MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

Nota Informativa

CIBERCRIME:
DENÚNCIAS RECEBIDAS
janeiro - junho 2022

13 de julho de 2022

ÍNDICE

CIBERCRIME:
DENÚNCIAS RECEBIDAS
janeiro – junho 2022

A. O CONTEXTO - CIBERCRIME

1. Comummente, inclui-se na expressão *cibercrime* um alargado conjunto muito heterogéneo de tipos legais de crime. Além dos ilícitos descritos na Lei do Cibercrime[1] (Lei nº 109/2009) assim acontece também com muitos outros crimes, quer incluídos no Código Penal[2], quer em diversas outras fontes legais avulsas[3].
Por este motivo, a quantificação estatística desta realidade (*cibercrime* em sentido mais alargado) não pode ser feita com rigor. São conhecidos os números dos crimes informáticos clássicos, mas na verdade, esta realidade criminal abrange também crimes tão diversos como burlas em plataformas de vendas ou de investimentos financeiros *online*, divulgação ilícita de fotografias, crimes contra a honra, difusão de pornografia infantil ou crimes contra o 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 neste meio, onde se expandiu de forma extraordinária.

2. As estatísticas da Justiça catalogam os ilícitos 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 existente sistema de estatísticas não está assim concebido de forma a permitir aperceber a dimensão numérica (estatística) deste complexo fenómeno.

3. Por isso, não é fácil avaliar, do ponto de vista estatístico, a real dimensão do cibercrime. O Gabinete Cibercrime da Procuradoria-Geral da República tem superado 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, a linha de recebimento de denúncias do endereço eletrónico do Gabinete Cibercrime (cibercrime@pgr.pt),

B. O PROCESSO DE RECEBIMENTO DE DENÚNCIAS

4. Com a finalidade de permitir aos cidadãos contactar com o Gabinete Cibercrime, está ativo, desde 2012, o endereço eletrónico cibercrime@pgr.pt, o qual, após o início de 2016 passou expressamente a aceitar também queixas da prática de crimes relacionados com a atividade do Gabinete.
Não estando ainda disponível uma ferramenta definitiva de comunicação eletrónica dos cidadãos com o Ministério Público, tem-se usado esta via para dar resposta às cada vez mais numerosas denúncias criminais remetidas por correio eletrónico, consequência da crescente digitalização da sociedade. As

[1] Falsidade informática, dano informático, sabotagem informática, acesso ilegítimo, interceção ilegítima, reprodução ilegítima de programa protegido e ainda os diversos crimes relacionados com meios de pagamento não corpóreos, introduzidos na ordem jurídica portuguesa por via da Lei nº 79/2021, de 24 de novembro.
[2] Designadamente a burla informática, a pornografia infantil ou o crime de abuso de cartão, que se tornou muito mais relevante após a alteração operada pela Lei nº 79/2021, de 24 de novembro.
[3] Por exemplo, os ilícitos criminais relacionados com a proteção de dados pessoais.

mensagens desta natureza, encaminhando denúncias relevantes para efeitos de processo penal, têm uma expressão numérica persistentemente crescente.

5. O Gabinete Cibercrime é um gabinete de coordenação nacional, criado pelo Conselho Superior do Ministério Público, nos termos do artigo 55º do Estatuto do Ministério Público. Não tem atribuições funcionais de direção da investigação criminal, nos termos do Código de Processo Penal – não lhe é legalmente permitido instaurar e dirigir concretas investigações criminais. Por esse motivo, quanto às denúncias que 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 as exigências formais (do Código de Processo Penal) a que o procedimento de queixa por correio eletrónico não consegue dar resposta.

6. Criaram-se critérios de análise destas queixas, tendo em vista a triagem daquelas que são remetidas para o DIAP de Lisboa, para abertura de inquérito, e aquelas que o não são.
Ainda que traduzam indicadores importantes da realidade do cibercrime, muitas das denúncias recebidas não reúnem elementos suficientes para abertura formal de um inquérito. Assim acontece, por exemplo, com algumas denúncias em que se dá conta de crimes meramente tentados, ou quanto a crimes particulares, ou ainda quanto a muitos dos crimes de natureza semipública. Sem apresentação formal de queixa pelo titular do direito à apresentação de queixa, muitas destas denúncias não reúnem condições processuais para que, apenas com origem nelas, seja aberto um inquérito. Por isso, sem prejuízo de se informarem os seus remetentes da possibilidade legal, que sempre existe, de apresentação de queixa formal, pelas vias normais, estas denúncias não são encaminhadas para abertura de inquérito.
O mesmo sucede com denúncias remetidas por pessoas que não se identificam (ou que não seja legal ou tecnicamente possível identificar), ou com denúncias descrevendo factos muito vagos ou genéricos. Também estas não são encaminhadas para inquérito.

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 consistentemente, de ano para ano, desde 2016. No ano de 2020 as denúncias aumentaram de forma excecional após a eclosão da pandemia da COVID–19. Em 2021, o aumento foi

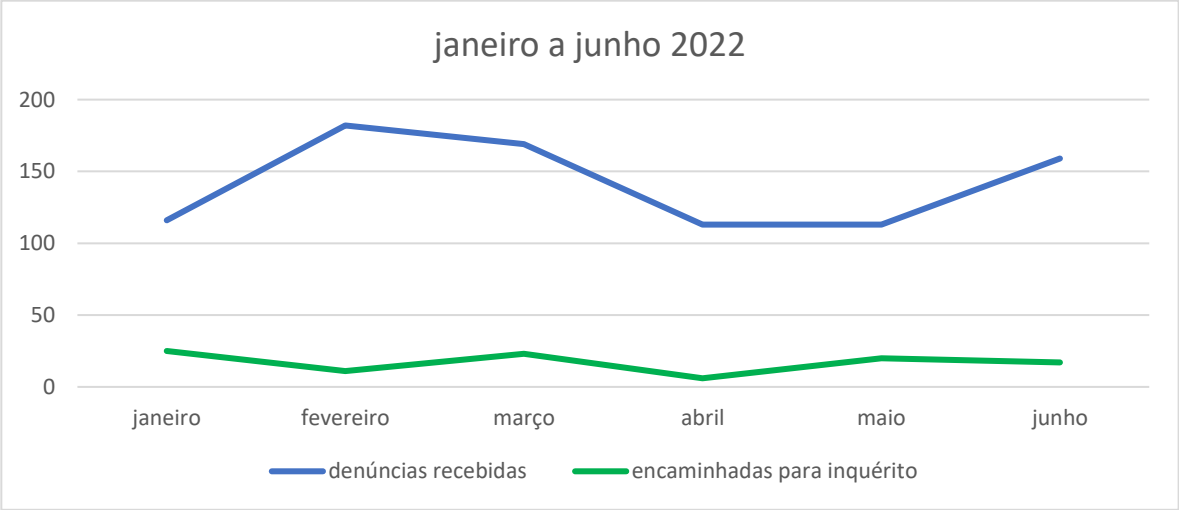
[4] As denúncias são remetidas para outros Departamentos de Investigação e Ação Penal, noutras comarcas, caso se aperceba liminarmente que os factos denunciados ocorreram na área geográfica de outra comarca, que não na de Lisboa. Em anos anteriores, apenas esporadicamente foi possível localizar as denúncias. A partir de 2021 (e também no que vai de 2022), esta possibilidade ocorreu com mais frequência.

ainda mais expressivo do que tinha sido em 2020: na totalidade do ano de 2021 foram recebidas 1160 denúncias, enquanto em 2020 tinham sido recebidas 544.
Os primeiros dados referentes a 2022 revelam que esta tendência de aumento se mantém: durante o primeiro semestre foram já recebidas 852 queixas. No período correspondente do ano de 2020 foram recebidas 305 denúncias e no mesmo período de 2021 foram recebidas 594.

9. Entre janeiro e junho de 2022 foram recebidas pelo Gabinete Cibercrime 852 denúncias, como melhor se descreve no quadro e no gráfico que seguem, onde se discriminam também aquelas que vieram a ser encaminhadas para abertura de inquérito (que foram 102). Do conjunto de todas as denúncias, 12 delas vieram a ser remetidas para a Polícia Judiciária, nos moldes que acima se referiram.

Denúncias Recebidas em 2022

mês	denúncias recebidas	encaminhadas para inquérito
janeiro	116	25
fevereiro	182	11
março	169	23
abril	113	6
maio	113	20
junho	159	17
total 1º semestre	**852**	**102**



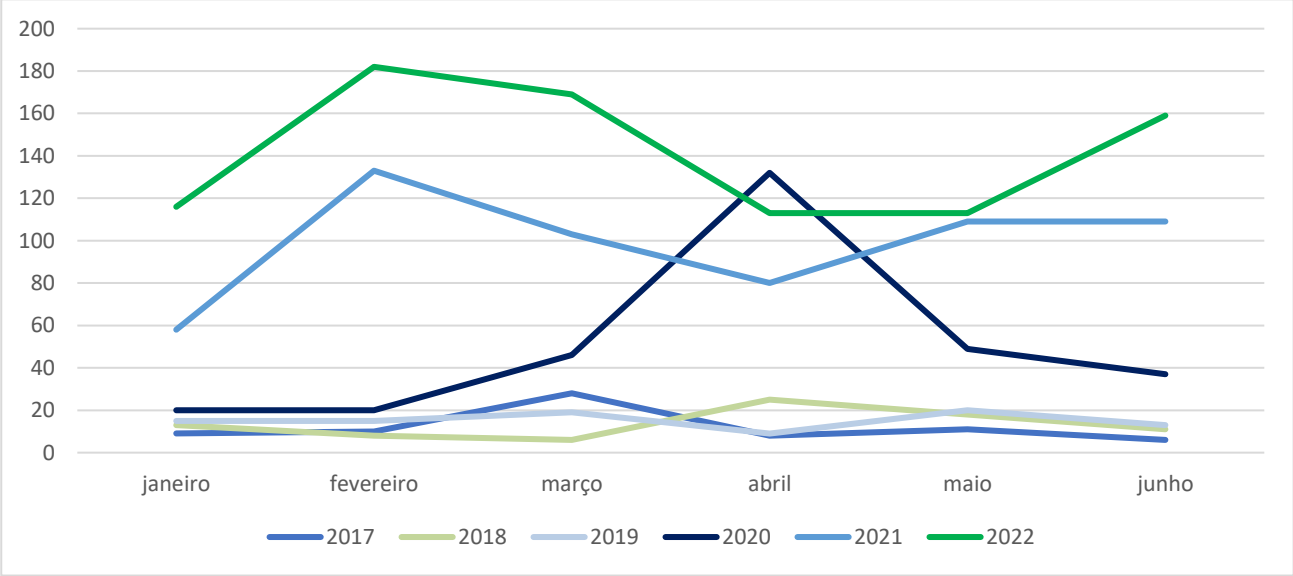
10. A análise do número de denúncias recebidas neste primeiro semestre revela, antes de mais, **que se mantém a tendência de consistente subida**. Entre janeiro e junho de 2022 o número de participações (852) atingiu valores correspondentes a 143% das queixas do mesmo período de tempo de 2021 (594) e correspondentes a 279% das do primeiro semestre de 2020 (305).
Tendo como referência o número de denúncias que deram entrada na totalidade do ano de 2021 (1160), neste primeiro semestre de 2022 já deram entrada participações correspondentes a 73,45 % das mesmas. Portanto, é de crer que, uma vez mais, no final do ano de 2022 os números das **participações entradas superem em muitíssimo as do ano anterior**.

as denúncias do primeiro semestre de 2022 ultrapassam em muito as do mesmo semestre do ano anterior (correspondem a 143%)

11. Observou-se alguma variação, de mês para mês. Porém, mesmo naqueles meses em que ocorreram menos denúncias (abril e maio, cada um deles, 113 participações e janeiro 116), ainda assim, registaram-se números superiores aos de qualquer dos meses de anos anteriores.
A esta conclusão tem apenas que fazer-se duas exceções: os meses de abril de 2020 e de fevereiro de 2021. Recorda-se que nestes dois meses, coincidentes com os períodos de confinamento decorrentes da pandemia provocada pela COVID-19, as denúncias aumentaram extraordinariamente. Todavia, com ressalva destes dois casos, sublinha-se, em cada um dos meses deste primeiro semestre foram registados números superiores aos de todos os meses dos anos anteriores.
Esta conclusão é evidenciada pelo quadro e pelo gráfico que seguem.

Denúncias Recebidas nos Primeiros Semestres 2017-2022

ano	janeiro	fevereiro	Março	Abril	Maio	Junho
2017	9	10	28	8	11	6
2018	13	8	6	25	18	11
2019	15	15	19	9	20	13
2020	20	20	46	131	51	37
2021	58	133	103	80	111	109
2022	116	182	169	113	113	159



12. Importa ainda sublinhar uma outra conclusão quanto aos valores excecionais ocorridos durante os confinamentos decorrentes da pandemia: os valores globais de queixas do primeiro semestre de 2022 são já muito superiores àqueles. Isto é, numa parte significativa dos meses de 2022 o número de participações que deram entrada foi muito superior ao dos meses críticos de abril de 2020 e de fevereiro de 2021.

o aumento verificado em 2022 é muito superior aos aumentos excecionais do período dos confinamentos, decorrentes da pandemia

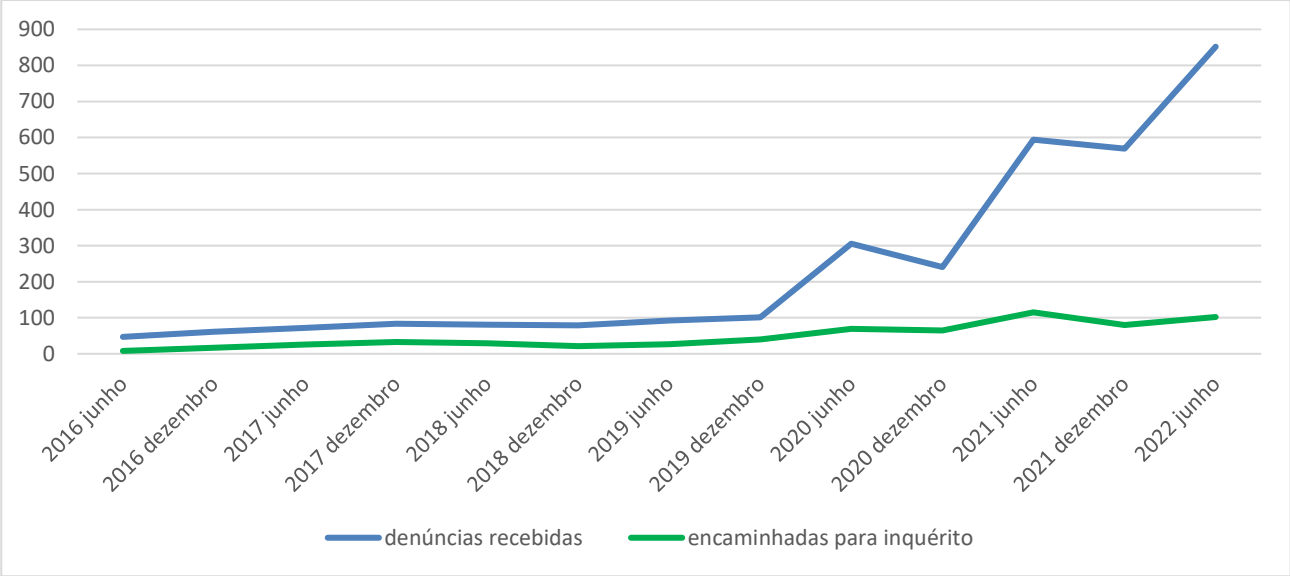
Portanto, sendo certo que naqueles meses ocorreram aumentos excecionais dos fenómenos de cibercriminalidade, é igualmente certo que no primeiro semestre de 2022, o aumento constante e persistente destes fenómenos ultrapassou aqueles valores excecionais. O incremento extraordinário do cibercrime

provocado pela pandemia foi pois 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 uma progressão, de ano para ano, do cibercrime. 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.
No quadro que vai de seguida, indicam-se as denúncias recebidas em cada ano, desde 2016. No gráfico que se lhe segue, os valores inscritos dividem-se por semestres, para permitir aperceber a dimensão deste primeiro semestre de 2022. Descrevem-se também, em ambos, aquelas denúncias que, de entre o conjunto total, foram encaminhadas para inquérito, em cumprimento dos critérios acima referidos.

denúncias 2016 - 2022

ano	denúncias recebidas	denúncias encaminhadas para inquérito
2016	108	25
2017	155	59
2018	160	50
2019	193	67
2020	544	138
2021	1160	195
2022 (apenas o 1º semestre)	852	102



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

desde 2016 é regular, constante e persistente o enorme aumento da cibercriminalidade, de ano para ano

D. CRIMINALIDADE MAIS FREQUENTE

15. Como se disse, 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 destas muitas centenas de denúncias não pode dar origem a dados estatísticos rigorosos, mas certamente permite que delas se infiram as grandes linhas do cibercrime que vitimiza os portugueses.

phishing

16. Numericamente, no primeiro semestre de 2022, a **tipologia criminosa mais reportada** ao Gabinete Cibercrime foi a do *phishing*. Durante todo o semestre sucederam-se inúmeras e diversas campanhas de *phishing*, com o propósito de facultarem aos seus autores os dados de acesso 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[5].

a tipologia criminosa mais denunciada foi a do *phishing*: 255 casos no primeiro semestre de 2022

17. Importa, porém, anotar que, como vem consistentemente sucedendo desde o início de 2021, esta metodologia tem vindo a deslocar-se. Isto é, tem passado menos a visar a acesso a contas bancárias, incidindo **mais intensamente sobre 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.

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.

Ao longo do semestre foram registadas variações no método específico utilizado. Nalguns casos as mensagens criminosas expedidas referiam enganosamente que existiam quantias a ser reembolsadas (chegando mesmo a ser, por vezes, abusivamente usadas imagens corporativas de diversas entidades, como a AT – Autoridade Tributária ou a EDP – Energias de Portugal, entre outras). Noutros casos, o processo criminoso passou pela expedição de mensagens de SMS ou WhatsApp, de forma indiscriminada, para números telefónicos aleatórios, solicitando o pagamento de uma "pequena taxa", relacionada com uma encomenda dirigida à vítima. Nos tempos que correm, este método é particularmente insidioso, por o comércio eletrónico estar em grande expansão e ser frequente a aquisição de bens *online*.

18. Ao longo do semestre, estas denúncias de *phishing* **(255 casos)** constituíram o conjunto mais numeroso do total das denúncias recebidas pelo Gabinete Cibercrime, correspondendo a **29,9% de todas as denúncias** recebidas.

19. Como acima se referiu, em novembro de 2021 o legislador nacional redesenhou o modelo incriminatório relacionado com meios de pagamento. 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

[5] Por estas razões, foi emitida, logo nos primeiros dias de 2022, o **Alerta Cibercrime de 13 de janeiro de 2022**.

falsos ou contrafeitos. Esta nova abordagem levou ao surgimento, neste primeiro semestre, de várias queixas relacionadas com o uso abusivo de dados de cartões. Foram recebidas no primeiro semestre 10 queixas deste teor (5 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 com criptomoedas e outros produtos financeiros

20. É também numericamente muito expressivo o conjunto de denúncias de defraudações em investimentos em criptoativos.
Anotou-se durante este semestre, 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.

as burlas relacionadas com investimentos em criptomoedas foram o segundo fenómeno mais numeroso

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 ser possível contactá-las, desaparecendo da Internet.

21. Entre janeiro e junho de 2022 foram recebidas pelo Gabinete Cibercrime **63 denúncias** 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. 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.
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 13 de entre elas foram encaminhadas para inquérito. Ainda assim, os inquéritos abertos respeitantes a fraudes em plataformas de criptomoedas corresponderam a **12,75% do total** (102) do semestre.

burlas *online*

22. 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.

23. Durante o primeiro semestre 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 e no Instagram). 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 efetivamente 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 mesmo.

24. 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.

Burlas no mercado imobiliário

25. Economicamente, uma das formas mais impactantes de burla *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 estrangeiros que passam em Portugal breves períodos de tempo, ou mesmo a generalidade dos cidadãos, quando procura uma casa para curtos 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.

houve um crescimento assinalável das burlas no arrendamento de casas

No primeiro semestre de 2022 foram recebidas **16 queixas** por estes motivos (dos quais 4 foram encaminhadas para inquérito). Anote-se que durante todo o ano de 2021 tinham sido recebidas 10 denúncias deste tipo.

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

26. Tal como vem sucedendo desde o ano de 2020, outro dos fenómenos criminosos que mais motivou denúncias no primeiro semestre de 2022, foi o das defraudações relacionadas com plataformas de vendas *online* e com a aplicação de pagamentos MBWAY. Como ocorreu em anos anteriores, também neste semestre este fenómeno atingiu muitas vítimas, embora se note agora uma grande diminuição daquelas que efetivamente são enganadas pelos agentes criminosos. Com efeito, 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 também 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.

27. 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.
Neste período, do primeiro semestre de 2022, observou-se que os métodos fraudulentos deixaram se ser tanto relacionados com os enganos sobre a aplicação MBWAY (embora ainda tenha havido casos) e evoluíram para novas formas de defraudação, em que os criminosos procuram convencer os vendedores de produtos *online* a pagar-lhes antecipadamente (aos compradores) quantias que depois prometem devolver.

28. Foram denunciadas muitas 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. 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.

29. Durante o primeiro semestre foram recebidas **61 denúncias** desta natureza. 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.

burlas com páginas "*falsas*"

30. Neste primeiro semestre 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.

31. 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.

32. 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.

33. Ao longo do semestre este tipo de páginas foi-se multiplicando, sendo denunciadas e identificadas, 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.

quase duplicaram as burlas em páginas falsas na Internet

Entre janeiro e junho de 2022, foram sinalizadas para **abertura de inquérito 23 das 42 denúncias** recebidas a este respeito. Anote-se que durante todo o ano de 2021 tinham sido recebidas 45 denúncias desta natureza. Este tipo de denúncias foi o conjunto mais numeroso de participações encaminhado para inquérito, correspondendo a **22,54 % do total** das aberturas de investigação.

burlas em relações pessoais

34. Continuaram a ser recebidas, durante o primeiro semestre de 2022, denúncias de burlas relacionadas com relacionamentos pessoais, amorosos, estabelecidos à distância, pela Internet, com desconhecidos (por exemplo, supostos militares da ONU em serviço no Iraque, 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, apenas neste primeiro semestre de 2022, foram recebidas **8 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.

falsas convocatórias policiais

35. Surgiu em 2022, ganhando relevante intensidade, que se manteve ao longo de todo o semestre, 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.

36. 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 primeiro semestre de 2022 foram recebidas *53 denuncias* deste tipo de crime, o que significa que, numericamente, este fenómeno de cibercrime é o **terceiro mais frequente**, sendo apenas ultrapassado em dimensão pelo *phishing* e pelas defraudações na utilização de plataformas de vendas *online* e em aplicações de pagamentos.
Nenhum dos denunciantes referiu ter efetivamente transferido as quantias exigidas, não tendo por isso ficado patrimonialmente lesado, razão pela qual nenhuma das mensagens de correio eletrónico recebidas foi encaminhada para abertura formal de inquérito.

ataques informáticos – ransomware e acesso ilegítimo

37. As denúncias respeitantes a crimes informáticos, ou *cibercrimes em sentido estrito*, recebidas pela linha cibercrime@pgr.pt, não representaram um conjunto muito numeroso, embora se reportem a fenómenos com grande repercussão pública e mediática. Uma parte destas denúncias relatou ataques de DDoS (*Distributed Denial of Service)* e outra ataques de *ransomware*.
Muito mais numerosa foram as denúncias deste tipo recebidas por outras vias (diretamente nos órgãos de polícia criminal, ou nos departamentos locais do Ministério Público), o que se percebe, pela dimensão e pelas consequências deste tipo de atos criminais. Não é frequente que a denúncia deste tipo de ataques seja remetida pelos próprios lesados, por via de correio eletrónico; pelo contrário, em geral estas denúncias são apresentadas de forma mais institucional, sendo normalmente patrocinadas por advogados, fazendo uso dos canais mais convencionais de apresentação de queixa.

38. Todavia, ainda assim, por via deste canal de comunicação (a linha cibercrime@pgr.pt), no primeiro semestre de 2022, foram recebidas **9 denúncias de *ransomware***. A sua generalidade descrevia ataques a pequenas e médias empresas.

39. Porém, o fenómeno criminoso mais denunciado neste conjunto, de crimes informáticos ditos *puros*, ou *stricto sensu*, foi o do acesso ilegítimo.
Dentro desta tipologia, a prática criminosa mais frequentemente denunciada foi a do acesso a contas de correio eletrónico e a contas de redes sociais. Desenhou-se de forma muito mais vincada neste semestre um fenómeno que já aflorara antes: o ataque informático especificamente dirigido a indivíduos muito presentes na Internet, designadamente em redes sociais, visando obter as suas credencias de acesso, para depois as alterar. Ao longo do semestre foram-se avolumando denúncias de queixosos que, sendo titulares de contas em redes sociais, que usam frequentemente, nalguns casos por razões profissionais, se viram privados do acesso a tais contas, pela ação de agentes criminosos. Estes, por métodos variados nem sempre identificados, lograram capturar de forma ilícita as respetivas credenciais de acesso, que alteraram. 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.

40. No caso das contas de correio eletrónico e de WhatsApp, foram denunciados casos em que, após a *captura* das credenciais de acesso, os agentes do crime abordaram os contactos do legítimo titular

daquela conta, como se fossem este último, solicitando quantias monetárias, alegando, por exemplo, estarem no estrangeiro, terem sido assaltados, precisando assim de ajuda monetária de amigos.

41. Durante o primeiro semestre de 2022, foram denunciados ao Gabinete Cibercrime, nas suas diversas modalidades, **39 casos de acesso ilegítimo**, dos quais 14 foram encaminhados para abertura de inquérito.

falsos telefonemas da Microsoft

42. Outro dos fenómenos que continuou a expandir-se no primeiro semestre de 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).

43. Trata-se de chamadas telefónicas que 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. Visam vítimas de todo o mundo e não especificamente vítimas de Portugal. Na maior parte dos casos os denunciantes que contactaram o Gabinete Cibercrime conseguiram identificar 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).
Entre janeiro e junho de 2022, foram recebidas **47 denúncias** deste tipo no Gabinete Cibercrime. É um número expressivo, correspondendo a 5**,52% do total** das queixas. Realça-se que no decurso de todo o ano de 2021 tinham sido recebidas apenas 28 denúncias por factos desta natureza.

CEO fraud

44. Também continuaram a ser denunciadas ao Gabinete Cibercrime situações da chamada "*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 do primeiro semestre de 2022 foram recebidas pelo Gabinete Cibercrime **10 denúncias** desta natureza, das quais apenas duas não foram encaminhadas para investigação. Anota-se que, durante todo o ano de 2021, tinham sido recebidas 14 denúncias deste tipo.

divulgação de dados privados e fotografias íntimas

45. 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 na criação de perfis ou contas em páginas de encontros. Foi nalguns casos denunciada a disponibilização de anúncios de prostituição, em páginas específicas, associando-se aos anúncios fotografias íntimas e dados verdadeiros das vítimas – o processo comummente referenciado como *revenge porn*.

46. Noutros casos, de tipo diferente, que ainda ocorreram neste semestre, embora em menor número que no passado, as denúncias reportavam a exigência de quantias sob pena de divulgação de imagens íntimas de natureza sexual – a situação conhecida comummente como *sextortion* – ocorrendo sobretudo com vítimas que, *online*, travaram conhecimento com pessoas desconhecidas.

47. 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 anos. Assim, foram recebidas denúncias de situações em que os agentes criminosos, por via de mensagens de correio eletrónico, que mandam para milhares de destinatários, tentam convencer vítimas 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.

48. Neste semestre as queixas relatadas nos três parágrafos anteriores foram 13 quanto ao primeiro tipo e 26 quanto ao conjunto do segundo e do terceiro tipo. Estes tipos de criminalidade são normalmente muito insidiosos e provocam grandes traumas pessoais nas vítimas. Representaram **4,58% das denúncias** recebidas.

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

49. Estes fenómenos criminógenos foram muito significativos no passado. Porém, no segundo semestre de 2022 **não tiveram expressão**. Não motivaram qualquer denúncia, com exceção dos crimes conta a honra.
E mesmo estes, apenas deram origem a 4 participações durante todo o primeiro semestre de 2022. Porém, ainda assim, 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).