“PHISHING” E “MONEY MULES”

Nota Prática nº 27/2024

20 de novembro de 2024

ÍNDICE

NOTA PRÁTICA nº 27/2024
20 de novembro de 2024

"*PHISHING*" E "*MONEY MULES*"

Esta Nota Prática pretende auxiliar os magistrados do Ministério Público a enquadrar penalmente as investigações de "phishing" e a intervenção dos chamados "money mules". Sem prejuízo das observações alinhadas no texto que segue, importa sublinhar reforçadamente que uma adequada qualificação jurídico-penal, em cada caso específico, depende sempre das respetivas circunstâncias particulares e dos factos que, no caso concreto, tenham sido apurados.

A. O MÉTODO CRIMINOSO

1. O "*phishing*" é um método criminoso pelo qual os agentes do crime tentam enganar as vítimas, levando-as a fornecer-lhes informações pessoais (códigos de acesso a contas, *passwords*, números de cartões de créditos, ou outros), as quais mais tarde utilizam em seu proveito. É uma das mais frequentes técnicas de defraudação *online*.

Em geral, o processo criminoso começa com a expedição, de forma indiscriminada e para inúmeros destinatários, de mensagens eletrónicas – *email*, SMS, WhatsApp ou análogas. Tais mensagens atraem aqueles destinatários para páginas *falsas*, mas aparentando ser páginas autênticas de redes sociais, bancos, entidades de pagamentos, entre outras. Nessas páginas é solicitado à vítima que ali introduza dados pessoais. Os agentes criminosos capturam esses dados. Na posse deles, atuam como se fossem o legítimo titular dos mesmos – por isso se tornou corrente, a este respeito, o uso da expressão *furto de identidade*.

B. OS DIVERSOS MOMENTOS DO "*PHISHING*"

2. A expressão "*phishing*" alude ao método utilizado pelos agentes criminosos: remetendo um imenso número de mensagens para inúmeras potenciais vítimas, têm a expetativa de que algumas delas *mordam o isco*. Já quanto a *furto de identidade*, não existe uma definição generalizadamente aceite nem uma utilização consensualizada deste termo.

Por isso, a generalidade dos sistemas jurídicos não pune especificamente o "*phishing*" ou o *furto de identidade*, antes punindo, de forma autónoma e individuada, as diversas atuações que compõem este método criminoso. O quadro normativo português encara-o de acordo com os diversos momentos de execução do mesmo:

a) Em geral, o primeiro momento de execução deste método concretiza-se com a expedição de mensagens eletrónicas fraudulentas. Tais mensagens podem simular ter origem num banco, ou numa entidade de pagamentos, ou numa rede social, ou num fornecedor de correio eletrónico. O propósito dos agentes criminosos é o de convencer as vítimas de que tais mensagens são autênticas e tiveram origem na entidade de onde alegadamente provêm, o que, claro, não corresponde à verdade.

b) Num segundo momento, recebida a mensagem, se a vítima acredita que é autêntica, segue as respetivas instruções e acede a uma página na Internet onde lhe é solicitado que introduza dados pessoais – códigos, *passwords*, credenciais de acesso ou outros.
c) Como a página em causa não é "*autêntica*", isto é, não pertence ao banco, ou à entidade de pagamentos, ou à rede social – pelo contrário, é controlada pelos agentes criminosos –, os dados que ali são inseridos pela vítima ficam em posse daqueles. Portanto, neste terceiro momento, os agentes criminosos obtêm acesso às credencias da vítimas, as quais guardam para si.
d) Na posse destas credenciais da vítima, num quarto momento, os agentes criminosos utilizam as mesmas para aceder à respetiva conta: pode tratar-se de uma conta bancária, ou de uma conta de correio eletrónico, ou de rede social. As credenciais capturadas podem também ser dados de cartões de crédito, situação em que é comum os agentes criminosos usarem os mesmos para efetuarem compras *online*.
e) Caso a conta cujas credenciais foram capturadas seja bancária ou de idêntica natureza (permitindo efetuar pagamentos), pode ocorrer um quinto momento, em que os agentes criminosos, acendendo à conta em causa, dali transferem valores para uma outra conta, por si controlada.
f) Nestes últimos casos pode ocorrer um sexto momento, em que os agentes criminosos, tendo procedido à transferência de valores para uma conta bancária por eles controlada, ainda procedem a uma outra transferência de valores, para um outro destino, com o propósito de dissipar o produto do crime ou de ocultar a origem destes valores.

3. Têm sido identificados casos em que a obtenção ilícita de dados pessoais (códigos de acesso, credenciais, *passwords*…) das vítimas foi efetuada por via de ataques informáticos (acesso ilegal a sistemas informáticos, *trojans*, *keyloggers*, *spyware* ou outros *malwares*) – portanto, por métodos diferentes do "*phishing*". Noutros ainda, por técnicas de *engenharia social*.
Têm também sido frequentemente identificados casos em que, na posse de tais dados pessoais, os agentes criminosos os vendem a terceiros, que depois os utilizam.

4. Quanto à utilização dos dados pelos agentes criminosos, embora as formas mais comuns sejam a utilização de dados bancários ou de dados de cartões de crédito para obtenção de quantias ilícitas (transferências, pagamentos…) têm sido identificadas muitas outras utilizações ilícitas de dados.
Têm sido identificados casos de utilização de dados oficiais de identificação, como por exemplo do Cartão de Cidadão, para abertura de contas bancárias (ou para a criação de cartões de crédito), ou ainda para a abertura de contas em plataformas de vendas *online*. Também, para contrair empréstimos ou para comprar, *online*, bens e serviços.
Por outro lado, têm sido identificados inúmeros casos de utilização de credenciais de acesso a contas de correio eletrónico – e sobretudo de contas em redes sociais –, para *controlar* essas contas e, a partir delas, praticar burlas *online* ou para difundir "*malware*".

C. A QUALIFICAÇÃO JURÍDICO-PENAL DO "*PHISHING*"

5. Os procedimentos gerais e mais comuns do "*phishing*" fazem enquadrar este método criminoso em diferentes tipos de crime. Porém, existem múltiplas variantes desta metodologia que escapam a uma tipificação simples. Importa sempre recordar que *cada caso é um caso*: não existe uma qualificação jurídica única e automática para as diversas fases das metodologias de "*phishing*", cujos aspetos operacionais são muito variáveis, fazendo por isso também variar o enquadramento penal.

6. Porém, em muitos dos casos, como se referiu, num primeiro momento, o procedimento de "*phishing*" passa pela expedição de mensagens eletrónicas fraudulentas. Pode tratar-se de mensagens telefónicas escritas (SMS, WhatsApp) ou de mensagens de correio eletrónico. Trata-se, em ambos os casos, de mensagens não solicitadas e inesperadas por quem as recebe. Sistematicamente, alegam provir de entidades de onde não provêm. Em geral incluem *links* que supostamente encaminham para a página na Internet daquela entidade, mas que na verdade encaminham para páginas que não pertencem à mesma nem por ela são geridas ou controladas. A generalidade destas mensagens são facilmente identificáveis pelo utilizador comum, por costumarem conter erros gramaticais e ortográficos. Frequentemente são geradas por tradutores automáticos ou provêm de agentes criminosos de outros países. Por outro lado, incitam sempre à urgência, exigindo uma resposta ou reação muito rápida.

falsidade informática e burla

7. Tratando-se estas mensagens de documentos digitais, importa a este respeito ponderar se, no caso concreto, a sua relevância probatória e a elaboração das mesmas faz os seus autores (e emissores) incorrer na prática de crime de falsidade informática, previsto e punido no artigo 3º, nº 1, da Lei do Cibercrime[1].

As mensagens serão *não genuínas*, no sentido de não provirem de onde dizem provir e no sentido de incluírem conteúdos enganosos. Mas também pretendem ser consideradas como sendo autênticas, daí podendo ser retiradas consequências jurídicas.

Por outro lado, ainda a este respeito, do primeiro e do segundo momento do processo do "*phishing*" (emissão das mensagens e captação das credenciais), importa considerar se o procedimento de preparação das mensagens, o seu conteúdo e a respetiva expedição para potenciais vítimas crédulas, pode ser considerado um artifício ardiloso (com o propósito de obtenção ilícita de credenciais de acesso), relevante para qualificação destes factos como crime de burla, previsto e punido pelo artigo 217º[2] do Código Penal. Ou, porventura, como crime de burla qualificada, previsto e punido pelo artigo 218º, nº 2, alínea b), designadamente nos casos das diversas formas de crime organizado a este respeito, em que os agentes criminosos fazem *da burla modo de vida*.

---

[1] *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. (…)

[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. (…)

8. Como acima se explicou, num terceiro momento do processo de "*phishing*", a vítima depara-se com uma página na Internet que se assume como a legítima e *autêntica* página, por exemplo de um banco, de uma entidade de pagamentos, ou de uma rede social (entre outras). Porém, assim não acontece: trata-se de uma página falsa, *fabricada* pelos agentes criminosos.
Portanto, importa também a este respeito aferir do preenchimento dos elementos do tipo de falsidade informática, previsto e punido pelo artigo 3º, nº 1, da Lei do Cibercrime.
Além disso, neste momento do processo de "*phishing*", as vítimas inserem os seus dados na página *falsa* – ficando aqueles dados na posse dos agentes criminosos.

acesso ilegítimo

9. Sabe-se que, com toda a probabilidade, o destino dos dados é o de serem utilizados pelos agentes criminosos para aceder a sistemas informáticos de acesso *fechado* (contas bancárias, contas de correio eletrónico, entre outros).
Com efeito, a metodologia do "*phishing*" supõe, como momento seguinte, que os agentes criminosos utilizem as credenciais da vítima, ilegitimamente obtidas, para aceder ao banco ou outra plataforma de pagamentos (ou outros sistemas informáticos *fechados*). Este procedimento poderá fazer incorrer o agente criminoso na prática de crime de acesso ilegítimo – artigo 6º da Lei do Cibercrime –, que, poderá ser agravado por força da alínea a) do nº 4 e da alínea a) do nº 5[3].

10. É igualmente sabido que este tipo de atividade é sobretudo desenvolvido por grupos de crime organizado e profissional. É cada vez mais frequentemente os dados serem ilegitimamente obtidos por um grupo criminoso e depois serem vendidos a outro grupo criminoso, que os *explora*.
Os modelos do negócio criminal vão variando e evoluindo. Importa pois, a respeito deste momento do processo de "*phishing*", apurar a verificação dos elementos do tipo de crime previsto no nº 2 do artigo 6º da Lei do Cibercrime[4].

11. Depois de aceder ilegitimamente à plataforma bancária ou de pagamentos, normalmente, o agente do crime utiliza a mesma para efetuar transferências de valores para uma outra conta bancária, por si controlada, ou para efetuar o pagamento da compra de bens ou de serviços que efetuou. Ou dito de outra forma, o agente do crime gera uma ordem (bancária) de transferência ou de pagamento.
A qualificação jurídico-penal deste momento, como de todos os outros, depende das circunstâncias do caso concreto. Pode, porém aproximar-se da falsidade informática (artigo 3º da Lei do Cibercrime), se com a atuação do agente forem gerados documentos digitais bancários não

---

[3] *Artigo 6º*
Acesso ilegítimo
(…) 4 – A pena é de prisão até 3 anos ou multa se:
a) O acesso for conseguido através de violação de regras de segurança; ou
(…)
5 – 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 (…)

[4] *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.
2 – Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.(…)

verdadeiros (assim pode suceder, por exemplo, se constar do documento gerado pelo sistema que o seu autor é o legítimo titular da conta, quando o verdadeiro responsável por esta ordem é o agente criminoso), aos quais é conferida força probatória.

abuso de cartão

12. Importa porém considerar a muito expressiva variante do "*phishing*" que tem como objeto a captura de dados de cartões de pagamento e a efetiva utilização desses dados pelos agentes criminosos.

Após a alteração da Lei do Cibercrime operada pela Lei nº 79/2021, de 24 de novembro, este diploma normativo foi expurgado das regras respeitantes ao uso abusivo de cartões e outros meios de pagamento, se autênticos. A punição de tais atos passou a ser assegurada pelo Código Penal. Com efeito, na versão legal posterior a 2021, o artigo 225º, nº 1, do Código Penal, passou a punir toda a utilização não autorizada e com intenção de enriquecimento ilícito de qualquer dispositivo que permita o acesso a sistema ou a meio de pagamento, incluindo cartões bancários. Do mesmo modo, por força da alínea d) deste número 1, passou a ser punida a utilização dos dados registados, incorporados ou respeitantes aos mesmos dispositivos. Será, por exemplo, o caso de utilização de dados de cartões de crédito para efetuar compras *online* – não apenas compras mas também qualquer forma de pagamento ou depósito, levantamento ou transferência de verbas[5].

a dissipação dos proventos

13. No trecho final do processo de "*phishing*", em particular quando se visam dados de contas bancárias, os agentes criminosos procuram transferir os valores a que têm acesso, ou de que conseguiram apropriar-se, para outras contas, por si controladas. Por vezes, após terem procedido a essa transferência de valores, ainda procedem a uma outra transferência desses mesmos valores, para outros destinos, com o propósito de dissipar o produto do crime e de ocultar a origem dos valores em causa.

Normalmente, as transferências de valores (e por vezes eventuais pagamentos) são efetuados para contas dos chamados *mulas*, ou "*money mules*". Trata-se de agentes terceiros em relação aos crimes acima descritos, mas que se dispuseram a colaboram com os agentes do crime. O tipo e a modalidade de colaboração destes "*money mules*" com os agentes principais do crime determinam o enquadramento penal da respetiva atuação. Esta vertente será abordada mais abaixo.

outros tipos de "*phishing*" - que não bancário ou respeitante a cartões

14. Fica ainda uma última nota para as modalidades de "*phishing*" que visam a apropriação de credenciais de acesso a contas de correio eletrónico ou de contas em redes sociais.

Têm sido detetados comportamentos criminosos especificamente visando esta finalidade. Um dos exemplos mais correntes passa pelo recebimento, pelas vítimas, de mensagens de supostos *amigos* do Facebook, que, por exemplo, lhes solicitam que votem neles, num qualquer concurso *online*. Normalmente, nestes casos fraudulentos, a página onde decorre a suposta votação, simulando ser a verdadeira página de credenciação do Facebook ou do Instagram, requer a

[5] A este propósito foi emitida a Nota Prática nº 24/2021, de 13 de dezembro de 2021, consultável aqui: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_24_novos_crimes_na_lei_cibercrime_2.pdf.

inserção das credenciais da respetiva conta. É nesse momento, nessa suposta página de autenticação no Facebook ou no Instagram, a qual é *falsa*, que, sem o saber, a vítima faculta as suas credenciais aos agentes criminosos. Mais tarde, na posse destas credenciais, aqueles alteram as mesmas e o telefone a elas associado, impedindo assim a vítima de voltar a aceder à conta em causa.

15. Depois, nuns casos, solicitam ao legítimo titular da conta um resgate, como condição para lhe devolverem as credenciais da conta – portanto, por via de extorsão. Noutros casos, a conta é utilizada para, usando a credibilidade que o seu legítimo titular tem, designadamente junto dos seus amigos e conhecidos, publicitar os mais diversos serviços fraudulentos. Têm, em particular, sido identificadas promoções a negócios em criptomoedas, que se inserem claramente na área das burlas.

Este tipo de "*phishing*" tem, portanto, um perfil e uma qualificação jurídica diferenciada. Na primeira modalidade deste tipo específico de "*phishing*", o propósito dos agentes criminosos é a prática de extorsão (artigo 223º do Código Penal): os criminosos atuam com propósitos lucrativos imediatos. Nos outros casos, antes de mais, os agentes criminosos acedem, de forma não autorizada, ao conteúdo das contas de em causa. Portanto, incorrerão na prática de crime de acesso ilegítimo, como previsto e punido no artigo 6º[6] da Lei do Cibercrime. Porque alteram as credenciais de acesso à conta, impedindo o seu legítimo titular de usar essa mesma conta, podem também incorrer na prática de crime de sabotagem informática, previsto e punido pelo artigo 5º[7] da Lei do Cibercrime.

Em geral, porém, os agentes criminosos que se dedicam a este tipo de "*phishing*" têm como propósito a prática de crimes de burla, abusando do nome e credibilidade dos legítimos proprietários das contas em causa.

D. "*MONEY MULES*" – ENQUADRAMENTO PENAL

16. Este tipo de interventores criminais assume um papel essencial nas diversas atividades fraudulentas praticadas por via das redes de comunicações, já que os mesmos são os encarregados de receber as quantias ilegitimamente obtidas e de as canalizar para os mentores principais dos crimes. Porque o fazem de modo a tentar não deixar pistas que permitam identificar aqueles últimos, é relevante considerar que, em inúmeras situações, os "*money mules*" são os únicos intervenientes dos processos criminosos que é efetivamente possível identificar e punir. Assim acontece, desde logo, em muitas das campanhas de "*phishing*".

17. As diversas práticas e modelos de "*phishing*" podem variar muito, variando também os concretos papéis desempenhados pelos "*money mules*". Por este motivo, varia também a valoração jurídico-penal da sua atuação. Ou dito de outra forma, o concreto enquadramento penal das suas

---

[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.(...)

[7] *Artigo 5º*
Sabotagem informática
1 — Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias. (...)

atuações dependerá das circunstâncias do caso concreto. Não obstante, de forma sumária, quando os "*money mules*" cooperam com operações de "*phishing*", segundo os factos ilícitos que em específico se verificarem, podem ser responsabilizados penalmente pela seguinte atuação ou pelos seguintes crimes, previstos no Código Penal:

- coautoria no projeto criminoso em geral;
- branqueamento (artigo 368º-A);
- recetação (artigo 231º);
- auxílio material (artigo 232º), ou ainda
- apropriação ilegítima em caso de acessão ou de coisa ou animal achados (artigo 209º).

coautoria no projeto criminoso

18. O "*money mule*" pode agir em coautoria com os restantes participantes na operação de "*phishing*", fazendo portanto parte do projeto criminoso no seu todo: enquanto outros estão encarregados de outras tarefas, ao "*money mule*" compete, em articulação com os restantes comparticipantes, transferir ou fazer dissipar as verbas ilicitamente obtidas.

Todavia, na prática e no caso concreto, tem-se revelado pouco frequente conseguir demonstrar a concertação de todos os interventores em volta de projetos desta natureza. A experiência tem revelado que, se quando em julgamento os arguidos optam por não prestar declarações, torna-se muito mais difícil estabelecer os laços e acordos que possa haver entre os diversos intervenientes.

É sabido que em muitas das situações fraudulentas que ocorrem, o "*money mule*" recebe as transferências ilícitas numa sua conta bancária e, logo após, transfere-as para outro destino. Em muitas destas situações, nem ele mesmo sabe para onde ou para quem. Já os casos em que as quantias transferidas permanecem mais duradouramente na sua conta podem indiciar que o "*money mule*" é um dos participantes do plano criminoso entre todos acordado.

branqueamento

19. Mesmo não se apurando factos que permitam concluir pela coautoria do "*money mule*", pode indiciar-se crime de branqueamento (artigo 368º-A do Código Penal[8]). Assim poderá acontecer, por exemplo, se a conta bancária onde for depositada a quantia ilícita for regular e habitualmente movimentada pelo suspeito, na sua vida do dia-a-dia. Têm sido identificados casos em que os "*money mule*" sustentam nas investigações que não sabiam que a sua conta tinha sido utilizada para fazer *circular* quantias. Nestes casos importa apurar se, no caso concreto, o "*money mule*" não podia deixar de ter tomado conhecimento daqueles movimentos, porque regularmente

[8] *Artigo 368.º-A*
Branqueamento
1 - Para efeitos do disposto nos números seguintes, consideram-se vantagens os bens provenientes da prática, sob qualquer forma de comparticipação, de factos ilícitos típicos puníveis com pena de prisão de duração mínima superior a seis meses ou de duração máxima superior a cinco anos ou, independentemente das penas aplicáveis, de factos ilícitos típicos de: (...)
b) Burla informática e nas comunicações, extorsão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, contrafação de moeda ou de títulos equiparados, depreciação do valor de moeda metálica ou de títulos equiparados, passagem de moeda falsa de concerto com o falsificador ou de títulos equiparados, passagem de moeda falsa ou de títulos equiparados, ou aquisição de moeda falsa para ser posta em circulação ou de títulos equiparados;
c) Falsidade informática, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima ou reprodução ilegítima de programa protegido; (...)
3 - Quem converter, transferir, auxiliar ou facilitar alguma operação de conversão ou transferência de vantagens, obtidas por si ou por terceiro, direta ou indiretamente, com o fim de dissimular a sua origem ilícita, ou de evitar que o autor ou participante dessas infrações seja criminalmente perseguido ou submetido a uma reação criminal, é punido com pena de prisão até 12 anos.
4 - Na mesma pena incorre quem ocultar ou dissimular a verdadeira natureza, origem, localização, disposição, movimentação ou titularidade das vantagens, ou os direitos a ela relativos.

movimentava a conta em causa. Portanto, em termos de estratégia de investigação, pode ser importante identificar, por exemplo, os movimentos a débito sobre a conta em causa, bem como o *canal* onde tiveram origem (e porventura o IP associado, se o canal foi *online*).

20. Os casos de branqueamento suscitam por vezes dúvidas, quando não se indicia o crime precedente. Assim ocorre por exemplo em burlas com arrendamento de imóveis, ou com as chamadas "*CEO Fraud*", casos em que quantias ilícitas são depositadas em Portugal, mas o crime precedente (a burla) ocorre noutro país. Ou vice-versa.
Nestas situações importa acautelar o *congelamento*[9] da quantia ilicitamente obtida pelos agentes do crime, para ulterior ressarcimento da vítima, mas importa também avaliar a competência (internacional) dos tribunais portugueses para conhecer do caso – ponderando-se a remessa do processado para a eventual jurisdição competente.

recetação

21. Ocorrem casos em que o "*money mule*" incorre na prática de crime de recetação (artigo 231º do Código Penal[10]). Assim acontece quando se demonstra no processo que a quantia depositada na conta do "*money mule*" foi, com o conhecimento deste, *obtida por outrem mediante facto ilícito típico*, como exigido pelo tipo de crime.
Nestas situações é importante demonstrar o conhecimento da ilicitude da transferência da quantia. Tal conhecimento de ilicitude não se verificará, por exemplo, quanto o "*money mule*", com acesso à conta da vítima, dali transfere ou retira quantias – porque tais quantias foram obtidas pela vítima, e portanto não se indicia que tenham sido obtidas mediante facto ilícito.

auxílio material

22. Quanto à verificação do crime de auxílio material (artigo 232º do Código Penal[11]), sucederá nas situações em que se demonstra que o "*money mule*" não participou nos factos criminosos – não é uma situação muito frequente, uma vez que, em geral, o "*money mule*" participa efetivamente nos factos, procedendo a transferência de valores para contas terceiras. Porém, poderá ocorrer, por exemplo, quando o "*money mule*" *cede* as credenciais da sua conta aos agentes criminosos, para que estes a usem para fazer *movimentar* quantias.

---

[9] Anota-se que, tratando-se de um *congelamento* no contexto da Lei nº 83/2017, por via de suspensão da operação, o mesmo (artigos 48º e 49º) deve ser tramitado pelo DCIAP.

[10] *Artigo 231.º*
Recetação
1 - Quem, com intenção de obter, para si ou para outra pessoa, vantagem patrimonial, dissimular coisa ou animal que foi obtido por outrem mediante facto ilícito típico contra o património, a receber em penhor, a adquirir por qualquer título, a detiver, conservar, transmitir ou contribuir para a transmitir, ou de qualquer forma assegurar, para si ou para outra pessoa, a sua posse, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.
2 - Quem, sem previamente se ter assegurado da sua legítima proveniência, adquirir ou receber, a qualquer título, coisa ou animal que, pela sua qualidade ou pela condição de quem lhe oferece, ou pelo montante do preço proposto, faz razoavelmente suspeitar que provém de facto ilícito típico contra o património é punido com pena de prisão até 6 meses ou com pena de multa até 120 dias.
3 - É correspondentemente aplicável o disposto:
a) No artigo 206.º; e
b) Na alínea a) do n.º 1 do artigo 207.º, se a relação familiar interceder entre o recetador e a vítima do facto ilícito típico contra o património.
4 - Se o agente fizer da recetação modo de vida, é punido com pena de prisão de 1 a 8 anos

[11] *Artigo 232º*
Auxílio material
1 - Quem auxiliar outra pessoa a aproveitar-se do benefício de coisa ou animal obtidos por meio de facto ilícito típico contra o património é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.
2 - É correspondentemente aplicável o disposto no n.º 3 do artigo 231.º

apropriação ilegítima

23. Por último, existem situações em que o "*money mule*" incorrerá na prática de crime de apropriação ilegítima (artigo 209º do Código Penal[12]). Assim sucederá nos casos em que o "*money mule*" não acordou com os restantes agentes criminosos o recebimento de quantias na sua conta bancária, uma vez que o tipo de crime requere que os valores em causa tenham *entrado na sua posse (…) por qualquer maneira independente da sua vontade*.

[12] *Artigo 209º*
Apropriação ilegítima em caso de acessão ou de coisa ou animal achados
1 - Quem se apropriar ilegitimamente de coisa ou animal alheios que tenham entrado na sua posse ou detenção por efeito de força natural, erro, caso fortuito ou por qualquer maneira independente da sua vontade é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2 - Na mesma pena incorre quem se apropriar ilegitimamente de coisa ou de animal alheios que haja encontrado.
3 - O procedimento criminal depende de queixa. É correspondentemente aplicável o disposto nos artigos 206.º e 207.º