MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

Nota Informativa
CIBERCRIME:
DENÚNCIAS RECEBIDAS
2025

gabinete cibercrime
fevereiro 2026

cibercrime@pgr.pt
http://cibercrime.ministeriopublico.pt/

ÍNDICE

CIBERCRIME:
DENÚNCIAS RECEBIDAS
2025

A. O CONTEXTO - CIBERCRIME

1. Em termos coloquiais, a expressão *cibercrime* agrega modernamente muito mais ilícitos do que aqueles que se descrevem na Lei do Cibercrime[1] (Lei nº 109/2009), estendendo-se ao Código Penal[2] e a outras fontes legais[3], incluindo numerosas manifestações criminógenas que antes apenas se praticavam de forma presencial e na atualidade migraram para o ambiente digital. É, por exemplo, o caso dos crimes contra a honra ou os crimes relacionados com o discurso de ódio. Mas é, sobretudo, o caso, que muito se tem avultado nos anos mais recentes, das inúmeras modalidades de burlas em contexto digital, nas diversas plataformas e canais de comunicação *online*.

2. As estatísticas da Justiça, que contabilizam as investigações segundo os tipos legais de crime (burlas, injúrias, difamações...), não considerando autónoma ou separadamente aqueles que ocorrem *online*, não permitem a quantificação estatística rigorosa desta realidade criminal. Esta particularidade torna crescentemente mais difícil conhecer verdadeiramente a criminalidade que ocorre por vias das redes de comunicações.
Não sendo possível avaliar com rigor estatístico a real dimensão deste fenómeno, o Gabinete Cibercrime da Procuradoria-Geral da República tem procurado aperceber o respetivo significado, recorrendo às denúncias que recebe por via da linha de correio eletrónico do gabinete (cibercrime@pgr.pt) que, não representado todas as denúncias apresentadas no território nacional, são um importantíssimo indicador destes fenómenos.

B. O PROCESSO DE RECEBIMENTO DE DENÚNCIAS

3. O endereço cibercrime@pgr.pt tem sido utilizado pelos cidadãos para remeter ao Ministério Público denúncias relevantes para efeitos de processo penal. Como o Gabinete Cibercrime não tem atribuições funcionais de direção da investigação criminal, após uma triagem das mesmas, são remetidas para abertura de inquérito aquelas que reúnem as condições para o efeito[4]. Quanto às restantes, os seus

[1] Falsidade informática (e as suas diversas modalidades respeitantes a meios de pagamento não corpóreo), dano informático, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido.
[2] Designadamente a burla informática e a pornografia infantil.
[3] Por exemplo, os ilícitos criminais relacionados com a proteção de dados pessoais.
[4] Fixaram-se critérios de análise destas queixas, que passam pela verificação das condições formais suficientes para abertura de uma investigação. Por exemplo, não são encaminhadas para inquérito as mensagens que reportem crimes meramente tentados por desconhecidos, ou atos preparatórios, ou crimes de natureza particular, ou crimes de natureza semipública, que não contenham informação que permita cabalmente identificar o titular do direito de queixa, ou quando o seu autor não manifesta vontade de procedimento criminal. O mesmo sucede com denúncias anónimas ou remetidas por pessoas que não se identificam (ou que não seja legal ou tecnicamente possível identificar) e com denúncias que descrevam factos vagos, ou genéricos, ou meras suspeições da prática de crimes.

remetentes são informados da possibilidade legal de apresentação de queixa formal. Uma pequena parte destas denúncias é encaminhada para a Polícia Judiciária, quando não se justifica a imediata abertura de inquérito, mas ainda assim, a informação é relevante para eventuais investigações pendentes ou para melhor identificação de procedimentos ou fenómenos criminosos.

C. AS DENÚNCIAS RECEBIDAS

4. As denúncias de *cibercrimes* em sentido alargado recebidas por via de correio eletrónico pelo Gabinete Cibercrime aumentam persistentemente, de forma consistente, de ano para ano, desde 2016.

No ano de 2020 as denúncias aumentaram de forma excecional, após a eclosão da pandemia resultante da COVID – 19. Em 2021 o aumento foi ainda mais expressivo, mais que duplicando os valores do ano anterior. Depois disso, o crescimento anual foi ajustando e estabilizando, mantendo sempre porém uma clara e consistente tendência ascendente.

No ano de **2025** foram recebidas **4497 denúncias**, o que significa um **aumento de 13,16%** em relação a 2024 (ano durante o qual foram recebidas 3973 denúncias).

Delas, **1059** foram remetidas para abertura de **inquérito**.

Denúncias em **2019:**
193
Denúncias em **2020:**
544
Denúncias em **2021:**
1160
Denúncias em **2022:**
2124
Denúncias em **2023**:
2916
Denúncias em **2024**:
3973
Denúncias em **2025**:
4497

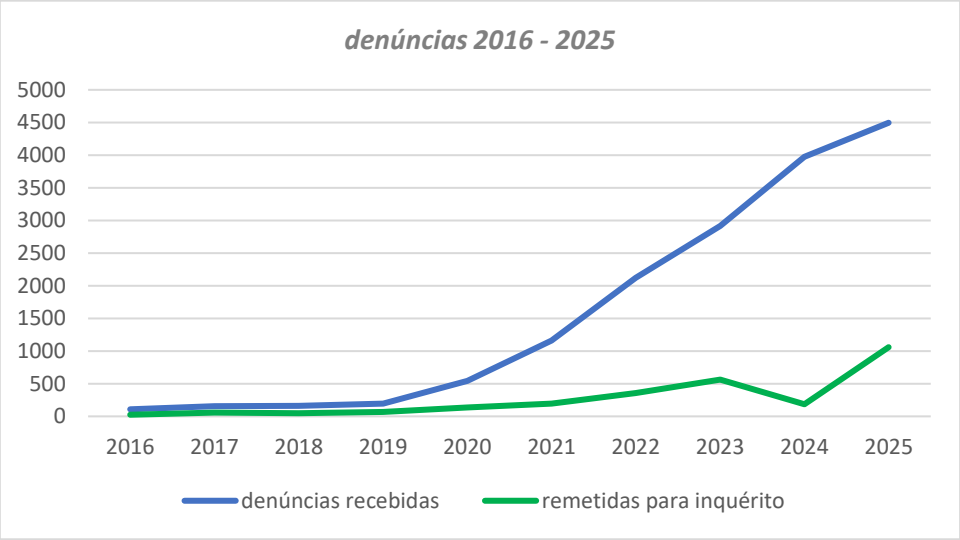
5. Portanto, tal como vem acontecendo há quase uma década, no ano de 2025 receberam-se muitas mais denúncias do que se tinham registado no ano imediatamente anterior. Neste ano mais uma vez se verificou que, como nos anos que o antecederam, este é um fenómeno em permanente expansão, continuando a observar-se, de ano para ano, um grande acréscimo das denúncias recebidas.

Mantém-se a tendência de consistente subida no número de denúncias. Não se trata somente de um número maior de denúncias, de ano para ano. Há claros sinais de persistente aumento das denúncias, reveladores de crescimento contínuo e regular do fenómeno. Como se referiu, no ano de 2024 foram recebidas por correio eletrónico 3973 denúncias. Portanto, em média, foram recebidas 331 denúncias em cada mês (mais que 10 por dia). Em 2023 tinham sido recebidas 2916 denúncias, portanto 243 denúncias por mês. Em 2025 foram recebidas 4497 denúncias, correspondendo a 375 denúncias por mês.

6. Os números constantes da tabela seguinte, visualmente representados no gráfico que se lhe segue, reforçam a conclusão que acima se formulou e ilustram claramente a progressão do cibercrime de ano para ano. Tal como em anos anteriores se antevia já, verifica-se que embora a pandemia da COVID-19, em 2020 e 2021, tenha impulsionado o aumento deste tipo de criminalidade, esta tendência crescente afigura-se constante e consistente, alheia à ultrapassagem da pandemia. No quadro e no gráfico que seguem indicam-se as denúncias recebidas em cada ano, desde 2016. Descrevem-se também as denúncias que, de entre o conjunto total, foram remetidas para inquérito.

denúncias 2016 – 2025

Ano	denúncias recebidas	remetidas para inquérito
2016	108	25
2017	155	59
2018	160	50
2019	193	67
2020	544	138
2021	1160	195
2022	2124	359
2023	2916	563
2024	3973	187
2025	4496	1059



7. Estes números revelam uma progressão constante e persistente do número de queixas recebidas no decurso dos anos: embora com oscilações, registou-se sempre, de um ano para outro, sem exceções, um aumento do número de denúncias.

Importa sublinhar que o **crescimento registado, de 13,16%** (4497 denúncias em 2025, contra as 3973 denúncias em 2024), ignifica já algum ajustamento. Como se referiu, o período pandémico de 2020/2022 impôs uma enorme e súbita *digitalização* da vida das pessoas, da economia e das instituições, a qual trouxe também uma proliferação enorme das atividades ilícitas a este respeito.

entre 2024 e 2025 as denúncias de cibercrime aumentaram 13,16%

Porém, desde então, embora progredindo, de ano para ano, o crescimento da criminalidade tem vindo a ajustar-se, consoante se vêm também multiplicando as diversas campanhas de prevenção e se têm incrementado a consciencialização social a este respeito e a literacia digital.

Enquanto em 2020 o aumento da cibercriminalidade foi de 88% e em 2021 foi de 113%, nos anos seguintes, o crescimento abrandou. Em 2022 passou a 73,58% e em 2023 e 2024, foi de 37,29% e de 36,25%, respetivamente.

Pode portanto dizer-se que o cibercrime não é um fenómeno em crescimento descontrolado, mas antes uma realidade que se expande na mesma medida em que progride o processo de digitalização.

8. Faz-se ainda uma breve referência às denúncias que, de entre as muitas recebidas, foram encaminhadas para abertura de inquérito. Verificou-se no decurso de 2025, tendo como referência os anos anteriores, um enorme aumento do número de denúncias que mereceram este destino.

Em 2024 tinha sido remetido para inquérito um número extraordinariamente baixo, de apenas 4,70 % das denúncias (por motivos específicos,[5] os quais na altura se aperceberam). Agora, em 2025, foram remetidas para inquérito 1059 do total das 4496 denúncias recebidas, correspondendo a 23,56% das mesmas – portanto, um aumento de 566,31%, em relação a 2024.
Trata-se de um volume nunca anteriormente verificado, resultante da peculiar circunstância de, no decurso do ano de 2025, terem sido recebidos alguns conjuntos de denúncias, todas elas de teor muito similar, pelos mesmos factos e contra os mesmos denunciados, mas provenientes de uma enorme diversidade de centenas de denunciantes. Ficou a impressão de que um conjunto de algumas centenas de cidadãos se articularam entre eles com o intuito de apresentarem, todos e cada um deles, em separado, a mesma denúncia contra a mesma pessoa (no caso, três pessoas diferentes), pelos mesmos factos (na verdade, três conjuntos factuais diferentes). Estas denúncias (no seu conjunto, 842), todas elas apresentadas em separado, vieram a ser canalizadas para três diferentes inquéritos[6], no DIAP de Lisboa.
Se se deduzirem estas 842 participações do conjunto das 1059 que foram remetidas para inquérito, conclui-se que o conjunto das restantes (217), é apenas um pouco superior ao número (de 187) que foi remetido em 2024. Isto é, deduzidos aqueles três conjuntos pontuais de denúncias remetidas para inquérito, o aumento real de 2024 para 2025 foi de 16% - coerente com o aumento geral das denúncias recebidas, que foi de 13,16%, como acima se disse.

9. Todas estas denúncias, recebidas por correio eletrónico pelo Gabinete Cibercrime, são apenas uma amostra do conjunto total das denúncias de cibercriminalidade apresentadas pelos cidadãos ao Ministério Público. Por isso, embora sejam indicadores reais, permitindo que delas se infiram as grandes linhas dos *cibercrimes* que vitimam os portugueses, não permitem gerar dados estatísticos rigorosos.

D. CRIMINALIDADE MAIS FREQUENTE

10. Tal como vem acontecendo desde 2023 e 2024, o ano de 2025 foi marcado pela continuada expansão dos chamados fenómenos criminais de "*massas*", isto é, do desenvolvimento de sucessivas campanhas criminosas específicas, desenvolvidas por grupos de crime organizado. Trata-se de iniciativas dirigidas simultaneamente a um muito grande número de vítimas, na esperança de que algumas delas *caiam* no logro. São exemplos destas iniciativas criminosas as campanhas de burlas do tipo conhecido como "*olá mãe, olá pai*", ou de burlas relacionadas com o pagamento de falsas dívidas.

11. Tal como vem acontecendo desde há anos, muitas das mensagens de denúncia recebidas pelo Gabinete Cibercrime não podem verdadeiramente qualificar-se como participações criminais por não reunirem minimamente os respetivos requisitos: são vagas, apenas descrevem genericamente factos criminais, meramente encaminham suspeitas, não identificam vítimas ou agentes criminais, vêm de endereços que não permitem a identificação de quem as subscreve. Nalguns casos não chega a ser visível o intuito de procedimento criminal. Não obstante, todos os remetentes destas mensagens têm sido informados da possibilidade legal de apresentação de queixa formal.
Em 2025 foram recebidas 494 mensagens que se integram neste conjunto, as quais, aludindo vagamente a um crime, não só não reuniam objetivamente as condições mínimas para remessa para investigação como também, por outro lado, não permitiam identificar minimamente a factualidade que pretendiam denunciar. Neste contexto e com o mesmo perfil, ainda foram recebidas mais 4 mensagens a que não

[5] Pode encontrar-se explicação detalhada dos respetivos motivos, aqui: https://cibercrime.ministeriopublico.pt/sites/default/files/2025-03/2025.03.18-denuncias-de-cibercrime-2024.pdf.
[6] Para o inquérito 3957/25.5T9LSB, foram canalizadas 678 das queixas, para o inquérito NUIPC 4268/25.1T9LSB, foram canalizadas 51 e, por último, para o inquérito NUIPC 4889/25.2T9LSB, foram remetidas 113 das denúncias.

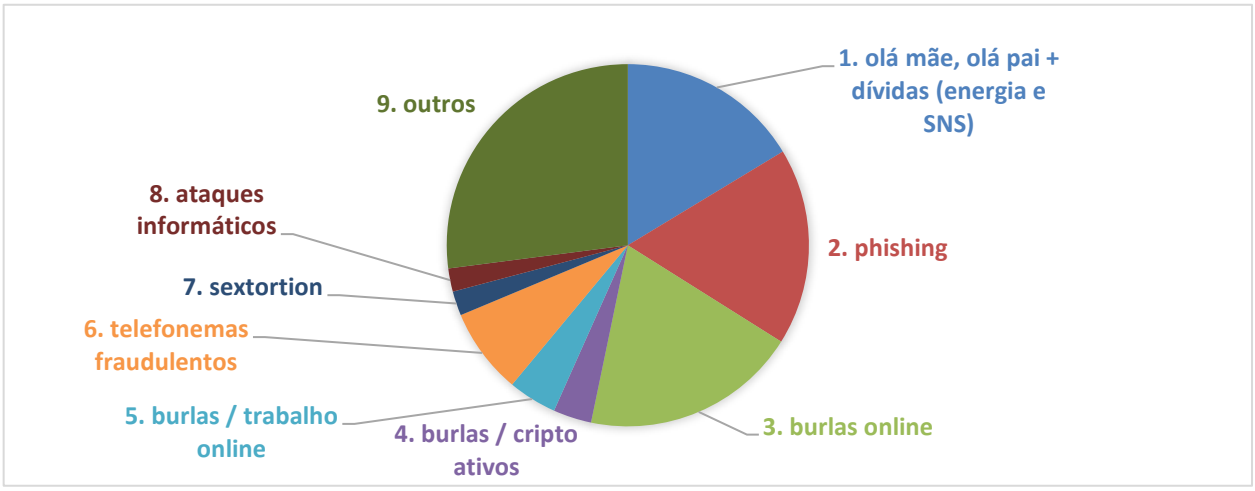
foi dada sequência, por serem denúncias anónimas e não reunirem suficientemente os requisitos que determinassem a abertura de inquérito.

12. Por outro lado, continuaram em 2025 a receber-se um conjunto de mensagens que unicamente pretendiam chamar a atenção para denúncias que os remetentes apresentaram por via de outros canais (em órgãos de polícia criminal ou noutros departamentos do Ministério Público), reforçando a mesma. Durante este ano foram recebidas 47 mensagens deste tipo.
Para se aperceber verdadeiramente o significado dos fenómenos sobre os quais versa esta Nota, e que de seguida vão descrever-se, na respetiva análise e contabilização, optou-se por se deduzirem estes três grupos de mensagens (494 + 4 + 47, ou seja, 545). Por conseguinte, nas considerações e ponderações que de seguida se seguem toma-se como indicador o valor de 3952 (portanto, deduzindo as 545 denúncias inconsistentes ao total de 4497 denúncias recebidas).

13. Descrevem-se na tabela e no gráfico que seguem os fenómenos criminais mais significativos, agrupados por tipologias.
Na categoria 1 ("*olá mãe, olá pai + dívidas energia e SNS*"), incluíram-se as denúncias estritamente respeitantes a estes dois tipos de defraudação, que partilham entre eles a metodologia. Na categoria 2 ("*phishing*"), descrevem-se as diversas abordagens criminosas denunciadas que tinham o propósito de obter dados bancários – designadamente de cartões bancários de pagamento. Quanto às categorias 3 a 5, incluíram diferentes tipos de "*burlas online*": nas categorias 4 ("*cripto ativos*") e 5 ("*trabalho online*") autonomizam-se duas modalidades particulares de burla que se destacam pelo significado estatístico e pelo enorme prejuízo patrimonial a que dão origem, sobretudo em vítimas desempregadas e de poucos recursos económicos. Na categoria 6 ("*telefonemas fraudulentos*") incluem-se os casos de uma muito incisiva iniciativa criminal, com recurso a engenharia social. O mesmo ocorre com o fenómeno cujos dados se incluem na categoria 7 (designadamente a "*sextortion*"). Na categoria 8 (*ataques informáticos*) incluem-se diversos fenómenos, tais como o *ransomware*, acessos ilegítimos ou a obtenção ilegítima (impropriamente referida como *furto*) de credenciais de acesso a contas. Finalmente, deixou-se a categoria 9 ("*outros*") para as restantes modalidades de crimes denunciados – neles se incluem, entre muitas outras, as denúncias de crimes contra a honra.

1. olá mãe + dívidas energia e SNS	646
2. *phishing*	695
3. burlas *online*	764
4. burlas / cripto ativos	135
5. burlas / trabalho *online*	172
6. telefonemas fraudulentos	303
7. *sextortion*	86
8. ataques informáticos	82
9. outros	1069

Nesta tabela não se incluíram as 545 denúncias referidas no antecedente ponto 12.



"*olá mãe, olá pai*" e falsos pagamentos de dívidas

14. Como acima se referiu, têm vindo a intensificar-se, desde 2023, campanhas criminosas na área dos chamados *crimes de massas*. Trata-se de fenómenos resultantes da atividade de grupos criminosos organizados que utilizam meios tecnológicos avançados para atingir, simultaneamente, uma enorme multiplicidade de vítimas.
Em muitos casos, os destinatários destas iniciativas criminosas identificaram facilmente a natureza fraudulenta das mensagens; noutros, convencidos pela argumentação utilizada nas mensagens criminosas, acederam aos seus intuitos, procedendo a pagamentos indevidos, ficando assim economicamente lesados. De anos anteriores, persistiram as burlas conhecidas como "*olá mãe, olá pai*" e as burlas relacionadas com o pagamento de falsas dívidas (contas de energia elétrica, de gás, de portagens de autoestradas). Já durante o ano de 2025, surgiu uma nova modalidade de burlas, relacionada com o pagamento de falsas dívidas ao Serviço Nacional de Saúde. Foi a este propósito emitido, a 19 de agosto de 2025, um novo Alerta Cibercrime. Já em anos anteriores tinham sido emitidos a este respeito os Alertas Cibercrime de 23 de março de 2023 e de 3 de maio de 2023.

15. Todas estas iniciativas criminosas utilizam o mesmo tipo de método e abordagem: os agentes criminosos expedem milhares de mensagens, sobretudo via WhatsApp, mas também por SMS, na esperança de que as vítimas, inadvertidamente, procedam aos pagamentos que solicitam.

16. Este conjunto de práticas criminosas é dos mais numerosos, uma vez que foram recebidas **646 denúncias** desta natureza (correspondendo a **481** burlas do tipo "***olá mãe, olá pai***", **100** denúncias de supostas **dívidas ao Serviço Nacional de Saúde** e **65** de supostas **dívidas respeitantes a energia elétrica**. No seu conjunto, estas 646 denúncias correspondem a **16,46 % do total** das 3952 denúncias.
Trata-se de burlas de *argumentário* muito elementar, cuja existência e disseminação tem aliás sido publicamente muito difundida. Não obstante, continuam a registar-se com muita frequência, razão pela qual tem que concluir-se que os intentos dos agentes criminosos continuam a ser compensadores.
Apesar disso, quanto às burlas do tipo "*olá mãe, olá pai*", assistiu-se a uma ligeira diminuição: em 2022 tinham sido recebidas 65 denúncias, que em 2023 passaram para 227. Em 2024 o conjunto destas burlas foi o mais numeroso: 696 denúncias. Porém, como se referiu, em 2025 foram recebidas 481 denúncias, antevendo-se assim que se atingiu já o auge desta prática criminosa, que estará em regressão.

17. Quanto às denúncias respeitantes a falsas reclamações de dívidas, alegadamente respeitantes a **contas de eletricidade** (surgiram também, apesar de menos, burlas respeitantes a dívidas de outros serviços, como o fornecimento de gás ou água), embora continuando a ocorrer de forma significativa, mantiveram-se em queda.
Recorda-se que este fenómeno foi identificado a partir do 2022, ano durante o qual foram recebidas 29 denúncias deste tipo. Em 2023 vieram a ser recebidas 381 denúncias mas em 2024 já foram apenas recebidas 246. Em 2025 foram somente recebidas 65. Também no decurso do próprio ano de 2025 se anotou uma quebra: no segundo semestre apenas foram registadas 23 denúncias, enquanto no primeiro tinham sido 42. Parece pois que, embora continuando ativo, este fenómeno parece estar em declínio.

18. Este declínio pode ter dado origem ao surgimento de burlas com novas "roupagens", invocando dívidas ao Serviço Nacional de Saúde, como já acima referido, as quais foram identificadas a partir de meados do verão de 2025. Como se disse, no decurso deste ano foram recebidas 100 denúncias deste tipo.

Já muito no final do ano de 2025 veio a ser identificado um novo tipo de burla desta natureza, invocando falsas dívidas à Segurança Social. Esta modalidade veio apenas a ganhar expressão já nos primeiros dias de 2026.

phishing

19. O ***phishing*** partilha com os métodos anteriores o modelo da abordagem à vítima: a expedição para milhares de destinatários de mensagens fraudulentas. Em 2023 tinham sido recebidas 326 denúncias desta natureza e em 2024 foram recebidas 489. Agora, em **2025**, foram **recebidas 695**, correspondendo a **17,59 %** das 3952 denúncias recebidas.

em 2025 as denúncias de *phishing* (dados de cartões de pagamento) aumentaram 42,15 %

Além do significado deste fenómeno, no contexto da cibercriminalidade em geral, sublinha-se que, entre 2024 (489 denúncias) e 2025 (695 denúncias), o **aumento foi de 42,15 %.** No ano anterior, de 2024, o aumento em relação a 2023, tinha sido de 50% (de 326 denúncias em 2023 para 489 em 2024).

Tal como em 2024, no decurso de 2025, continuaram a suceder-se inúmeras e diversas campanhas de *phishing*, usando variadas imagens institucionais (dos CTT - Correios, da Autoridade Tributária, da Via Verde, da Caixa Geral de Depósitos e outros diversos bancos), quase todas elas visando os dados de cartões bancários de pagamento[7].

Surgiram entretanto novas modalidades de *phishing*, abusando da imagem da Autoridade Nacional de Segurança Rodoviária – ANSR e do Cartão Continente. Quanto à modalidade de *phishing* com abuso da imagem da ANSR teve uma difusão muito expressiva: foram recebidas 306 denúncias. A este respeito foram aliás emitidos novos Alertas Cibercrime, a 7 de fevereiro de 2025 e a 11 de setembro de 2025, respetivamente. No passado tinham já sido emitidos a este respeito, na continuação de inúmeros outros em anos anteriores, os Alertas Cibercrime de 12 de março de 2024, de 17 de julho de 2024 e de 24 de outubro de 2024.

burlas *online*

20. As burlas em compras *online* têm ganho, ao longo dos anos, uma extraordinária dimensão, provocando um muito significativo prejuízo económico aos portugueses. Trata-se de uma criminalidade que alimentará as chamadas cifras negras: por um lado, porventura por vergonha ou pudor, muitos lesados preferem assumir e esquecer o prejuízo que tiveram; por outro, alguns lesados não denunciam a burla por não terem expetativa na recuperação do valor perdido. Em qualquer dos casos, estatisticamente estas situações são dificilmente identificáveis já que, nas estatísticas da Justiça, as mesmas se diluem na categoria geral das burlas.

21. Durante o ano de 2025 o Gabinete Cibercrime continuou a receber, na linha do que aconteceu em anos anteriores, denúncias de burlas praticadas com recurso aos meios de comunicação e às redes sociais.

Um dos segmentos mais significativos destas burlas são as relacionadas com vendas através de diversas legítimas plataformas de compras e vendas *online* e com vendas nas redes sociais. Mantém-se eficaz, na perspetiva dos agentes criminosos, a repetida técnica de criar uma conta numa plataforma de vendas ou numa rede social, nela disponibilizando produtos para venda; depois de proceder à venda e de o comprador ter pago o bem em causa, o criminoso apaga a conta e "*desaparece*" do ciberespaço. Este

[7] Tal como vem consistentemente sucedendo desde 2021, em função do reforço da segurança no acesso *online* a contas bancárias, esta metodologia criminosa tem visado quase exclusivamente dados de cartões de crédito. Praticamente desapareceram as denúncias de *phishing* visando o acesso imediato a contas bancárias.

método causa grandes prejuízos económicos e permite ao agente do crime defraudar sucessivamente muitas vítimas.

No seu conjunto, as diversíssimas formas reportadas de praticar **burlas *online***, no ano de 2025, contabilizaram **660 denúncias** (em geral correspondentes a burlas simples, portanto crime de natureza semipública, muitas das quais na forma tentada) que não foram encaminhadas para investigação. Este volume de denúncias significa um **acréscimo de 10,18 %** em relação às denúncias recebidas em 2024 (599 denúncias).

Se a estas denúncias, não encaminhadas, se acrescentarem aquelas que, pelos respetivos contornos ou detalhes, foram encaminhadas para abertura de inquérito (incluindo as chamadas *burlas de romance*, as *páginas falsas* e outras defraudações com falsidade informática), em **2025 contabilizam-se 764 denúncias de burlas por meios tecnológicos**.

páginas "*falsas*"

22. Do conjunto das burlas *online*, com recurso a falsidade informática, realça-se, tal como sucedeu em anos anteriores, que também em 2025 foi recebido um número considerável de denúncias de páginas "*falsas*" na Internet – páginas *web* que imitam as autênticas e legítimas páginas na Internet de diversas marcas de roupa, calçado, equipamento desportivo, entre outras, com o propósito de convencer as vítimas a comprar e pagar, nessas páginas "*falsas*", bens que depois a vítima nunca vem a receber.

Tais páginas são, em geral, cópias das autênticas páginas das marcas em causa. Anunciam sempre grandes promoções, saldos ou enormes descontos (70 ou 80% do preço de base). Nunca indicam qualquer forma de contacto com os respetivos responsáveis e, em geral, exigem o pagamento das compras com cartão de crédito.

23. Além destas "*falsas*" páginas de marcas, continuaram a ser recebidas denúncias de práticas fraudulentas cometidas por via da criação na Internet de páginas alegando falsamente pertencer a departamentos ou serviços públicos e referindo prestar serviços aos cidadãos – cobrando, pela prática de tais serviços, sem naturalmente os prestar. Assim sucedeu com páginas supostamente permitido a prática de atos de registo predial, ou de registo civil (casamentos e divórcios *online*, por exemplo) ou mesmo a obtenção *online* de carta de condução, sem qualquer necessidade de aulas ou exames.

Este tipo de denúncia foi o mais numeroso dentro das mensagens recebidas que vieram a ser encaminhadas para inquérito – em 2025 foram encaminhadas para investigação denúncias de 83 páginas falsas na Internet e outras burlas conjugados com falsidade informática. Se ainda acrescerem, a estas, as 38 denúncias de casos de *CEO Fraud* (que mais abaixo melhor se descreverão), o número conjunto destas defraudações remetidas para inquérito é de 121 denúncias (em 2024 tinham sido 145 denúncias).

burlas em supostos investimentos em cripto ativos

24. Desde 2021 que, consistentemente, têm vindo a ser denunciados casos de ofertas fraudulentas de planos de investimento em cripto ativos. Em 2021, foram denunciados 38 casos; no ano seguinte, de 2022, foram 94 os casos. Por sua vez, em 2023, foram recebidas pelo Gabinete Cibercrime 106 denúncias. Em 2024, foram recebidas 139 denúncias desta natureza e por último, em 2025, 135 denúncias. Embora não se tenha registado um aumento numérico das participações recebidas, verifica-se constância e persistência no número das mesmas.

Trata-se de situações em que as vítimas se queixam de terem sido aliciadas para investir, em plataformas *online*, quantias que depois perderam. Em geral, as quantias são avultadas (nalguns casos, dezenas de milhares de euros). Normalmente, após tentativas para reaver o valor supostamente investido, as

plataformas onde foi feito o investimento deixaram de estar *online*, não se conhecendo qualquer detalhe ou contacto que permita apurar o servidor da Internet onde estava a mesma alojada.
Por outro lado, em geral, as vítimas não dispõem de prova nem de referências seguras quanto às plataformas em causa: confiaram na informação que nelas consultavam, *online* e, quando estas desaparecerem deixaram de ter dados concretos e rigorosos que permitam proceder a uma investigação eficaz.

burlas no mercado imobiliário

25. Esta forma de defraudação tem vindo a manifestar-se regularmente, provocando sempre um grande impacto financeiro nas vítimas. Passa pela difusão de anúncios enganosos propondo dar de arrendamento imóveis que não existem (ou que existindo, não pertencem ao anunciante, nem estão disponíveis para arrendamento). As vítimas deste tipo de crime são sobretudo estudantes universitários que procuram casas para habitar quando se deslocam para estudar noutra cidade, ou cidadãos estrangeiros que passam em Portugal breves períodos de tempo. Trata-se de um tipo de criminalidade de natureza internacional: em Portugal operam burlões que dizem ser estrangeiros e pretendem receber as rendas do suposto imóvel em contas bancárias no estrangeiro; foram noticiados casos em que burlões operam noutros países e pretendem receber as rendas em contas bancárias em Portugal. A este respeito foi emitido, já em 2023, o Alerta Cibercrime de 12 de julho de 2023.

as burlas relacionadas com arrendamentos *online* aumentaram 44,11% em 2025

Durante o ano de 2023 tinham sido recebidas 31 denúncias desta natureza. Em 2024 foram recebidas 34. Agora, em **2025**, foram recebidas **49 denúncias** desta tipo. Portanto, registou-se um **acréscimo de 44,11%** em relação ao ano anterior.

CEO fraud

26. Também continuaram a ser denunciadas ao Gabinete Cibercrime burlas conhecidas no jargão policial como *CEO fraud*, ou *Business Email Compromise Fraud*, técnica de engenharia social pela qual os agentes criminosos tentam induzir em erro uma determinada estrutura empresarial, levando-a a efetuar pagamentos a terceiros (os criminosos), que se fazem passar por autênticos fornecedores ou parceiros de negócio da empresa. Em geral, esta atuação ilícita é desencadeada por grupos de crime organizado internacional e os prejuízos económicos causados são de grande montante.
Foram recebidas pelo Gabinete Cibercrime denúncias deste tipo remetidas por empresas estrangeiras, queixando-se de que foram enganosamente induzidas a efetuar pagamentos para contas bancárias de bancos em Portugal. Do mesmo modo, entidades portuguesas denunciaram ter efetuado pagamentos com destino a contas bancárias estrangeiras. Em 2021 tinham sido recebidas 14 denúncias deste tipo; foram 23 no ano de 2022. Em 2023 foram recebidas 18 denúncias e, em 2024, 25 denúncias. Agora, em **2025**, foram recebidas **38 denúncias** (o que significa um **aumento de 52%**) em relação a 2024. Todas elas foram remetidas para investigação, desde logo por se tratarem de denúncias de crime público.
Anota-se **persistência deste fenómeno**, que é **imensamente lucrativo** para os agentes criminosos.

27. Importa porém anotar também alguma evolução no paradigma deste método criminoso: no passado, os alvos eram sempre estruturas empresariais de maior dimensão e os pagamentos em causa respeitavam a supostos fornecimentos de bens ou serviços, por terceiros. Em 2025 uma parte muito substancial dos casos ocorridos revelou outra modalidade de atuação: as mensagens fraudulentas expedidas pelos agentes criminosos simulavam ter origem em colaboradores da entidade em causa e solicitavam a alteração da conta bancária onde normalmente é depositado o respetivo salário.

"falsos" trabalhos *online*

28. Este fenómeno criminógeno surgiu durante o ano de 2023 e ganhou enorme expansão em 2024. Trata-se de um sofisticado processo fraudulento, com múltiplas variantes, de propostas de execução de tarefas ou trabalhos *online*. Originariamente, tais propostas surgiam em anúncios, sobretudo nas redes sociais, mas progressivamente passaram a ser mais expandidos por via de mensagens diretas (designadamente WhatsApp), utilizando os métodos de outros modelos criminais.
Mais recentemente o modelo tem sido o da remessa de mensagem de voz para o telefone da vítima, solicitando que a mesma subscreva um canal de WhatsApp ou Telegram.
Normalmente, trata-se de propostas de tarefas muito simples, para desempenhar a partir de casa, por via da Internet, às quais correspondem pagamentos muito generosos. Tinha sido a este propósito, logo no início de 2023, emitido o Alerta Cibercrime de 27 de janeiro de 2023. Ulteriormente, os métodos tornaram-se mais diversificados.
Em todos os casos identificados, as vítimas receberam pequenas compensações por pequenas tarefas iniciais. Porém, depois, invariavelmente, os agentes criminosos solicitaram às vítimas que envolvessem nestas atividades os seus próprios recursos financeiros, que prometiam multiplicar e devolver muito aumentados. Também invariavelmente, as vítimas acabaram por perder todo o seu próprio dinheiro, não recebendo nunca qualquer montante.

29. Em 2023 tinham sido recebidas 42 denúncias desta natureza, mas em 2024, foram 253. Neste ano, de **2025**, foram recebidas **172 denúncias** deste tipo
Trata-se de um método de defraudação que tem vindo a sofisticar-se e a ganhar uma enorme dimensão económica, provocando grande prejuízo patrimonial às vítimas, agravado por estas serem normalmente pessoas desempregadas ou de baixos recursos.

defraudações na utilização de plataformas de vendas *online* e em aplicações de pagamentos

30. Tal como vem regularmente sucedendo desde 2020, também em 2025 foram recebidas denúncias por burlas associadas a vendas *online*, com a aplicação de pagamentos MBWAY. Trata-se de um fenómeno muito divulgado na comunicação social, que deu origem a muitas investigações e até a detenções, julgamentos e condenações. Talvez por isso, o número de denúncias não só não tem registado o aumento de outros fenómenos como, pelo contrário, tem diminuído. Porém, a verdade é que esta modalidade criminosa persiste e prova ser ainda rentável, uma vez que os agentes criminosos insistem na sua prática.
No ano de 2022 tinham sido recebidas 84 denúncias desta natureza, enquanto em 2023 se registaram 68. Em 2024 foram recebidas 78 denúncias. Por último, quanto ao ano de **2025**, foram já somente recebidas **46 denúncias** por tentativas de defraudação com utilização da aplicação **MBWAY**

telefonemas fraudulentos

31. Vem de há vários anos a denúncia do recebimento de telefonemas fraudulentos, que pretendem convencer as vítimas a efetuar pagamentos a terceiros.
Em 2024 tinha-se assistido ao surgimento de uma nova modalidade criminosa: as burlas praticas por meio de **telefonemas de *falsos* intermediários de cripto ativos**. Foi aliás a este propósito emitido o Alerta Cibercrime de 2 de outubro de 2024.
Trata-se de uma abordagem criminosa sofisticada pela qual, ao contrário do que tem sucedido com outras metodologias de defraudação por via de telefonemas, não é realizada uma quantidade indiscriminada de chamadas telefónicas para vítimas aleatórias. Pelo contrário, neste caso, as vítimas

são escolhidas porque o seu número de telefone, o seu endereço de email e o seu nome constam de listagens em poder dos agentes criminosos (normalmente organizadas a partir do acesso ilegítimo a servidores e a dados pessoais – tais listas são correntemente transacionadas na *Darknet*). Ou seja, quando o agente criminoso realiza uma determinada chamada telefónica, está já munido de alguma informação sobre o titular do respetivo número telefónico. O propósito desta abordagem é convencer a vítima de que é titular de uma antiga e *esquecida* carteira de cripto ativos, entretanto muito valorizada mas que, por estar inativa há demasiado tempo corre o risco de ser encerrada – a menos, claro, que a vítima proceda a um pequeno depósito na mesma. O resto do processo é o habitual nestes casos: se a vítima proceder a qualquer pagamento ou depósito, não mais conseguirá reaver estas suas quantias.

32. Importa referir que estas chamadas telefónicas não têm origem em Portugal. Muitas delas provêm de países muito distantes, como a Índia e ou a Nigéria, ou outros, com quem a cooperação judiciária é mais difícil ou demorada. Os agentes criminosos falam sempre com as vítimas em inglês e visam vítimas de todo o mundo, e não especificamente vítimas de Portugal. Na generalidade dos casos os denunciantes que contactaram o Gabinete Cibercrime identificaram a atuação e o intuito fraudulento, não tendo cedido aos intentos dos criminosos.

33. Este fenómeno, ainda com pouca visibilidade no início de 2024, veio progressivamente a tornar-se muito expressivo ao longo do ano, vindo a ser denunciados 127 casos desta natureza. Agora, no ano de **2025**, foram recebidas **303 denúncias** deste tipo – portanto, **mais 137,80%** do que em 2024. Trata-se pois de um fenómeno em grande expansão.

as burlas por meio de telefonemas fraudulentos aumentaram 137,80% em 2025

34. A esta expansão correspondeu a regressão fortíssima de modalidades diferentes do mesmo tipo de defraudação, muito expandidas no passado.
Assim aconteceu com uma forma de defraudação por via de telefonemas alegadamente efetuados por uma suposta "*polícia internacional*", tentando convencer as vítimas de que as suas contas bancárias foram utilizadas em atividades de branqueamento de capitais, sugerindo que, antes do respetivo "*congelamento*" pelas autoridades judiciárias, os respetivos saldos sejam transferidos para uma outra conta (*controlada* pelo agente criminoso). Este fenómeno surgiu em 2023 (foram recebidas 135 denúncias), tendo sofrido uma enorme expansão no ano de 2024 (foram recebidas 241 denúncias). Porém, em 2025 quase desapareceu: apenas foram recebidas 3 denúncias desta natureza.

35. Outro tipo de telefonemas fraudulentos muito significativos no passado traduziam abordagens em que os agentes criminosos procuravam convencer as vítimas de que os respetivos equipamentos informáticos estavam infetados com vírus, persuadindo-os assim a facultar-lhes acesso remoto aos mesmos, ou a instalar neles *malware*, ou ainda a fazer-lhes pagamentos. Nestes casos, os agentes criminosos alegavam serem colaboradores do "*apoio técnico*" da Microsoft. Este fenómeno, persistente durante quase uma década[8], deixou de ter expressão. Em 2024 tinham sido recebidas 41 denúncias, mas no ano de 2025 não foi recebida qualquer denúncia deste tipo.

ataques informáticos – ransomware e *"furto de credenciais de acesso a contas"*

36. As denúncias recebidas respeitantes a crimes informáticos, ou *cibercrimes em sentido estrito*, representaram em 2024 um conjunto numericamente pouco significativo, mas em geral tiveram grande

[8] O primeiro Alerta Cibercrime a este respeito foi emitido em 2015, sendo renovado em 2020 (https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/alerta_cibercrime_microsoft_14-02-2020_5.pdf).

repercussão nas vítimas. Uma boa parte destas denúncias relatou ataques de ***ransomware***, sobretudo a pequenas e médias empresas. Outros dos casos denunciados respeitavam a **acesso ilegítimo** a sistemas diversos. Em geral, todas estas denúncias foram remetidas para investigação: no caso do *ransomware*, foram encaminhadas para investigação 7 denúncias e quanto a casos de acesso ilegítimo foram encaminhadas 12.

37. Este fenómeno criminoso não pode ser desligado de uma específica consequência e manifestação do mesmo: o do **acesso ilegítimo a contas de redes sociais**. Têm sido denunciados muitos acessos ilegítimos, com abuso das respetivas credenciais de acesso, que são "*furtadas*" mediante a expedição de mensagens contendo algum tipo de *malware*, ou um *link* para um site comprometido. Normalmente, após o acesso ilegal, o agente criminoso altera as credenciais de acesso à conta, impedindo assim o acesso à mesma pelo seu legítimo titular. Após este acesso, há casos em que o agente criminoso utiliza a conta para propagandear negócios fraudulentos, por exemplo relacionados com cripto ativos ("*abusando*" da credibilidade do respetivo dono junto dos seus contactos). Noutros casos, o agente criminoso exige ao "*dono*" da conta o pagamento de quantias monetárias para lhe "*devolver*" as credenciais.
Este procedimento criminoso tem visado especialmente indivíduos muito presentes na Internet, designadamente em redes sociais, nalguns casos por razões profissionais. Este tipo de atuação tem causado grandes prejuízos económicos a donos de pequenos negócios baseados nas redes sociais, bem como prejuízos de outra natureza a quem utiliza as redes sociais numa vertente profissional. Em 2023 tinha sido emitido a este respeito o Alerta Cibercrime de 18 de setembro de 2023. No decurso desse ano (2023) foram recebidas 49 denúncias desta natureza. Já em 2024 foram recebidas 147 denúncias. Agora, em **2025**, foram recebidas **63 denúncias** deste tipo.

38. Foram ainda identificadas denúncias de **mensagens de correio eletrónico contendo *malware*** de diversa natureza, em geral inconsequentes, isto é, os seus destinatários identificaram a sua natureza e acabaram por evitar ser vítimas das mesmas.
No decurso de **2025** foram recebidas **70 denúncias** deste tipo.

"falsas" convocatórias policiais

39. Surgiu em 2022, com grande intensidade, uma modalidade de burla *online* que passa pela expedição de uma multiplicidade de mensagens, para destinatários indiscriminados. Em anexo à mensagem é remetido um documento simulando ser uma espécie de notificação judicial, referindo que o destinatário é suspeito de diversos atos relacionados com abuso sexual de crianças. Ao mesmo tempo, o destinatário é advertido de que, sendo alvo de uma investigação criminal, a mesma pode ser encerrada mediante um pagamento de uma quantia monetária, a título de multa. Caso o destinatário responda a esta mensagem, solicitando instruções para o pagamento, em resposta é facultado um IBAN, para onde deve ser efetuada uma transferência – em geral, na ordem dos dois a três mil euros.
Durante o ano de 2022 tinham sido recebidas 224 denúncias deste tipo de crime, mas em 2023 já foram apenas 113 denúncias. A tendência de diminuição desta prática criminosa manteve-se em 2024, ano durante o qual foram apenas recebidas 64 denúncias. Por último, em **2025**, foram recebidas apenas **59 denúncias** desta natureza.
Isto é, embora continue a manifestar-se (o que evidencia que continua a ser uma atividade criminosa lucrativa) a verdade é que, desde a sua eclosão, em 2022, este fenómeno tem vindo a regredir.

sextortion

40. Têm persistido o surgimento de denúncias diferentes, mas paralelas às que acima acabaram de descrever-se, em que as vítimas relatam ter recebido pedidos de pagamento de quantias (em cripto moedas), sob pena de divulgação de imagens íntimas, geralmente de natureza sexual. Estas situações são diferentes das que acima se referiram: naquelas, os agentes criminosos expedem milhares de mensagens para destinatários desconhecidos e esperam que o seu "*bluff*" convença as vítimas a pagar. Nestas outras, que agora se referem, as vítimas são abordadas personalizadamente. Num primeiro momento, são abordadas *online*, sobretudo em sites de namoro, com o intuito de estabelecer uma relação pessoal, que vem a evoluir para alguma proximidade, no contexto da qual o agente criminoso acaba por obter imagens da vítima de natureza íntima ou sexualizadas. De seguida o agente criminoso exige à vítima o pagamento de quantias, sob pena de não o fazendo proceder à divulgação das imagens. Este fenómeno ocorreu frequentemente entre 2019 e 2021. Neste último ano foram apresentadas 21 denúncias desta natureza. Porém, em 2022 deixou de ter expressão. Entretanto, no ano de 2023 vieram a ser recebidas 34 denúncias deste tipo, anunciando-se, portanto, a retoma desta atividade criminosa. Esta retoma confirmou-se em 2024, ano no qual foram recebidas 56 denúncias desta natureza. Já em 2025, foram apenas recebidas 27 denúncias deste tipo.
Consideradas conjugadamente com as denúncias do fenómeno imediatamente anterior, foi recebido um conjunto de **86 denúncias** a este respeito.

crimes contra a honra

41. O Gabinete Cibercrime tem recebido recorrentemente denúncias reportando crimes contra a honra, sobretudo referentes a publicações em redes sociais. Pela natureza do ilícito em causa (e pelas exigências processuais penais associadas à mesma), o procedimento adotado é o de informar os denunciantes de que deverão formalizar a sua participação criminal e a manifestação de vontade na constituição como assistentes. Assim é porque no quadro legislativo português este tipo de ilícito tem natureza particular – portanto, o início da investigação criminal está legalmente dependente da apresentação de queixa e da constituição como assistente (com constituição de um advogado como mandatário judicial).
Trata-se de um ilícito "menor" (desde logo, pela sua mesma natureza, de crime particular). Porém a verdade é que continua a motivar denúncias, ao longo dos anos.
Durante **2025** foram recebidas **36 denúncias** deste tipo. No anterior, de 2024, tinha dado origem a 40 denúncias.