jurisprudência.pt

Tribunal da Relação de Évora
Processo nº 82/20.9PACTX-A.E1

Relator: MARTINHO CARDOSO
Sessão: 25 Maio 2021
Votação: UNANIMIDADE

MB WAY **FALSIDADE INFORMÁTICA** **BURLA INFORMÁTICA**

CONCURSO DE INFRACÇÕES

Sumário

1 – Está em causa a ocorrência em que um indivíduo, a pretexto de pagar uns objectos que dizia querer comprar à ofendida e por esta postos à venda no OLX, logrou por meio fraudulento induzir a ofendida a aderir ao serviço MBWAY e a associar a referida aplicação ao número de telemóvel do agente, transmitindo-lhe o código de acesso.
Na posse desses dados e com a conta da ofendida associada à aplicação MBWAY no seu telemóvel, o agente acedeu sem autorização a essa mesma conta e, contra a vontade da ofendida, efectuou transferências de dinheiro da mesma para outra conta bancária.

2 – Tal conduta, além de integrar a prática do crime de burla informática, p. e p. pelo art.º 221.º, n.º 1, do Código Penal, em concurso aparente com o de acesso ilegítimo, p. e p. pelo art.º 6.º, da Lei do Cibercrime (Lei n.º 109/2009, de 15-9), integra também a prática de um crime de falsidade informática, p. e p. pelo art.º 3.º da Lei do Cibercrime.

3 - Se a burla informática, p. e p. pelo art.º 221.º, do Código Penal, se realizou mediante a introdução de dados incorrectos/falsos no sistema informático da aplicação MB WAY por um autor mediato que para tanto convence a vítima e lhe dá por telemóvel instruções de como o tem de fazer, correspondendo, pois, ao cometimento pelo agente mediato do crime de falsidade informática, p. e p. pelo art.º 3.º, n.º 1 e 2, da Lei do Cibercrime, existe concurso efectivo entre aquela burla e esta falsidade informática.

Texto Integral

Acordam, em conferência, na Secção Criminal do Tribunal da Relação de Évora:
Nos presentes autos de inquérito acima identificados, do Departamento de Investigação e Acção Penal do (…), Comarca de (…), investiga-se a ocorrência em que (…) e a pretexto de o mesmo pagar uns objectos que dizia querer comprar à ofendida e por esta postos à venda no OLX, ter logrado por meio fraudulento induzir a ofendida a aderir ao serviço MBWAY e a associar a referida aplicação ao número de telemóvel do agente, transmitindo-lhe o código de acesso.
Na posse desses dados e com a conta da ofendida associada à aplicação MBWAY no seu telemóvel, o agente acedeu sem autorização a essa mesma conta e efectuou (…) transferências para outra conta bancária, debitando da conta da ofendida o valor total de (…) €.
Porém, entende o M.º P.º que tais factos são susceptíveis de integrar, além do crime de burla informática, p. e p. pelo art.º 221.º, n.º 1, do Código Penal, em concurso aparente com o de acesso ilegítimo, p. e p. pelo art.º 6.º, da Lei do Cibercrime (Lei n.º 109/2009, de 15-9), também a prática de um crime de falsidade informática, p. e p. pelo art.º 3.º da Lei do Cibercrime, podendo assim aceder, por força da moldura penal abstracta deste ilícito, à localização celular do número de telemóvel pretensamente usado pelo agente – diligência que em consequência e além doutra requereu ao JIC.
E o mesmo indeferiu através do seguinte despacho:
Investigam-se nestes autos factos suscetíveis de integrar a prática dos crimes de burla informática (artigo 221º, n.º 1, do CPenal), em concurso aparente com o crime de acesso ilegítimo (artigo 6º, da Lei do Cibercrime).
Indicia-se em concreto que o agente dos factos, ainda não identificado, logrou por meio fraudulento induzir a ofendida a aderir ao serviço MBWAY e a associar a referida aplicação ao número de telemóvel do agente, transmitindo-lhe o código de acesso.
Na posse desses dados e com a conta da ofendida associada à aplicação MBWAY no seu telemóvel, o agente acedeu sem autorização a essa mesma conta (…) transferências para outra conta bancária, debitando da conta da ofendida o valor total de € (…).
Discordamos assim da posição assumida pelo MºPº que qualificou estes factos como integrando o crime de falsidade informática, p. e p. pelo artigo 3º, da Lei

do Cibercrime.
Esta norma estatui que “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.”.
Nota-se pois que o agente do crime não falsificou qualquer documento digital ou quaisquer dados informáticos, simplesmente usou sem autorização os dados de acesso genuínos que lhe haviam sido transmitidos pela ofendida, para aceder à sua conta sem autorização desta.
Fê-lo com intenção de obter para si ganho ilegítimo, utilizando dados (código de acesso) sem autorização de quem de direito.
Promove o MºPº que seja determinado à operadora MEO/ALTICE que remeta os dados de faturação detalhada e localização celular do número de telemóvel (…), entre (…) e a presente data.
O artigo 18º, da Lei do Cibercrime, estatui que:
“1 - É admissível o recurso à intercepção de comunicações em processos relativos a crimes:
a) Previstos na presente lei; ou
b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.
2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.
3 - A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.
4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.”.
No caso dos autos, está em causa a investigação de factos que integram um

crime previsto na lei do cibercrime (acesso ilegítimo), pelo que é legalmente admissível o recurso à intercepção de comunicações (dados de tráfego ou de conteúdo), que é também indispensável à descoberta da verdade material, na medida em que o crime em causa foi cometido por meio de comunicações telefónicas que cumpre registar documentalmente.
No entanto, já não é permitido o acesso a dados de localização celular, porquanto o acesso a estes dados não está previsto na lei do cibercrime para os crimes aí previstos.
Tal acesso está apenas previsto no artigo 189º, n.º 2, do CPP, que estatui que "A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo.".
Os crimes em causa não integram o "catálogo" do artigo 187º, n.º 1, do CPP, pelo que quanto a estes não pode ser solicitada a obtenção dos dados de localização celular.
De igual modo, quanto aos dados de tráfego, apenas relevam as comunicações ocorridas no dia dos factos (…) e o dia seguinte (tendo em conta que os factos se situam próximo da meia-noite).
*
Pelo exposto, ao abrigo do disposto no artigo 18º, da Lei do Cibercrime, determino que a operadora MEO/ALTICE remeta a estes autos os dados de faturação detalhada do número de telemóvel (…), entre os dias (…) e (…), com listagem das chamadas efetuadas e recebidas, números de chamada/destino e duração das comunicações.
No mais, pelos motivos indicados indefiro o promovido.
D.N.
#
Inconformado com o assim decidido, o M.º P.º interpôs o presente recurso, apresentando as seguintes conclusões:
1. Ao contrário do Ministério Público, que subsume uma parte da factualidade aqui em causa ao tipo de crime *falsidade informática,* defende o Mmo. Juiz de Instrução Criminal que a mesma, no seu todo, integra tão-somente o crime de *burla informática.*
2. Arrancando da qualificação jurídico-penal acima indicada, e que é a sua, o Mmo. Juiz de Instrução Criminal, e atento o disposto no artigo 18.^{0} da Lei do Cibercrime, entende que inexiste substracto legal necessário e suficiente para viabilizar o acesso a dados de localização celular do agente justamente porque o limite máximo da moldura penal prevista para o crime de *burla informática*

não é superior a 3 (três) anos sendo esta - isto é, "*pena de prisão superior, no seu máximo,* a 3 *anos*" - a condição (cláusula) geral inscrita na alínea a) do n.º 1 do artigo 187.^{0} do Código de Processo Penal (CPP), norma para a qual o citado artigo 18.^{0} da Lei do Cibercrime remete.
Ora, com o devido respeito pela opinião do Mmo. Juiz de Instrução Criminal, até porque (igualmente) entendemos que os factos aqui investigados podem, em abstracto, configurar (também) um crime de *burla informática,* não podemos concordar quando pugna pela não possibilidade legal de subsumir trechos da factualidade aqui em causa ao tipo de crime *falsidade informática.*
4. Na verdade, e em síntese preliminar, a circunstância de parte dos factos objecto do presente inquérito poder integrar a prática de um crime de *burla informática* não significa, pelo contrário, que outra parte dos mesmos (os quais, no todo, completam o globo da factual idade investigada) não possa preencher o crime de *falsidade informática.*
5. Assim, o que procuraremos demonstrar com o presente recurso é que no instante procedimento estamos perante factos que integram, em concurso real, os crimes de *burla informática* e de *falsidade informática* e que, sendo este último punível, em abstracto, com uma pena de prisão superior a 3 (três) anos, existe base jurídico-legal bastante para poder ser admitido o acesso aos dados de localização celular do agente.
6. Afirma o Mmo. Juiz de Instrução Criminal que "o *agente não falsificou qualquer documento digital ou quaisquer dados informáticos*" e que "*simplesmente usou sem autorização* os *dados de acesso genuínos que lhe haviam sido transmitidos pelo ofendido, para aceder* à *sua conta sem autorização deste*",
Sendo sobre estas duas premissas que elabora a sua construção qualificante dos factos objecto do presente inquérito e sendo esta a construção que sustenta a tese do Mmo. Juiz de' Instrução Criminal no sentido de não se verificar, em tese geral a operar exclusivamente no plano subsuntivo dos factos à(s) norma(s) incriminatória(s), é exactamente no patamar das premissas e, em particular, numa delas *("o agente não falsificou qualquer documento digital ou quaisquer dados informáticos"),* que atacamos a posição jurídica e processual por si defendida.
8. No contexto circunstancial (incluindo o espácio-temporal) que enforma a factualidade aqui analisada de modo controvertido, o agente actuou determinando a vítima a, no quadro das disponibilidades do sistema de pagamento MB WAY (o qual constitui um "*sistema informático*", nos termos e para os efeitos da alínea a) do artigo 2.° da Lei do Cibercrime), inscrever no mesmo o seu (do agente) número de telemóvel e um código PIN igualmente por si (agente) indicado.

9. Ora, a conduta do agente concretiza-se com uma "*actuação sobre* o *titular do cartão bancário*" (neste sentido, Alda Fontes, *MBWAYFraude na Utilização: Subsunção Jurídico-Penal de um Caso,* Revista do Ministério Público, 162, Abril/Junho 2020, p.249), instrumentalizando-o em ordem à prossecução e atingimento das suas (agente) finalidades teleologicamente orientadas: obter a possibilidade de acesso à conta bancária da vítima.
10. A antes indicada *actuação sobre* o *titular do cartão bancário* corporiza um fenómeno de instrumentalização da vítima jurídicopenalmente relevante e consubstancia um encadeado estruturado e organizado de actos de manipulação do comportamento da vítima que se materializa e exterioriza no mecânico e heteroorientado cumprimento das indicações do agente.
11.Assim, a vítima, para lá de vítima do crime, é também vítima de um processo de coisificação que a torna um instrumento físico (isto é, material) utilizado pelo agente na prossecução dos seus firmes propósitos.
12. lsto é, o agente, quando de modo contínuo e ordenado e num quadro sequencialmente pré-estruturado, conduz a vítima a viabilizar o seu (do agente) acesso à sua (da vítima) conta bancária num determinado banco está, precisamente com os actos que tal consubstanciam, a praticar, mediatamente, nos termos e para os efeitos do artigo 26.^{0} do Código Penal (leia-se, por via material da objectiva manipulação e mecânica coisificação da vítima, assim transformada em mero objecto instrumental da prática do crime), uma conduta integradora do tipo de crime *falsificação informática,* previsto e punido pelo artigo *3.°,* n.ºs 2 e 3, da Lei Cibercrime, e para o qual o limite máximo da moldura penal é superior a 3 (três) anos.
13. Na verdade, o agente nunca perde o domínio do facto e é por isso que, independentemente de o executor das operações materiais de associação do número de telemóvel e de inserção de um código PIN ser o próprio titular do cartão e não ele, é este (agente) o autor mediato do crime de *falsidade informática.*
14. Relativamente ao indeferimento do requerido quanto ao acesso à facturação detalhada - o MP requereu o acesso a partir de (…) -, também não podemos concordar com a decisão do Mmo. Juiz de Instrução Criminal, o qual despachou favoravelmente o acesso apenas entre os dias (…) e (…), por considerar que "*apenas releva* as *comunicações ocorridas no dia dos factos (…)* e o *dia seguinte (tendo* em *conta que* os *factos* se *situam próximo da meia-noite*."
15. Na verdade, e bem sabendo o Ministério Público que com o requerido procurava assegurar o cumprimento do macro dever de respeitar o equilíbrio constitucional entre direitos, liberdades e garantias circunstancialmente conflituantes num concreto posicionamento histórico, tal decisão do Mmo. Juiz

de Instrução Criminal, aceitando o enquadramento legal do pedido de acesso à facturação detalhada pela sua importância para a descoberta da verdade material, mas restringindo o período admitido para o efeito, penetra num campo de juízo de oportunidade investigatória para cuja formulação é competente o Ministério Público.
16.Competindo ao Ministério Público a direcção da investigação criminal, constituindo os tipos criminais aqui em causa fenómenos criminógenos em acelerado desenvolvimento e sofisticação e atenta a necessidade da sua prevenção por imperativo constitucional -e legal, a limitação do acesso ao dia da prática do facto investigado constituiria uma limitação intolerável à prossecução das finalidades da investigação criminal, com prejuízo, até, no que toca a questões processuais tão elementares como a determinação de conexões processuais (sejam elas subjectivas, sejam elas objectivas).
17. A actuação detectada nos autos, decerto integrada num grupo de pessoas que em concertação de esforços pratica este tipo de, aponta em termos de normalidade para uma actividade continuada, organizada e sistemática, pelo que, no caso dos autos, justifica-se análise da facturação detalhada do telemóvel com o número (…) conforme promovido.
18. Não há combate à prática de factos criminais de modo organizado sem organização da investigação criminal e esta não pode prescindir de nenhum dos meios ao seu dispor no sentido de captar uma fotografia abrangente e homogénea da factualidade que constitui o seu concreto (esquema criminoso).
19. A promovida facturação detalhada do número de telemóvel (…) a partir do dia (…), com listagem das chamadas efectuadas e recebidas, números de chamada/destino e duração das comunicações visa isso mesmo.
20. Por conseguinte, ao decidir como decidiu, o Mmo. Juiz de Instrução Criminal violou o disposto nos violou o disposto nos artigos 3.°, n.º 2, 11.°, 14.°, 18.°, todos da Lei do Cibercrime, e artigos 189.°, nºo 2, 187.°, n.os 1 e 4, alínea a), ambos do Código Processo Penal.

Termos em que, e nos mais de direito, deve ser julgado procedente o recurso interposto pelo Ministério Público e, consequentemente, ser revogado o despacho recorrido que deve ser substituído por outro que determine o acesso aos dados de localização celular do número de telemóvel (…), utilizado pelo agente dos factos, bem como a remessa dos dados de faturação detalhada do número de telemóvel (…), a partir do dia (…), com listagem das chamadas efetuadas e recebidas, números de chamada/destino e duração das comunicações, assim se fazendo JUSTIÇA!
#

Nesta Relação, o Exmo. Procurador-Geral Adjunto emitiu parecer no sentido da procedência do recurso.
Procedeu-se a exame preliminar.
Colhidos os vistos e realizada a conferência, cumpre apreciar e decidir.
III
De acordo com o disposto no art.º 412.º, n.º 1, do Código de Processo Penal, o objecto do recurso é definido pelas conclusões formuladas pelo recorrente na motivação e é por elas delimitado, sem prejuízo da apreciação dos assuntos de conhecimento oficioso de que ainda se possa conhecer.
De modo que as questões postas ao desembargo desta Relação são as seguintes:
1.ª – Se a factualidade indiciada nos autos é ou não susceptível de integrar também a prática de um crime de falsidade informática, p. e p. pelo art.º 3.º da Lei do Cibercrime (Lei n.º 109/2009, de 15-9), podendo assim o M.º P.º requerer o acesso, por força da moldura penal abstracta deste ilícito, à localização celular do número de telemóvel pretensamente usado pelo agente entre 18/03/2020 e a actualidade; e
2.ª – Se, como decidiu o Senhor Juiz de Instrução quanto aos dados de facturação detalhada, apenas relevam as comunicações ocorridas no dia dos factos e no dia seguinte, tendo em consequência apenas determinado que a operadora MEO/ALTICE remetesse aos autos os dados de facturação detalhada do número de telemóvel (…), entre os dias (…) e (…), com listagem das chamadas efectuadas e recebidas, números de chamada/destino e duração das comunicações; ou, como pretende o M.º P.º, esses dados devem antes ser os a partir de (…) até à actualidade.

Vejamos:
No tocante à 1.ª das questões postas:
Comecemos pela parte de se a factualidade indiciada nos autos é ou não susceptível de integrar também a prática de um crime de falsidade informática, p. e p. pelo art.º 3.º da Lei do Cibercrime (Lei n.º 109/2009, de 15-9).
Este preceito legal, sob a epígrafe de *falsidade informática*, estabelece que:
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.
2 - Quando as acções descritas no número anterior incidirem sobre os dados

registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.
3 - Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.
4 - Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.
5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.
Deste texto legal, a parte que nos interessa considerar é a seguinte, a que prevê a punição de:
1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir (...) dados informáticos (...), 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 - Quando as acções descritas no número anterior incidirem (...) em qualquer (...) dispositivo que permita o acesso a sistema ou meio de pagamento, (...) a pena é de 1 a 5 anos de prisão.
3 - Quem, actuando com intenção (...) de obter um benefício ilegítimo, para si ou para terceiro, usar (...) dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.
De acordo com o sumário do ac. TRE de 19-5-2015, proc. 238/12.8PBPTG.E1, www.dgsi.pt, relator António Latas:
1. O tipo objetivo do crime de falsidade informática previsto no nº 1 do artigo 3º da Lei nº 109/2009, de 15 de setembro, é integrado, no plano objetivo, pela introdução, modificação, apagamento ou supressão de dados informáticos ou por qualquer outra forma de interferência num tratamento informático de dados, de que resulte a produção de dados ou documentos não genuínos, consumando-se o crime apenas com a produção deste resultado.
2. Do ponto de vista subjetivo, o tipo legal supõe o dolo, sob qualquer das formas previstas no artigo 14º do Código Penal, exigindo, enquanto elemento

subjetivo especial do tipo, a intenção de provocar engano nas relações jurídicas, bem como, relativamente à produção de dados ou documentos não genuínos, a particular intenção do agente de que tais dados ou documentos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos.
3. O crime de falsidade informática previsto no artigo 3º da Lei nº 109/2009 visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar a confidencialidade, integridade e disponibilidade de sistemas informaìticos, de redes e de dados informáticos.

Ora 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 respectivos cartões (de origem e de destino da quantia em causa). Na aplicação MB WAY, a movimentação de quantias efectua-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.
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, procurando aí identificar pessoas que tenham disponibilizado objectos para venda;
• depois, contacta telefonicamente tais pessoas, manifestando a vontade firme de comprar esses objectos 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.
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.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 efectuar levantamentos em numerário em caixas Multibanco (este é, aliás, um dos casos mais frequentes).(https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/alerta_mbway_2020_04_07.pdf)
O caso indiciado nos presentes autos, obedece também a este figurino.
Por outro lado, os *dados informáticos* mencionados no art.º 3.º da Lei do Cibercrime são expressões gerais que descrevem características das entidades sobre as quais operam algoritmos. A palavra tem origem no latim *datum* (aquilo que se dá), uma informação que permite chegar ao conhecimento de algo ou deduzir as consequências legítimas de um facto, que serve de apoio. Estas expressões devem ser apresentadas de maneira a que possam ser tratadas por computador. Os dados por si só não constituem informação, a menos que esta surja do adequado processamento de dados. A Lei do Cibercrime define também o que são *dados informáticos* para efeitos jurídico-penais no seu art.º 2.º al.ª b), como *qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função*.
Posto isto, temos que, quando o agente convenceu/determinou a ofendida a ir ao Multibanco, indicando-lhe todos os passos que teria de proceder para receber a transferência da venda – introduzir o seu cartão de débito, associar-lhe o número de telemóvel indicado pelo agente e inserir o código de seis dígitos que o agente lhe indicava e o que a ofendida fez de forma automática, porque completamente alheia ao esquema pensado pelo agente –, estava, através de outrem, a introduzir dados num sistema informático que criavam uma autenticação falsa.
Ao ser usada a APP com o correcto código PIN de seis dígitos para efectuar um levantamento de dinheiro, o sistema informático da SIBS reconhece a APP como associada a um determinado cartão de débito, e comunica ao sistema informático do banco onde está sedeada a conta associada ao cartão a quantia

que se pretende levantar e este sistema há-de, ou não, possibilitar o levantamento e/ou montante, após confirmação do respectivo saldo.
Todas estas operações são informáticas e entre sistemas informáticos de diferentes instituições, mas com vista ao mesmo fim – possibilitar a movimentação de dinheiro ou as transacções comerciais de forma rápida e segura.
Quando alguém associa uma APP a um cartão, ao associar-lhe um telemóvel e escolher um PIN, está a criar um documento de «autenticação» no sistema informático do prestador de serviço. Quando o PIN é criado, ele estabelece uma relação de confiança com o prestador do serviço e o utilizador e cria um par de chaves assimétricas usado na autenticação. De modo que, posteriormente, quando se insere o PIN, este tem como função desbloquear a chave de autenticação e usa a chave para assinar a solicitação enviada ao servidor de autenticação.
Ou seja, quando é escolhido o PIN para a aplicação, o utilizador está a produzir um documento de autenticação electrónica com vista a uma finalidade jurídica relevante – o reconhecimento pela SIBS, no seu sistema informático, como pertencendo verdadeiramente ao utilizador do cartão contratado e, em substituição do *car*tão, a possibilidade de realizar – sendo reconhecido pelo sistema como legítimo – todas as funções que a aplicação permite.
Logo, se for introduzido um número de telemóvel que não corresponde ao titular do cartão e inserida uma palavra passe que não foi escolhida pelo titular do cartão, mas por alguém actuando sobre a sua vontade e convencendo-o que o seu procedimento o faria receber dinheiro na sua conta e não o contrário, estará a ser produzido um documento de autenticação electrónica/digital falso.
O que preenche o tipo legal do crime de falsidade informática, p. e p. pelo art.º 3.°, n.° 1 e 2, da Lei do Cibercrime.
E não se diga que assim não pode ser porque quem inseriu os dados foi o próprio titular do cartão.
É que neste caso, ainda que o "executor" das operações de inserção/ associação do número do telemóvel e "escolha"/inserção do PIN seja o próprio titular do cartão, ele não o faz de forma livre e esclarecida, mas sim convencido em erro pelo agente (que actua sobre ele à distância, manipulando a respectiva vontade) de que, ao proceder acriticamente, passo a passo, da forma como lhe é indicada ao telefone, está a dar autorização para que alguém (no caso, o seu interlocutor e alegadamente comprador da produto, que, antes de lhe dar as instruções, se assegurou que o titular do cartão não conhecia o meio de pagamento MB WAY*)*, lhe transfira dinheiro para a conta associada ao

seu cartão.
Trata-se, pois, de um caso de autoria mediata (cf. art.º 26.° do Código Penal), na medida em que o agente determina outrem a praticar os actos de execução necessários à consumação do mesmo, sem nunca perder o domínio do facto, para o que necessitava que outra pessoa, no caso o próprio titular do cartão, praticasse determinados actos: introdução do seu cartão de débito na ranhura da caixa *Multibanco* e a inserção do PIN do seu cartão e, de seguida, através da associação do número do telemóvel e do código PIN que lhe são facultados pelo agente, criasse uma autenticação de uma aplicação sua a um cartão alheio como se fosse o próprio utilizador autorizado do cartão – o que é falso.
Assim, temos que o agente/autor mediato:
a) Criou um documento falso – autenticação da aplicação *MB* WAY na SIBS, inserindo dados no sistema informático – número de telefone e PIN – (elemento objectivo do tipo), associando-a a um determinado cartão de débito (através da introdução/utilização do PIN do cartão), que não lhe pertencia, mas que, a partir deste acto, passa a ser reconhecido como se lhe pertencesse – com o que cria uma "assinatura digital" falsa;
b) Sendo que o fez através de manipulação do titular do cartão, determinando-lhe a prática dos actos de execução, que este executou automaticamente e sem juízo crítico, convencido que estava a consentir coisa completamente diversa (que seria receber dinheiro da venda que estava ciente ter acabado de efectuar);
c) Com intenção de provocar engano nas relações jurídicas (elemento subjectivo especial do tipo) – criar a convicção no sistema informático da SIBS que o utilizador da aplicação MB WAY é o mesmo utilizador, legítimo, do cartão de débito;
d) E com intenção (dolo/elemento subjectivo) de que estes sejam considerados ou utilizados para finalidades jurídicas relevantes – efectuar operações financeiras/transacções, todas as ordens de levantamento e/ou transferência que venham a ocorrer através daquela aplicação – que serão aceites como válidas como sendo emitidas pelo próprio titular do cartão de débito.
De facto, o crime de falsidade informática está consumado com a validação da aplicação – através do método *supra* descrito.
E, tratando-se de um crime de perigo abstracto, pode até acontecer que através daquela aplicação nunca se venha a processar qualquer operação bancária que venha a produzir prejuízo económico ao ofendido. Efectivamente, o crime de falsidade informática visa proteger o bem jurídico fiabilidade dos documentos no tráfico jurídico probatório (onde se inclui a segurança nas transacções electrónicas) e, reflexamente, a integridade dos sistemas informáticos.

Trata-se aqui de uma interferência no tratamento de dados informáticos, no sentido de influenciar o modo desse tratamento, a fim de o mesmo não ocorrer do modo como, sem a actuação do agente, ocorreria.
Neste caso, com a integração dos dados informáticos no sistema informático – criar a autenticação (*input)* –, o programa instalado no sistema informático não é alterado, apenas trabalhará com dados falsos e, por isso, o tratamento dos dados daí decorrente – ao utilizar posteriormente a aplicação – vai gerar um resultado falso – uma ordem dada por quem não tinha legitimidade para o fazer – pelo que a ordem que venha a ser gerada pela utilização (*output)* – também será falsa porque houve falsificação dos dados integrados (o número de telemóvel e o PIN da aplicação não pertencem ao utilizador do cartão de débito).
(Cf. Alda da Conceição Costa Fontes, *MB WAY – Fraude na Utilização. Subsunção Jurídico-Penal de um Caso*, Revista do Ministério Público, 162, Abril/Junho 2020, p. 250 e ss. – que temos vindo a seguir de perto).
Uma última nota para referir que se a burla informática, p. e p. pelo art.º 221.º, do Código Penal, se realizou mediante a introdução de dados incorrectos/falsos no sistema informático da aplicação MB WAY por um autor mediato que para tanto convence a vítima, correspondendo, pois, ao cometimento pelo agente mediato do crime de falsidade informática, p. e p. pelo art.º 3.º, n.º 1 e 2, da Lei do Cibercrime, existe concurso efectivo entre aquela burla e esta falsidade informática, como também já o decidiu o Ac. TRP de 14-9-2016, proc. 2177/09.0PAVNG.P1, www.dgsi.pt,
Na verdade, dada a similitude daqueles ilícitos com os crimes de burla, p. e p. pelos art.º 217.º e 218.º do Código Penal, e de falsificação de documento, p. e p. pelo art.º 256.º, do Código Penal, necessariamente temos por boa a argumentação usada no Acórdão Uniformizador de Jurisprudência n.º 10/2013, de 5-6-2013, concluindo pela verificação de concurso real entre as normas incriminadoras, pois que também os crimes destes autos – burla informática, p. e p. pelo art.º 221.º, do Código Penal, e falsidade informática, p. e p. pelo art.º 3.º Lei n.º 109/2009, de 15-9 (Lei do Cibercrime) – tutelam bens jurídicos de diversa natureza: no da burla informática, visando-se, essencialmente, proteger o património e, no de falsidade informática, a protecção não do património, mas, sim, da integridade dos sistemas de informação, através do qual se pretende impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas de redes e dados.
Pois que, se é certo que a falsificação pode constituir o meio, o artifício fraudulento, que está no cerne da burla, igualmente é exacto que, na

comparação dos dois tipos, existe uma bipolaridade de bens jurídicos protegidos, o que aliás se revela na sua diferente natureza (pública no caso da falsidade informática e semi-pública no caso da burla informática *simples* p. e p. pelo art.º 221.º, n.º 1, 2, 3 e 4, do Código Penal), reflectindo tal diversidade. Consequentemente, à pluralidade de tipos legais integrados deve corresponder uma pluralidade de crimes.

Aqui chegados, temos assim como removido o obstáculo apontado pelo Senhor Juiz de Instrução Criminal ao pedido do M.º P.º para que no âmbito da presente investigação lhe sejam fornecidos os dados referentes à localização celular do número de telemóvel pretensamente usado pelo agente.
Assim, verificados que estão os requisitos apontados pelos art.º 3.º, n.º 1 e 2, 11.º e 18.º, da Lei n.º 109/2009, de 15-9 (Lei do Cibercrime), e 189.º, n.º 2 e 187.º, n.º 1 e 4 al.ª a), do Código de Processo Penal, impõe-se que o Senhor Juiz de Instrução Criminal defira a mencionada pretensão do M.º P.º, ordenando em consonância com a mesma.
Mas não sem antes delimitarmos o período temporal durante o qual perdurará aquela localização celular do número de telemóvel pretensamente usado pelo agente, que a Digna Magistrada do M.º P.º recorrente pretendia fosse a partir do dia (…) até à actualidade – problemática temporal que entronca a final na da questão seguinte, a de estabelecer o lapso de tempo pelo qual perdurará a também pretendida facturação detalhada do número de telemóvel usado pelo agente e será, pois, estabelecida em conjunto e por período idêntico.
#
No tocante à 2.ª das questões postas no recurso, a de se, como decidiu o Senhor Juiz de Instrução quanto aos dados de facturação detalhada, apenas relevam as comunicações ocorridas no dia dos factos e no dia seguinte, tendo em consequência determinado que a operadora MEO/ALTICE remetesse aos autos os dados de facturação detalhada do número de telemóvel (…), apenas referente aos dias (…) e (…), com listagem das chamadas efectuadas e recebidas, números de chamada/destino e duração das comunicações; ou, como pretende o M.º P.º, esses dados devem antes ser os a partir de (…) até à actualidade.
A questão posta (tal como a do período temporal durante o qual perdurará a localização celular do número de telemóvel pretensamente usado pelo agente) reclama sejam tecidas algumas considerações sobre a problemática da obtenção dos meios de prova em processo penal, em particular no que respeita a escutas telefónicas e acesso a dados sobre comunicações por tal via, tendo presente, em primeira linha, o quadro constitucional que essa obtenção deve respeitar.

Estatui o art.º 18.º da Constituição da República Portuguesa (CRP) que:
1. Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas.
2. A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.
(…).
No art.º 26.º, prescreve a Lei Fundamental:
1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada a familiar (…).
2. A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.
(…).
Sob a epígrafe «*Garantias do processo criminal*», o art.º 32.º da CRP preceitua:
1. O processo criminal assegura todas as garantias de defesa, incluindo o recurso.
(…)
8. São nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.
No art.º 34.º, sob a epígrafe *Inviolabilidade do domicílio e da correspondência*, a CRP garante que
1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.
(…)
4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicações, salvos os casos previstos na lei em matéria de processo criminal.
Na lição de Gomes Canotilho e Vital Moreira[1], as normas contidas no art.º 18.º da CRP, integrando o essencial do regime constitucional específico dos direitos, liberdades e garantias, condensam princípios fundamentais de uma *doutrina geral de direitos, liberdades e garantias constitucionalmente adequada*, especificando o n.º 1 a *força normativa* de todos os preceitos constitucionais referentes a direitos, liberdades e garantias, enquanto os n.ºs

2 e 3 estabelecem o *estatuto global das leis restritivas*, individualizando os princípios constitucionais heteronomamente vinculativos das intervenções do legislador na esfera dos direitos, liberdades e garantias.
Este regime próprio dos direitos, liberdades e garantias é caracterizado, em primeira linha, pela *(a)* eficácia imediata e de aplicação directa das normas que lhe dão corpo (n.º 1) – os preceitos constitucionais respeitantes aos direitos liberdades e garantias não carecem de mediação, desenvolvimento ou concretização legislativa para serem aplicáveis, aplicando-se mesmo na *ausência de lei*; por outro lado, as leis que infrinjam as normas respeitantes a direitos, liberdades e garantias são inválidas, caso em que são aplicáveis, *contra a lei* e *em vez da lei*, essas normas; depois, porque *(b)* as normas do regime próprio dos direitos, liberdades e garantias vinculam as entidades públicas (ao Estado, enquanto legislador, está vedado emitir normas incompatíveis com os direitos fundamentais, sob pena de inconstitucionalidade; na esfera de competência dos tribunais inscreve-se constitucionalmente o direito e o dever de fiscalização da constitucionalidade das leis, *desaplicando-as*, sempre que estiverem em contradição com as normas constitucionais) e também, e imediatamente, as entidades privadas (porque também sujeitas a um *dever* de não perturbar ou impedir o exercício de direitos fundamentais), pelo que, com propriedade, se pode afirmar que às normas de «direitos, liberdades e garantias» é inerente uma eficácia geral, *erga omnes*.
Mas este regime específico dos «direitos, liberdades e garantias» não veda a possibilidade de restrição, por via de lei, do exercício dos direitos, liberdades e garantias; todavia, para que sejam constitucionalmente legítimas, tais restrições devem, cumulativamente, ser expressamente admitidas (ou, eventualmente, impostas) pelo próprio texto constitucional (n.º 2, 1.ª parte), visar a salvaguarda de outro direito ou interesse constitucionalmente protegido (n.º 2, *in fine*), que a restrição seja exigida por essa salvaguarda, apta para o efeito e se limite à medida necessária para atingir esse objectivo (n.º 2, 2.ª parte), e não aniquile o direito em causa atingindo o conteúdo essencial do respectivo preceito (n.º 3, *in fine*).
Para além da verificação destes *pressupostos materiais*, a validade das leis restritivas de direitos liberdades e garantias reclama ainda a observância de três *requisitos* quanto ao carácter da própria lei: a lei deve revestir carácter geral e abstracto (n.º 3, 1.ª parte), não pode ter efeito retroactivo (n.º 3, 2.ª parte) e tem de emanar da Assembleia da República ou, ao menos, revestir a forma de decreto-lei autorizado.
O primeiro pressuposto material de legitimidade das restrições ao exercício de direitos, liberdades e garantias traduz-se na exigência de previsão

constitucional expressa dessa mesma restrição, ou seja, é necessário que a admissibilidade da restrição encontre no texto constitucional *expressão suficiente e adequada*, seja essa restrição directamente prevista pela Constituição ou criada pela lei ordinária porque admitida pela Constituição.
O segundo pressuposto material de legitimidade das restrições àquele exercício decorre da circunstância de a restrição só poder encontrar justificação para salvaguarda de um outro direito ou interesse constitucionalmente protegido, o que significa que o sacrifício, ainda que parcial, de um direito fundamental não pode ser arbitrário, gratuito, desmotivado.
O terceiro pressuposto material para a restrição legítima de direitos, liberdades e garantias consiste no chamado princípio da proporcionalidade ou *princípio da proibição do excesso*, que se decompõe em três subprincípios: *(a) princípio da adequação*, isto é, as medidas restritivas legalmente previstas devem revelar-se como meio adequado à prossecução dos fins visados (salvaguarda de outros direitos constitucionalmente protegidos); *(b) princípio da exigibilidade*, que significa que as medidas restritivas previstas na lei devem revelar-se necessárias, pois os fins por ela visados não podiam ser obtidos através de outros meios menos onerosos para os direitos, liberdades e garantias; e *(c) princípio da proporcionalidade* em sentido estrito, isto é, os meios legais restritivos e os fins obtidos devem situar-se numa «justa medida», assim se impedindo a adopção de medidas legais restritivas desproporcionadas e excessivas em relação aos fins obtidos.

Vem isto a propósito da questão da fixação do período temporal pelo qual deve perdurar a informação da facturação detalhada, bem como a da localização celular, a fornecer pela operadora MEO/ALTICE do número de telemóvel presumivelmente pertencente ao agente dos ilícitos indiciados nos presentes autos.
Se referente apenas aos dias (…) e (…), como concedeu o Senhor JIC; se a partir de (…) até à actualidade, como pretende o M.º P.º.
Ora bem.
Pretender informação da facturação detalhada e da localização celular a partir de (…) até à actualidade é um manifesto e insuportável exagero, por violar os princípios da adequação e proporcionalidade acima mencionados.
Depois, que a facturação detalhada e a localização celular o sejam dos dias (…) e (…) percebe-se, por através delas se poder estabelecer a ligação entre o telemóvel usado pelo agente e o da ofendida e a competência territorial da comarca para a investigação e eventual julgamento.
Mas já não vemos qual seja a real utilidade em relação à facturação detalhada

e à localização celular da semana ou do mês ou meses a seguir, uma vez que a Digna Magistrada do M.º P.º recorrente não revela em seu recurso ter em investigação qualquer lista de números telefónicos de ofendidos que tenham sido contactados para fins ilícitos idênticos pelo n.º de telemóvel agora investigado e em relação aos quais também importasse estabelecer correlação.
De modo que improcederá o recurso na parte em que se pretendia que tais informações fossem pela operadora prestadas para além dos dias 18 e 19/03/2020.
IV
Termos em que, concedendo parcial provimento ao recurso, se decide:
1.º
Revogar o despacho recorrido na parte em que negou ao M.º P.º o acesso aos dados de localização celular do número de telemóvel 96 401 84 36, pretensamente usado pelo agente.
2.º
Estabelecer que os dados de localização celular e os de facturação detalhada de tal telemóvel se reportam aos dias (…) e (…).
3.º
Ordenar que o Senhor Juiz de Instrução Criminal, em consequência, determine à operadora MEO/ALTICE remeta aos autos os dados de localização celular e de facturação detalhada do número de telemóvel (…), referente aos dias (…) e (…), com listagem das chamadas efectuadas e recebidas, números de chamada/destino e duração das comunicações.
4.º
Não é devida tributação.
#
Évora, 25-5-2021
Martinho Cardoso, relator
Maria Leonor Esteves, adjunta
(assinaturas digitais)

---

[1] - Constituição da República Portuguesa Anotada, 3ª edição revista, Coimbra Editora, 1993, pp. 144 e sgs., aqui seguida de muito perto.