MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

Nota Informativa

CIBERCRIME:
DENÚNCIAS RECEBIDAS
2022

ÍNDICE

CIBERCRIME:
DENÚNCIAS RECEBIDAS
2022

A. O CONTEXTO - CIBERCRIME

1. A expressão *cibercrime* alberga tradicionalmente mais tipos legais de crime do que os ilícitos descritos na Lei do Cibercrime[1] (Lei nº 109/2009), estendendo-se ao Código Penal[2] e a outras fontes legais avulsas[3]. Como fenómeno criminógeno, sociologicamente abarca outros crimes tão diversos como as burlas *online*, a divulgação ilícita de dados pessoais ou fotografias, a difusão de pornografia infantil ou as violações de direito de autor. Uma boa parte destas práticas criminosas, que já existia antes da popularização e massificação das redes de comunicações eletrónicas, ganhou um novo espaço e uma nova dimensão neste meio, onde se expandiu de forma extraordinária.

2. Estas circunstâncias impede a quantificação estatística rigorosa desta realidade criminal: as estatísticas da Justiça registam detalhadamente os números de crimes segundo os tipos legais de crime (por exemplo burlas, injúrias ou difamações, crimes contra o direito de autor), não considerando autónoma ou separadamente aqueles que ocorrem *online*. O sistema de estatísticas não foi concebido de forma a permitir aperceber a dimensão numérica (estatística) do complexo fenómeno da cibercriminalidade: embora identifique bem os crimes *informáticos* propriamente ditos, deixa de fora muitos outros crimes, ditos *clássicos*, mas praticados *online*.

3. Por isso, do ponto de vista estatístico não é possível avaliar a real dimensão do cibercrime. O Gabinete Cibercrime da Procuradoria-Geral da República tem procurado superar esta dificuldade por via do contacto com os magistrados que integram a sua rede de pontos de contacto em todas as comarcas do país, os quais vão reportando, embora de forma empírica, esta realidade. Mas tem também usado, como indicador destes fenómenos, as denúncias recebidas por via da linha de correio eletrónico do Gabinete Cibercrime (cibercrime@pgr.pt).

B. O PROCESSO DE RECEBIMENTO DE DENÚNCIAS

4. O endereço eletrónico cibercrime@pgr.pt, atribuído ao Gabinete Cibercrime, tem vindo a ser utilizado por cidadãos, desde 2016, para remeter ao Ministério Público denúncias, relevantes para efeitos de processo penal.

O Gabinete Cibercrime é um gabinete de coordenação nacional, criado pelo Conselho Superior do Ministério Público, no quadro do artigo 55º do Estatuto do Ministério Público, não tendo atribuições funcionais de direção da investigação criminal, nos termos do Código de Processo Penal. Isto é, não lhe é legalmente acometida a função de instaurar e dirigir concretas investigações criminais.

[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.

5. Por esse motivo, quanto às denúncias criminais que o Gabinete Cibercrime recebe, estabeleceu-se um entendimento informal com o Departamento de Investigação e Ação Penal de Lisboa, fixando os parâmetros de um procedimento de recebimento e encaminhamento das denúncias para aquele departamento do Ministério Público[4]. Este procedimento, procura, por um lado, dar solução ao inexorável crescimento das denúncias recebidas por correio eletrónico; por outro, procura satisfazer algumas das exigências formais (do Código de Processo Penal) a que o procedimento de queixa por correio eletrónico não consegue ainda dar resposta.

6. Fixaram-se critérios de análise destas queixas, tendo em vista a triagem daquelas que são remetidas para abertura de inquérito. Sendo os seus remetentes sempre informados da possibilidade legal de apresentação de queixa formal, pelas vias comuns, algumas das denúncias não são encaminhadas para abertura de inquérito.
Assim acontece, por exemplo, com denúncias que não reúnem elementos ou condições formais suficientes para abertura de uma investigação. É o caso de 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.

7. Importa ainda referir que uma parte destas últimas denúncias (as que não são remetidas para abertura de inquérito), é encaminhada para a Polícia Judiciária (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica – UNC3T). Assim acontece quando a denúncia recebida não justifica ou impõe a imediata abertura de inquérito (e quem a remeteu não o pretende) mas, ainda assim, contém informação relevante para eventuais investigações pendentes ou para melhor identificação de procedimentos ou fenómenos criminosos.

C. AS DENÚNCIAS RECEBIDAS

8. As denúncias de *cibercrimes* em sentido alargado recebidas por 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, designadamente após a eclosão da pandemia resultante da COVID–19. Em 2021, porém, o aumento foi ainda mais expressivo do que tinha sido em 2020, mais que duplicando. Em **2022** esta tendência manteve-se: foram recebidas **2124 denúncias,** quando em **2021** tinham sido **recebidas 1160**. Portanto, registou-se um **aumento de 73,58%.**
Pode dizer-se que, em termos médios, com oscilações anuais, em cada ano desde 2019, **são recebidas o dobro das denúncias do ano anterior**.

Denúncias em **2019:**
193
Denúncias em **2020:**
544
Denúncias em **2021:**
1160
Denúncias em **2022:**
2124

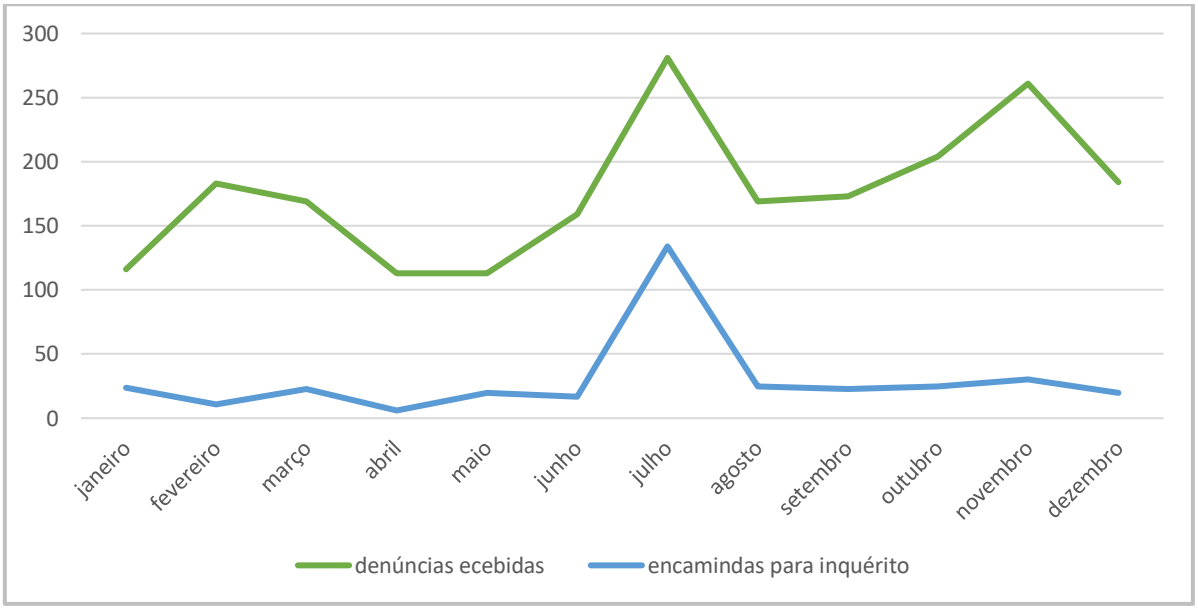
9. No decurso do ano de 2022 foram recebidas no Gabinete Cibercrime as denúncias que melhor se descrevem no quadro e no gráfico que seguem, onde se discriminam também aquelas que vieram a ser encaminhadas para **abertura de inquérito** (que foram **359** – em **2021** tinham sido **195**, tendo, portanto, havido um aumento de **84,10%)** ou para a Polícia Judiciária, nos moldes que acima se referiram.

[4] As denúncias são remetidas para outras comarcas, caso se aperceba liminarmente que os factos denunciados ocorreram na área geográfica de outra comarca, que não na de Lisboa.

denúncias recebidas em 2022

Mês	denúncias recebidas	encaminhadas para inquérito	encaminhadas para a PJ
janeiro	116	24	3
fevereiro	183	11	2
março	169	23	6
abril	113	6	0
maio	113	20	1
junho	159	17	0

Mês	denúncias recebidas	encaminhadas para inquérito	encaminhadas para a PJ
julho	281	134	1
agosto	169	25	2
setembro	173	23	1
outubro	204	25	2
novembro	261	30	1
dezembro	184	20	0



10. A análise do conjunto das denúncias recebidas no ano de 2022 revela que se **mantém a tendência de consistente subida**: por exemplo, no mês de dezembro de 2022 foram recebidas 184 denúncias, portanto muito mais que as recebidas no mês de janeiro do mesmo ano (116). No mês de dezembro do ano anterior, de 2021[5], tinham sido recebidas 95 denúncias. Isto é, de um ano para o outro, no mesmo mês, registou-se um aumento para muito próximo do dobro. Esta tendência mantém-se constante desde o ano de 2020: em janeiro de 2020[6] foram recebidas 20 denúncias, enquanto no mês de dezembro do mesmo ano foram recebidas 44; em dezembro de 2021, como se referiu, foram recebidas 95 denúncias, valor também não muito longe do dobro das recebidas em janeiro desse ano (58 denúncias).

11. Em 2022, os números das **participações entradas superam em muitíssimo as do ano anterior**. Observaram-se algumas variações mensais (com grandes aumentos do número de denúncias), que ficaram a dever-se à ocorrência de fenómenos criminais específicos, que pontualmente provocaram um grande número de vítimas. Assim ocorreu particularmente no mês de julho de 2023, durante o qual decorreu uma muito expressiva campanha criminosa com grande incidência *online*, do tipo "esquema de pirâmide".

[5] https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime-25-01-2022.pdf.
[6] https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_2020.pdf.

12. Estas variações pontuais em nada se relacionam com variações ocorridas em anos anteriores, designadamente nos meses de abril de 2020 e de fevereiro de 2021, coincidentes com os períodos de confinamento decorrentes da pandemia provocada pela COVID-19, alturas em que as denúncias aumentaram extraordinariamente (em fevereiro de 2020 foram recebidas 133 denúncias e em abril de 2021 foram recebidas 131).
Em 2022 foram recebidas, em média, 177 denúncias por mês – portanto, muito mais do que nos meses mais críticos dos períodos de confinamento. O aumento constante e persistente destes fenómenos criminais ultrapassou já aqueles valores excecionais. O incremento extraordinário do cibercrime provocado pela pandemia foi já ultrapassado pelo aumento corrente, regular e permanente destes fenómenos.

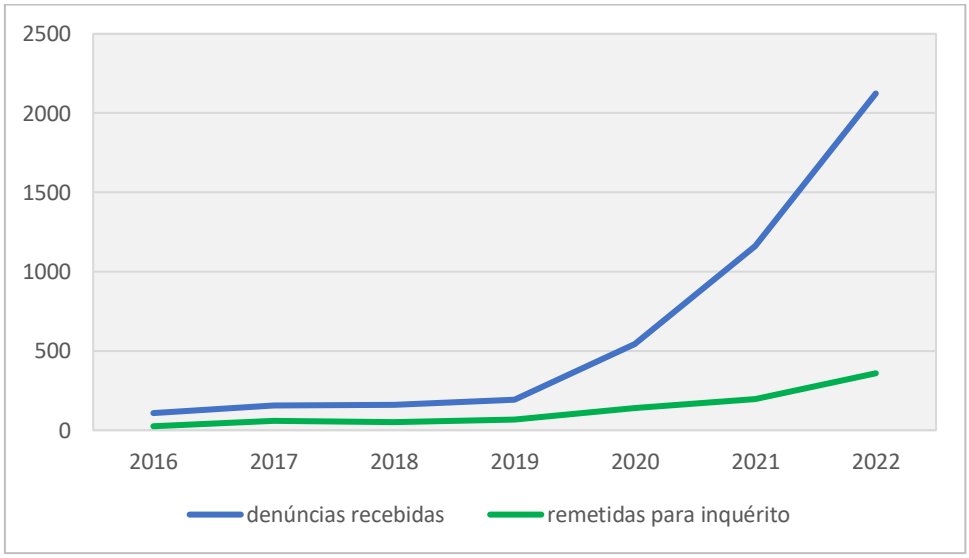
13. Os números constantes da tabela seguinte, visualmente representados no gráfico que se lhe segue, reforçam a conclusão que acima se formulou e ilustram claramente a progressão do cibercrime de ano para ano. Tal como em anos anteriores se antevia já, verifica-se que embora a pandemia tenha impulsionado o aumento deste tipo de criminalidade, esta tendência crescente afigura-se constante e consistente, alheia ao esbatimento da pandemia.

desde 2016 é regular, constante e persistente o aumento da cibercriminalidade

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 - 2022

Ano	denúncias recebidas	denúncias remetidas para inquérito
2016	108	25
2017	155	59
2018	160	50
2019	193	67
2020	544	138
2021	1160	195
2022	2124	359



14. 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.

de 2021 para 2022 as denúncias de cibercrime aumentaram 73,58%

De 2016 (108 denúncias) para 2017 (155 denúncias), registou-se uma subida de 44%. Foi muito mais moderada a evolução para 2018 (160 denúncias, contra as 155 de 2017). Mas já em 2019 (193 denúncias) regressou a progressão (na ordem dos 18 %). Quanto a 2020 e 2021, o aumento no número de denúncias foi excecional e superou em muito os dos anos anteriores. De **2019** (193 denúncias) **para 2020** (544 denúncias), **o aumento foi de 88%**, enquanto **de 2020** (544 denúncias) **para 2021** (1160 denúncias), **o aumento foi de 113%**. Como se referiu acima, **de 2021 para 2022** (2124 denúncias), o **aumento foi de 73,58%**.

D. CRIMINALIDADE MAIS FREQUENTE

15. As denúncias recebidas por via do endereço cibercrime@pgr.pt fornecem indicadores reais quanto ao conjunto total das denúncias de cibercriminalidade apresentadas pelos cidadãos ao Ministério Público. A informação recolhida destes já milhares de denúncias não gera dados estatísticos rigorosos, mas certamente permite que dela se infiram as grandes linhas dos *cibercrimes* que vitimam os portugueses.

A leitura destas grandes linhas tem que ser feita tendo presente que a cibercriminalidade é muito evolutiva. A realidade observada em anos anteriores foi diferente daquela que ocorreu em 2022 e será também seguramente diferente da que 2023 revelará.

16. Já se referiu que no mês de julho de 2022 foi recebido um número excecional de denúncias, por ter sido identificada uma campanha criminosa específica que se dirigiu a muitas vítimas. Durante todo o mês foram recebidas 281 denúncias, correspondentes a 13,2% do total anual (2124). Nesse mesmo mês de julho foram remetidas para investigação 134 denúncias (correspondentes a 37,3 % do total das remessas do ano, que foram 359). De entre elas, 127 corresponderam a denúncias respeitantes ao fenómeno específico que se referiu, enquanto as restantes 232 respeitam a diversos fenómenos criminógenos. Por estes motivos, as considerações comparativas seguintes apenas se reportam a estas 232 denúncias, excluindo-se da análise as 127 restantes.

phishing

17. Em 2022, numericamente, a **tipologia criminosa mais reportada** ao Gabinete Cibercrime foi a do *phishing*. Durante todo o ano sucederam-se inúmeras e diversas campanhas de *phishing*, com o propósito de facultarem aos seus autores os dados de acesso a cartões e a contas bancárias (e a outro tipo de contas *online*) das vítimas. A **generalidade dos bancos portugueses** (ou melhor, os seus clientes) foram alvos deste tipo de iniciativas criminosas[7].

o *phishing* foi o fenómeno criminoso mais denunciado: 358 casos em 2022

18. Como vem consistentemente sucedendo desde 2021, esta metodologia criminosa tem evoluído, visando menos o acesso a contas bancárias e **mais intensamente os dados de cartões de crédito**. Esta mutação pode ter tido origem no reforço das medidas de segurança de acesso às contas de *homebanking*, designadamente com a implementação de múltiplos fatores de autenticação.

[7] Por estas razões, foi emitida, logo nos primeiros dias de 2022, o **Alerta Cibercrime de 13 de janeiro de 2022**, tendo ainda sido emitidos mais dois alertas, a **29 de setembro de 2022** e a **10 de outubro de 2022**.

Nas manifestações mais recentes de *phishing* observou-se assim uma muito maior prevalência das tentativas de obtenção ilícita de dados de cartões de crédito. Porém, o modelo da atuação criminal permaneceu inalterado: continua a passar pela remessa de milhões de mensagem de *email*, pelas quais os agentes do crime induzem as vítimas a aceder a páginas *falsas*, por si geridas, onde são incentivadas a introduzir os dados dos seus cartões de crédito.

19. Ao longo do ano estas denúncias de *phishing* **(358 casos)** constituíram o conjunto mais numeroso do total das denúncias recebidas pelo Gabinete Cibercrime, correspondendo a **16,85% de todas as denúncias** recebidas. Em 2021 tinham sido recebidas 167 denúncias desta natureza. Registou-se, pois, um **aumento de 114,37%** de denúncias a este respeito.

20. Quanto a ilícitos relacionados com cartões de crédito, recorda-se que, em novembro de 2021, o legislador nacional redesenhou o modelo incriminatório relacionado com este e outros meios de pagamento não corpóreo. De forma muito simples pode dizer-se que a lei passou a enquadrar no artigo 225º do Código Penal (crime de *abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento*) todos os atos ilícitos relacionados com o uso abusivo de cartões de crédito autênticos e dos seus dados, deixando para a Lei do Cibercrime os atos relacionados com cartões falsos ou contrafeitos.
Esta nova abordagem levou ao surgimento, em 2022, de várias queixas relacionadas com o uso abusivo de dados de cartões. Foram recebidas no primeiro semestre muitas queixas deste teor, 7 das quais foram remetidas para investigação, reportando-se todas elas a uso abusivo de dados de cartões, por agentes desconhecidos, em compras na Internet.
Além destas queixas, foi dado conhecimento ao Gabinete Cibercrime de numerosíssimas outras situações de uso abusivo de dados dos cartões de crédito emitidos por uma específica instituição bancária que opera *online*. Tais dados terão sido obtidos por via de *phishing*.

burlas online

21. Todos os indicadores apontam no sentido de que o comércio eletrónico se desenvolve em grande velocidade e intensidade. Em paralelo a este desenvolvimento, surgiram práticas criminosas com ele relacionadas e, por isso, também as burlas em compras *online* se expandiram de forma extraordinária, tornando-se num dos fenómenos de cibercriminalidade mais frequente, provocando um grande prejuízo económico efetivo aos portugueses.

22. Durante o ano de 2022 continuaram a ser identificadas e denunciadas inúmeras formas de burla, relacionadas com vendas através de diversas plataformas de compras e vendas *online* legítimas. Da mesma forma, foram identificadas burlas com vendas nas redes sociais (designadamente no Facebook). Trata-se de burlas clássicas, em que a especificidade resulta apenas do meio tecnológico utilizado. A técnica usada é repetida: o criminoso cria uma conta numa plataforma de vendas ou numa rede social, nela disponibilizando produtos para venda. Procede à venda e o comprador paga o bem em causa, mas o mesmo nunca é entregue. Desta forma, o agente do crime consegue burlar muitas vítimas num espaço muito curto de tempo, após o qual encerra subitamente a sua conta na plataforma de vendas ou na rede social, sem que mais nada se saiba quanto ao que aconteceu ao mesmo.

23. Na sua generalidade, do lado de cada vítima, todas estas situações envolveram valores pouco elevados, raramente ultrapassando as dezenas de euros. Em todo o caso, pelo enorme número de vítimas que esta atuação atingiu, o seu significado económico é muito relevante.

Durante o ano de 2022, este tipo de crime ocupou o **maior grupo** das denúncias que foram remetidas para investigação: foram remetidas para investigação **35 denúncias**, correspondendo a **15%** das denúncias remetidas para inquérito. A elas acrescem outras 82 denúncias de factos do mesmo teor, que não foram encaminhadas para investigação por não reunirem requisitos para esse efeito (sendo os denunciantes informados do direito, que sempre existe, de apresentarem queixa).

burlas com páginas "falsas"

24. Durante o ano de 2022 foi recebido um grande número 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 muito fiéis 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.

25. Tal como ocorreu com as burlas *online* em plataformas legítimas, este tipo de páginas foi-se multiplicando ao longo do ano, surgindo e desaparecendo muito rapidamente, consoante os agentes do crime iam auferindo proventos ou o respetivo URL era bloqueado, pelo servidor da *cloud* onde, invariavelmente, estavam alojados. No decurso de **2022** foram encaminhadas para **abertura de inquérito**, **35 das denúncias recebidas** a este respeito. Em 2021 tinham sido 28, registando-se, portanto, uma subida de 25%.

as investigações de *falsas* páginas de marcas de roupa e calçado aumentaram 25%

Este foi, conjuntamente com as burlas *online*, o conjunto **mais numeroso de participações encaminhado para inquérito**.

26. Além das *falsas* páginas de marcas de roupa, de marcas calçado ou de equipamento desportivo, este fenómeno manifestou-se também em *falsas* páginas de entidades que concedem crédito *online*, em *falsas* páginas de hotéis ou de alojamento local ou ainda de *falsas* páginas de venda de medicamentos e de venda de lenha e outros combustíveis de queima.

27. Em paralelo às denúncias resultantes deste fenómeno, 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 exame.

28. As denúncias de páginas falsas, das diferentes naturezas, encaminhadas para **abertura de inquérito, foram 41**, correspondendo a **17,67 % do total** das que foram remetidas para abertura de investigação. 17 outras denúncias recebidas não foram encaminhadas.

burlas no mercado imobiliário

29. Economicamente, uma das formas mais impactantes das burlas *online* ocorre no mercado imobiliário e passa por enganosas propostas de arrendamento de imóveis que não existem (ou que existindo, não pertencem ao anunciante, nem estão disponíveis para arrendamento).

São vítimas deste tipo de crime os 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, ou mesmo a generalidade dos cidadãos, quando procura uma casa para períodos de férias.

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.

triplicaram as investigações de burlas no arrendamento de casas (de férias, para estudantes e estrangeiros)

Durante o ano de 2022 foram encaminhadas para inquérito 10 das **47 denúncias** recebidas a este respeito. Anote-se que durante todo o ano de 2021 apenas tinham sido remetidas 3 denúncias deste tipo.

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

30. Tal como vem sucedendo desde o ano de 2020, outro dos fenómenos criminosos que mais motivou denúncias em 2022 foi o das defraudações relacionadas com plataformas de vendas *online* e com a aplicação de pagamentos MBWAY. Como ocorreu em anos anteriores, também em 2022 este fenómeno atingiu muitas vítimas, embora se note agora uma grande diminuição daquelas que efetivamente são enganadas pelos agentes criminosos. Talvez por haver mais conhecimento e mais sensibilidade geral para este tipo de atuação criminosa, a generalidade dos cidadãos que reportou este tipo de prática afirmou que não foi enganado, porque se apercebeu da mesma e não anuiu aos intentos dos agentes do crime. Todavia, houve ainda casos em que assim não ocorreu, tendo as vítimas efetivamente sido levadas a efetuar pagamentos indevidos aos criminosos.

31. Note-se que não se trata de meras burlas clássicas, em que um vendedor engana um comprador, como aquelas a que acaba de referir-se, nas secções anteriores. Este tipo de burla é de natureza diferente. Quem a comete não vende enganosamente bens a terceiros: pelo contrário, apresenta-se como comprador e, recorrendo a processos enganosos mais complexos leva as vítimas, que são vendedores, a fazer pagamentos ao criminoso, mesmo sabendo que estão a vender um bem e não a comprá-lo.

32. Durante 2022, observou-se que os métodos fraudulentos deixaram se ser relacionados com os enganos sobre a aplicação MBWAY e evoluíram para novas formas de defraudação, em que os criminosos procuram convencer os vendedores de produtos *online* a pagar antecipadamente (aos compradores) quantias que depois prometem devolver. Não obstante, registaram-se ainda assim **84 denúncias** por tentativas de defraudação com utilização da aplicação **MBWAY**.

Trata-se, em geral, de situações de crime de burla, de natureza semipública. Por isso e porque a maior parte das vítimas não foi enganada pelo processo criminoso, apenas 3 delas foram encaminhadas para inquérito.

33. Foram denunciadas muitas outras situações em que, logo que a vítima disponibilizou um bem para venda numa qualquer legítima plataforma *online*, foi abordada por um terceiro que manifestou vontade

de comprar aquele bem, sem o ver, sem saber qual era o respeito estado e sem discutir o seu preço. Estabeleceu todos os contactos sempre e apenas por via de mensagens de WhatsApp, escritas com evidentes erros, que indiciavam ter sido usado um tradutor automático (sendo portanto estrangeiro). De seguida, este agente criminoso informou que ia ser enviado a casa do vendedor um estafeta, para buscar o bem, levando com ele, em numerário, o dinheiro para pagamento do respetivo preço. Depois de acordado um dia e uma hora para a transação, informou ainda que a empresa transportadora afinal exigia que fosse feito um seguro, a pagar pelo vendedor – mas que o mesmo seria reembolsado pelo comprador. Nos casos em que o vendedor acedeu a pagar essa quantia, o criminoso não mais entrou em contacto, passando a ser impossível contactá-lo. Ficou com a quantia paga antecipadamente pelo vendedor e não pagou nunca o bem em causa.
Foram, porém, identificadas situações em que, por o vendedor se recusar a pagar a quantia, o comprador o abordou de forma agressiva e intimidatória, instando a fazê-lo.
Durante o ano de 2022 foram recebidas **43 denúncias** desta natureza.

burlas com criptomoedas e outros produtos financeiros

34. É também numericamente muito expressivo o conjunto de denúncias de defraudações em investimentos em criptoativos.
Anotou-se durante este ano, como nos anteriores, uma grande expansão da oferta de investimentos em criptomoedas e também no chamado mercado *forex*. Alguma desta oferta é criminosa e não tem qualquer outro propósito senão o de burlar terceiros. Pululam na Internet páginas supostamente correspondentes a entidades que aceitam e gerem investimentos em criptomoedas (*traders*), prometendo lucros muito rápidos e avultados. Recorrem a massivas campanhas publicitárias na Internet, muito visíveis e ruidosas, com frequência usando abusivamente a imagem de figuras públicas. Quando as vítimas são atraídas para elas, estas entidades criminosas recebem os respetivos investimentos e dão-lhes acesso a páginas na Internet onde se simula haver grandes ganhos no capital investido. Este processo é falso, porque não há qualquer real investimento. Quando o investidor pretende reaver o seu dinheiro, numa primeira fase, procuram dissuadi-lo, criando dificuldades burocráticas ou exigindo o pagamento preliminar de taxas elevadas, a título de supostas comissões. Numa segunda fase, pura e simplesmente deixa de ser possível contactá-las, desaparecendo da Internet.

35. Em 2022 foram recebidas pelo Gabinete Cibercrime **94 denúncias** (em 2021 tinham sido 38) de cidadãos que se queixaram de terem perdido, em inúmeras plataformas, avultadas quantias, que nalguns casos foram da ordem das dezenas de milhares de euros. Registou-se, pois, um **aumento muito significativo de denúncias**, que mais do que duplicaram. Na altura da queixa, a generalidade das plataformas tinha já deixado de estar *online*, não se conhecendo qualquer detalhe ou contacto que permitisse apurar o servidor da Internet onde estava a mesma alojada.

em 2022, as burlas relacionadas com investimentos em criptomoedas mais que duplicaram

Por outro lado, a generalidade das denúncias recebidas continha pouca informação e consistência, porque as vítimas também dispunham de pouca informação do contexto em que entregaram o seu dinheiro para supostamente realizarem investimentos. Invariavelmente transferiram o seu dinheiro para pessoas que não conheciam, nem viram nunca, com quem apenas falaram por telefone, ou até apenas por mensagens escritas. Na maior parte dos casos, a informação relacionada com estes supostos investimentos foi apenas sendo carreada para a plataforma fraudulenta que, subitamente, foi encerrada, deixando assim as vítimas com muito pouca informação comprovativa da burla que sofreram.

Por este motivo, somente parte das denúncias reunia condições para dar origem à abertura de investigação: apenas 20 de entre elas foram encaminhadas para inquérito. Ainda assim, os **inquéritos abertos respeitantes a fraudes em plataformas de criptomoedas** corresponderam a **8,62% do total** (232) do ano.

burlas em relações pessoais

36. Continuaram a ser recebidas em 2022 denúncias de burlas relacionadas com relacionamentos pessoais, amorosos, estabelecidos à distância, pela Internet, com desconhecidos (por exemplo, supostos militares da ONU em serviço em cenários de guerra, ou supostos comandantes de navios a navegar em alto mar, ou supostos médicos em serviço em zonas de outros conflitos militares).
Nestes casos, em geral, depois de uma aproximação por via da Internet aparentemente normal e inocente, toda a atuação dos criminosos acaba por desembocar na solicitação de quantias monetárias às vítimas. Em todas as situações deste tipo identificadas, os burlões não são quem anunciam ser, usam nomes e fotografias falsas e vivem em lugares que em nada coincidem com aqueles onde dizer residir.
Durante todo o ano de 2021 tinham sido recebidas pelo Gabinete Cibercrime 10 denúncias deste tipo; agora, em 2022, foram recebidas **26 denúncias** desta natureza. Como antes acontecera, as vítimas são, todas elas, senhoras de meia-idade que invariavelmente sofreram prejuízos de dezenas de milhares de euros.

burla invocando pagamentos em falta

37. Já em anos anteriores tinham sido denunciadas campanhas criminosas de expedição de mensagens telefónicas que, alegando estar em dívida um pagamento de dívida respeitante a eletricidade, levavam as vítimas a efetuar pagamentos não devidos, aos agentes criminosos.
Em 2022 foram recebidas 29 denúncias deste teor, embora a generalidade dos denunciantes tenha referido que não efetuou qualquer pagamento.

o fenómeno conhecido como "olá mãe, olá pai"

38. Surgiu, no outono de 2022, um fenómeno criminal que tem vindo a ser tratado pela comunicação social como burla "*olá mãe, olá pai*" e que se traduz na abordagem, por parte dos agentes criminosos, a vítimas, por via do WhatsApp, com o propósito de os convencer de que são os seus filhos e perderam o respetivo telefone, estando a utilizar um número provisório. O processo acaba sempre em pedidos de realização de transferências bancárias a favor de terceiros.
As denúncias deste tipo de burla começaram a surgir em setembro de 2022, tendo sido, desde então, recebidas **65 queixas** de crimes deste tipo. Na generalidade dos casos, os denunciantes manifestaram não ter sido efetivamente burlados, porque perceberam que estavam a ser alvos de uma tentativa criminosa. Portanto, na verdade, apenas um muito reduzido número de vítimas procedeu efetivamente aos pagamentos que lhe foram pedidos. Por este motivo, de entre as denúncias sinalizadas pelo Gabinete Cibercrime, apenas 6 delas deram origem a abertura de inquérito.
Nestes últimos casos, os pagamentos solicitados pelos agentes criminosos às vítimas variaram entre as muitas centenas de euros (o mais baixo registado foi de 750 euros) e os poucos milhares (nenhum pagamento solicitado ultrapassou os 4000 euros).

CEO fraud

39. Também continuaram a ser denunciadas ao Gabinete Cibercrime situações conhecidas na gíria policial como "*CEO fraud*", ou "*business email compromise*", técnica de engenharia social pela qual se pretende 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.
No decurso de 2022 foram recebidas pelo Gabinete Cibercrime **23 denúncias** desta natureza, das quais apenas 6 não foram encaminhadas para investigação. Durante o ano de 2021 tinham sido recebidas 14 denúncias deste tipo.

falsos telefonemas da Microsoft

40. Outro dos fenómenos que continuou a expandir-se em 2022 foi o do chamado "*technical support scam*", método de engenharia social que tem em vista convencer as vítimas de que os respetivos equipamentos informáticos estão infetados com vírus, persuadindo-os assim a facultar-lhes acesso remoto aos mesmos, ou a instalar neles *malware*, ou ainda a fazer-lhes pagamentos.
O processo criminoso passa pela realização de chamadas telefónicas fraudulentas em que, de forma astuciosa e enganadora, são abordados utilizadores da Internet, alegadamente pelo "apoio técnico" da Microsoft. A vítima é informada de que existe um problema técnico com o seu computador: em geral, refere-se que o computador está infetado com um vírus, ou foi atacado por *hackers*. Depois, informam que têm resolução para o problema. Foram identificados alguns casos em que a vítima foi "conduzida" a instalar *software* que lhe foi remetido por correio eletrónico (o qual supostamente seria adequado a resolver o suposto problema). Normalmente, este *software* é de origem maliciosa e pode danificar, roubar dados, encriptar ou até mesmo inutilizar o sistema. Noutros casos identificados, foi sugerido à vítima que acedesse a uma página na Internet e aí introduzisse dados confidenciais, como os do seu cartão de crédito ou de acesso à sua conta de email. Foram ainda identificadas situações em que o "atacante" pediu à vítima que partilhasse o seu ecrã e que, mantendo o ecrã partilhado, acedesse à sua conta de *homebanking*. Noutros casos referenciados, o "atacante" afirmou conseguir resolver o problema técnico mediante um pequeno pagamento, que a vítima podia saldar com o respetivo cartão de crédito (cujos dados então solicitou, ficando assim em posição de os vir a utilizar mais tarde, em seu proveito).

41. 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 criminosos falam 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. Por estas razões, embora todos os queixosos tivessem sido informados do direito de apresentação formal de queixa, não se encaminharam estes casos para investigação criminal (com uma exceção, apenas).
Em 2022 foram recebidas **50 denúncias** deste tipo no Gabinete Cibercrime. No decurso do ano de 2021 tinham sido recebidas 28 denúncias por factos desta natureza.

falsas convocatórias policiais

42. Surgiu em 2022, ganhando relevante intensidade, que se manteve ao longo de todo o ano, uma nova modalidade de burla *online*, que passa pela expedição de milhões 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. Caso o destinatário responda a esta mensagem, solicitando instruções para o pagamento, em resposta é facultado um NIB, para onde deve ser efetuada uma transferência – em geral, na ordem dos dois a três mil euros. Foi a este propósito emitido **Alerta Cibercrime de 30 de agosto de 2022**.

43. As mensagens deste tipo são muito rudimentares e os documentos anexos também. Referem recorrentemente nomes de autoridades nacionais. Não se afiguram, em geral, verosímeis. Porém, a verdade é que têm persistido, sendo sinalizadas com regularidade, o que indicia que os agentes do crime acabam por obter algum retorno desta atividade.
Durante o ano de 2022 foram recebidas **224 denúncias** deste tipo de crime, o que significa que, numericamente, este fenómeno de cibercrime é o **segundo mais frequente**, sendo apenas ultrapassado em dimensão pelo *phishing*.
Nenhum dos denunciantes referiu ter efetivamente transferido as quantias exigidas, não tendo por isso ficado patrimonialmente lesado, razão pela qual muito poucas das mensagens de correio eletrónico recebidas foram encaminhadas para abertura formal de inquérito.

ataques informáticos – ransomware *e acesso ilegítimo*

44. As denúncias respeitantes a crimes informáticos, ou *cibercrimes em sentido estrito*, recebidas pela linha cibercrime@pgr.pt, representaram em 2022 um conjunto significativo, tendo por vezes grande repercussão pública e mediática. Uma boa parte destas denúncias relatou ataques de ***ransomware***.
Foram, durante este ano, remetidas para investigação **20 denúncias** deste tipo (em 2021 tinham sido 13). A sua generalidade descrevia ataques a pequenas e médias empresas.
Às denúncias remetidas para investigação acrescem **71 outras** denúncias de mensagens de correio eletrónico contendo *malware* de diversa natureza, que não foram encaminhadas para investigação porque foram inconsequentes, isto é, porque os seus destinatários identificaram a sua natureza e acabaram por evitar ser vítimas das mesmas.

45. Porém, o fenómeno criminoso mais denunciado neste conjunto, de crimes informáticos ditos *puros*, ou *stricto sens*u, foi o do acesso ilegítimo. Durante o ano de 2022 foram recebidas pelo Gabinete Cibercrime, **81 denúncias** deste tipo – em 2021 tinham sido 8.
Dentro desta tipologia, a prática criminosa mais frequentemente denunciada foi a do acesso ilegítimo a contas de redes sociais. Desenhou-se de forma muito vincada em 2022 um fenómeno que já aflorara antes: o ataque informático especificamente dirigido a indivíduos muito presentes na Internet, designadamente em redes sociais, nalguns casos por razões profissionais, visando obter as suas credencias de acesso, para depois as alterar, bloqueando-lhe o respetivo acesso. Depois, exigiram pagamentos aos legítimos titulares das contas, para lhes devolverem o acesso às mesmas.
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.

46. Identificaram-se também casos de acessos ilegítimos a contas de correio eletrónico e de WhatsApp, em que os agentes do crime abordaram terceiras pessoas, incluídas da lista de contactos do legítimo titular daquela conta, como se fossem este último, solicitando quantias monetárias, alegando, por exemplo, estarem no estrangeiro, terem sido assaltados, ou precisando assim de ajuda monetária de amigos.

divulgação de dados privados e fotografias íntimas

47. Continuaram a ser recebidas, como tem ocorrido desde 2016, denúncias em que se relata violação da privacidade e divulgação *online* de dados pessoais (ou fotografias). É o caso de situações de uso não autorizado de fotografias, por exemplo para criação de perfis ou contas em páginas de encontros. Foi nalguns casos denunciada a disponibilização de anúncios de prostituição associando-se aos anúncios fotografias íntimas e dados verdadeiros das vítimas – o processo comummente referenciado como *revenge porn*.

Durante o ano, o Gabinete Cibercrime recebeu **28 denúncias** deste tipo.

48. Além deste específico fenómeno, foram também remetidas ao Gabinete Cibercrime denúncias de casos muito mais massificados, dando continuidade a situações que se vêm identificando nos últimos três a quatro anos. Foram recebidas denúncias de situações em que os agentes criminosos remetem a inúmeros destinatários (que desconhecem), mensagens de correio eletrónico por via das quais tentam convencer os destinatários a pagar-lhes quantias monetárias, em bitcoins, sob a ameaça de divulgação pública de dados, imagens ou informações pessoais das mesmas. Trata-se de uma tentativa massificada, em que o criminoso explora o desconhecimento e o receio da vítima, que não conhece e da qual não tem qualquer informação. No decurso do ano de 2022 foram recebidas **50 denúncias** deste tipo.

discurso de ódio* online*, crimes contra a honra e contra a propriedade intelectual

49. Estes fenómenos criminógenos foram muito significativos no passado. Porém, em 2022 **não tiveram expressão**. No seu conjunto, motivaram escassas denúncias, a maior parte delas de crimes conta a honra. Quanto a estes, pela natureza do ilícito em causa (e pelas exigências processuais penais associadas à mesma), o procedimento que tem sido 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).