forma geral, os agentes do crime escolhem as vítimas que abordam de entre as pessoas que disponibilizam o seu número de telefone em plataformas *online*, em anúncios de produtos que colocam para venda. É por isso importante recolher imediatamente elementos de prova a este respeito.
Normalmente, aquando da queixa, o anúncio em causa estará ainda disponível *online*, em fonte aberta. É portanto possível, de forma livre, aceder ao mesmo por via da Internet e imprimir o anúncio (conjuntamente com o respetivo *link*, ou URL) para junção ao processo.
Não sendo obtida esta informação deste modo, a mesma pode ser solicitada à plataforma em causa, por ordem do Ministério Público, nos termos do artigo 14º, nº 1 da Lei do Cibercrime. Porém,

este procedimento será mais demorado e de resultado mais incerto, porque é variável o tipo de informação preservado pelas diversas plataformas.

E. 6. O CONTACTO DO AGENTE DOS FACTOS COM A VÍTIMA

39. A emergência na formulação da queixa, muitas vezes feita oralmente num posto policial, nem sempre permite à vítima descrever, naquela ocasião, detalhes importantes dos contactos que manteve com o agente do crime. Anote-se que todos esses contactos terão normalmente sido telefónicos e, na perspetiva da vítima, focados na venda de um produto.
Na primeira análise da queixa importa verificar se a vítima facultou o número (ou números) de telefone do agente dos factos, bem como o registo das chamadas efetuadas e recebidas. Importaria ainda obter, caso não tenham sido fornecidas, eventuais mensagens de SMS ou *WhatsApp* trocadas com o agente dos factos.
Toda esta informação pode ser junta ao processo, entre outras formas, por registo fotográfico, como acima se disse já.

40. Deve também verificar-se se a queixa descreve a perceção que a vítima teve do agente dos factos e das respetivas caraterísticas, tanto quanto o contacto telefónico permitiu aperceber (forma de falar, regionalismos no discurso, sotaque, etc.).

E. 7. INFORMAÇÃO BANCÁRIA

41. Já acima se referiu que, sendo este tipo de criminalidade realizada, em boa medida, por via do sistema bancário, importa recolher no inquérito informação a este respeito: os dados exatos de identificação da conta bancária e do cartão da vítima, bem como a identificação de eventuais contas bancárias destinatárias de transferências bancárias efetuadas pelo agente do crime.

42. Como se disse, esta informação pode ser voluntariamente solicitada pela vítima ao seu banco – e por ela fornecida ao inquérito. Não o sendo, pode ser solicitada, pelo Ministério Público, ao banco onde está domiciliada a conta, apesar de estar abrangida pelo sigilo bancário, nos termos nos termos do artigo 79º, nº 2, alínea e) do Decreto-Lei nº 298/92 de 31 de Dezembro.

43. Em termos operacionais, uma das informações mais importantes em posse do banco, é a da concreta caixa ATM onde possam ter sido efetuados levantamentos ilegítimos, pelo agente do crime. Além de ser uma informação de investigação muito importante, conhecê-la vai permitir saber se a caixa ATM em causa dispõe, ou não, de câmaras de vigilância. Se dispuser de tais câmaras, importará obter a gravação das imagens das mesmas.

Além da informação bancária, muitos **bancos dispõem ainda de registo de imagens** (vídeo) da utilização das máquinas ATM

44. Como é sabido, algumas das caixas ATM dispõem de sistemas de vigilância por câmaras de vídeo, que captam e gravam imagens. Tal registo é feito por permissão do Artigo 31º, da Lei nº 34/2013, de 16 de maio (regime do exercício da atividade de segurança privada). Segundo esta norma, as gravações resultantes desta vigilância "*são conservadas, em registo codificado, pelo prazo de 30 dias contados desde a respetiva captação, findo o qual são destruídas*".

Este prazo de conservação é muito curto e, caso se queiram obter as gravações dos utilizadores de uma determinada máquina ATM (onde, por exemplo, tenham sido efetuados levantamentos ilegítimos em numerário), o pedido das mesmas ao banco que as efetuou terá que ser muito célere. Processualmente, esta diligência reveste a forma de injunção para apresentação de dados, prevista no artigo 14º, nº 1 da Lei do Cibercrime, diligência processual da competência do Ministério Público.

45. A limitação do prazo de conservação das imagens pode recomendar, no caso concreto, que se solicite ao banco a preservação dessas imagens, se no imediato não estiverem reunidas condições para a solicitação das mesmas – diligência prevista no artigo 12º, nº 1, da Lei do Cibercrime. A preservação das imagens pode, nos termos do nº 2 deste mesmo artigo 12º, ser "*ordenada pelo órgão de polícia criminal (...) quando haja urgência ou perigo na demora*".

E. 8. INFORMAÇÃO DOS OPERADORES DE COMUNICAÇÕES

46. Este tipo de crimes depende do estabelecimento de comunicações telefónicas, cujos registos (e outros dados) são essenciais à investigação. É pois importante, no inquérito, obter os dados disponíveis quanto à identificação do titular do telefone (ou telefones) usado pelo agente do crime, bem como eventuais registos comprovativos das comunicações estabelecidas.

47. O agente do crime é desconhecido da vítima. Porém, como a abordagem da vítima é feita por telefone, é possível, logo num primeiro momento da investigação, apurar junto da operadora de comunicações a quem pertence esse mesmo número de telefone, da mesma forma que é possível obter dados relacionados com a utilização do mesmo.
Os pedidos de informações a operadores de comunicações são o objeto da Nota Prática nº 8/2016, do Gabinete Cibercrime[11], cujas conclusões se mantêm válidas. Por outro lado, tais pedidos devem ser realizados com utilização dos formulários previstos na Circular nº 12/2012 da Procuradoria-Geral da República[12].

48. Os dados em posse do operador telefónico podem permitir apurar, antes de mais, a identificação do agente do crime, caso esta seja conhecida do operador. Mesmo não o sendo, o operador pode porém informar sobre o IMEI (*International Mobile Equipment Identity*) do aparelho telefónico onde foi utilizado o número telefónico do agente do crime, bem como sobre outros números telefónicos utilizados por aquele aparelho.
O pedido deste tipo de informação, em inquérito, é uma diligência da competência do Ministério Público, nos termos do artigo 14, nº 4, b) da Lei do Cibercrime.
Tal informação é preservada pelos operadores pelo período de seis meses. Esta solicitação pode ser efetuada logo que seja conhecido o número telefónico utilizado pelo agente do crime o qual, normalmente é referido na participação inicial.

Os **operadores de comunicações** podem conhecer a identidade dos utilizadores de telemóveis e, mesmos que assim não aconteça, conhecem o **IMEI** daqueles telemóveis, bem como **outros números de telemóvel utilizados pelo mesmo aparelho**

[11] A Nota Prática nº 8/2016 está disponível em fonte aberta aqui: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp_0.pdf.
[12] Estes formulários estão disponíveis no SIMP Cibercrime, aqui: https://simp.pgr.pt/destaques/des_ficha.php?nid_destaque=1999.

49. Todavia, em alguns casos poderá ser útil à investigação solicitar ao operador de comunicações dados referentes às comunicações efetuadas pelo agente dos factos (registo de chamadas efetuadas e recebidas, ou localização celular, por exemplo).
O pedido deste tipo de informação a operadores de comunicações depende de autorização judicial, nos termos do artigo 18º da Lei do Cibercrime e dos artigos 187º e seguintes do Código de Processo Penal. Além disso, apenas será possível se os factos indiciados no caso concreto forem suscetíveis de preencher os tipos de crime de falsidade informática (artigo 3º, nº 1 da Lei do Cibercrime) e acesso ilegítimo (artigo 6º, nº 4, alínea a) da Lei do Cibercrime). Tais dados não podem legalmente ser solicitados em casos em que apenas se indicie crime de burla, previsto no artigo 217º, nº 1, do Código Penal (embora o possam ser em casos de burla qualificada, prevista no artigo 218º, nºs 1 ou 2, do Código Penal).

E. 9. INFORMAÇÕES ADICIONAIS

50. Nalguns casos pode ainda ser necessário obter informação adicional. Assim acontecerá, por exemplo, se o agente do crime tiver contactado a vítima por via de correio eletrónico. Nestes casos é importante apurar os dados de identificação do titular da conta de email usada pelo agente do crime.
Se tal conta de email pertencer a um fornecedor de serviços sedeado em Portugal, tal pedido deverá ser efetuado nos termos descritos (e com os formulários previstos) na Circular nº 12/2012 da Procuradoria-Geral da República, que já acima se referiu.
Se a conta de email pertencer à Google (*gmail*), o pedido deve ser feito da forma descrita na Nota Prática nº 14/2019 do Gabinete Cibercrime[13]. Por outro lado, se a conta de email pertencer à Microsoft (*hotmail* ou *outlook*, por exemplo), os pedidos devem ser feitos da forma descrita na Nota Prática nº 18/2020[14] e na Nota Prática Provisória nº 19/2020[15].

Caso tenha havido **comunicações por email,** importa obter informação do fornecedor de serviço e os cabeçalhos técnicos das mensagens

51. Caso tenha havido comunicações por via de correio eletrónico entre o agente do crime e a vítima, deve solicitar-se a esta última a versão digital das mensagens de email, de modo a que seja possível obter os cabeçalhos técnicos daquelas mensagens. Esses cabeçalhos técnicos fornecerão informação (e designadamente o endereço de IP de origem) da comunicação, a qual porventura permitirá determinar de onde esta fisicamente proveio.

52. Como já acima se disse, a generalidade das situações factuais a que se refere esta Nota Prática tem origem em anúncios de venda de objetos publicados em plataformas de vendas *online*. Estas plataformas geram e guardam informação referente à consulta dos anúncios, que potencialmente pode vir a ser útil nalguns inquéritos.
Trata-se de informação que pode ser solicitada, em inquérito, por despacho do Ministério Público, nos termos do artigo 14, nº 4, b) da Lei do Cibercrime.

---

[13] A Nota Prática nº 14/2019, de 20 de dezembro de 2019, está disponível aqui: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_14_pedidos_a_google.pdf.
[14] A Nota Prática nº 18/2020, de 27 de março de 2020, está disponível aqui: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_18_pedidos_de_informcao_a_microsoft.pdf.
[15] A Nota Prática Provisória nº 19/2020, de 29 de abril de 2020, está disponível aqui: https://simp.pgr.pt/destaques/mount/anexos/7937_2020_04_29_nota_pratica_19___pedidos_de_informacao_a_microsoft.pdf.

A título exemplificativo, descrevem-se no Anexo III as informações técnicas recolhidas pela plataforma OLX na utilização da mesma. A plataforma OLX pertence a um grupo multinacional e é representada em Portugal pela OLX Portugal, com instalações no Edifício Atrium Saldanha, Praça Duque de Saldanha, nº 1, piso 3, fração H, 1050-094 Lisboa.

ANEXO I
PEDIDO DE INFORMAÇÕES EM PROCESSO PENAL

SIBS, Forward Payment Solutions, S.A. Rua Soeiro Pereira Gomes, lote 1, 1600-198 Lisboa
Remeter por email para: investigations.fraud@sibs.com

Departamento ou Serviço do Ministério Público:		
Endereço de email para resposta:		
Ofício nº	***Data***	***NUIPC***

Nos termos dos Artigos 263º e 267º do Código de Processo Penal, o Ministério Público solicita a V.Exª que informe o inquérito acima referenciado dos dados mais abaixo referidos, referentes ao seguinte utilizador do **serviço MB WAY**:

Nome	
Número de cartões de débito/crédito	
Número de IBAN da Conta	
Número de telemóvel do lesado	
Números de telemóvel usados na fraude	

Solicita-se que seja prestada a seguinte informação, respeitante ao utilizador da Aplicação MB WAY acima identificado:

Período da informação pretendida	No dia Clique ou toque para introduzir uma data. Entre o dia Clique ou toque para introduzir uma data. e o dia Clique ou toque para introduzir uma data.
☐	Movimentos efetuados no cartão (**débitos e transferências**), com indicação da data, hora, local, IBAN da conta de destino, respetivos beneficiários, morada e números de telefone a estes associados
☐	Movimentos efetuados no cartão (**levantamentos em numerário**), com indicação do montante, data, hora e identificação da concreta máquina ATM onde os mesmos foram realizados
☐	**Cartões MB Net** gerados através da aplicação e registo de transações efetuadas, com indicação do montante atribuído, data, hora e local das transações, IP utilizado e entidade beneficiária
☐	Informação sobre se os **números de telefone** acima indicados, utilizados na fraude, estão associados a queixas de fraude dirigidas à SIBS, solicitando-se, em caso afirmativo, a remessa de cópia das mesmas
☐	Informação sobre se os **cartões de débito/crédito** acima indicados, ou a conta bancária a que respeitam, se encontram associados a queixas de fraude dirigidas à SIBS, solicitando-se, em caso afirmativo, a remessa de cópia das mesmas
☐	**Outras utilizações**, indicando descrição das mesmas e os respetivos beneficiários

Assinatura:
Magistrado do Ministério Público)

ANEXO II
INFORMAÇÃO ADICIONAL QUE PODE SER SOLICITADA À SIBS

A) INFORMAÇÃO TÉCNICA GERADA NA UTILIZAÇÃO DO MB WAY

1) *cookies*;
2) *pixel tags*[16];
3) dados de atividade ou tráfego:
   a) tipologia de operações utilizadas;
   b) volume de utilização;
   c) valor das operações realizadas;
   d) setores de atividade de compra;
   e) configurações;
   f) prestador do Serviço MB WAY;
   g) sistema operativo, marca e modelo do equipamento;
   h) conclusão do fluxo das operações e
   i) estado do serviço.

B) INFORMAÇÃO FORNECIDA PELOS UTILIZADORES

Com base nos dados de registo e de utilização, a plataforma MB WAY procede ao tratamento dos seguintes dados pessoais dos seus utilizadores, pelo período de um ano:

a. nome;
b. endereço de correio eletrónico;
c. número de telemóvel;
d. endereço de IP de acesso;
e. ID do dispositivo[17] e
f. *browser* utilizado no acesso.

---

[16] O Pixel TAG é um gráfico com dimensão de 1x1 pixel que é carregado quando se acede aos conteúdos de uma página web ou aplicação, e é utilizado essencialmente para traking e partilha de informação entre OSP's para efeitos de publicidade e gestão de conteúdos apresentados ao utilizador.
Pela utilização de um pixel tag em página web ou aplicação pode ser recolhida, designadamente a seguinte informação:

a) Informação implícita (IP e browser ID);
b) Dados anónimos de perfil de utilizador (Profile ID e targeting criteria) – dados estes que, mesmo não identificando pessoalmente o utilizador, podem ser recolhidos em diversos acessos para identificar o profile ID comum;
c) Dados de comportamento de utilizador (visualização de conteúdos, cliques em conteúdos, tempo gasto na visualização de conteúdos).

[17] O ID do dispositivo, quando gerado para identificação de telemóvel com GSM, pode permitir aferir o IMEI do dispositivo, uma vez que aquele pode derivar deste (https://www.digi.com/resources/documentation/digidocs//90001488-13/concepts/c_device_ids_based_on_gsm_imei.htm).

ANEXO III
INFORMAÇÃO GERADA NA UTILIZAÇÃO DA PLATAFORMA OLX

Na utilização da plataforma OLX, por qualquer utilizador, registado ou não, são recolhidos os seguintes dados técnicos:

1) dados do dispositivo:
   a) sistema operativo;
   b) *device ID* e
   c) rede móvel;
2) dados de localização;
3) dados de cliente e de registo:
   a) IP do dispositivo;
   b) *time stamp*;
   c) sistema operativo;
   d) data de registo;
   e) data do último início de sessão e
   f) tipo e versão do *web browser*;
4) dados de *clickstream*:
   a) *websites* de acesso à plataforma;
   b) registo de data e hora de cada acesso;
   c) pesquisas realizadas;
   d) listagens ou *banners* de publicidade acedidos;
   e) interação com anúncios de publicidade ou listagens;
   f) duração do acesso e
   g) ordem de acesso ao conteúdo na plataforma;
5) *cookies* e
6) *pixel tags*.