MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

Nota Informativa

CIBERCRIME:
DENÚNCIAS RECEBIDAS
janeiro - junho 2023

30 de setembro de 2023

ÍNDICE

CIBERCRIME:
DENÚNCIAS RECEBIDAS
janeiro – junho 2023

A. O CONTEXTO - CIBERCRIME

1. A expressão *cibercrime* é comummente utilizada para abarcar um alargado conjunto, muito heterogéneo e abrangente, de tipos legais de crime: desde logo, os descritos na Lei do Cibercrime[1], mas também muitos outros, 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, ou *cibercrimes em sentido restrito*, mas, na verdade, esta realidade criminal abrange também outros 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 de ódio *online*. Todas estas práticas criminosas se têm expandido, à velocidade da massificação do uso das redes de comunicações eletrónicas.

2. Estas circunstâncias impedem 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 meramente 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. Desde 2016, o endereço eletrónico cibercrime@pgr.pt tem recebido denúncias de cidadãos, 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

[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.

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.

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 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 ainda mais expressivo, mais que duplicando. Em 2022 esta tendência manteve-se. Os primeiros dados referentes a **2023** revelam que esta **tendência de aumento se mantém**, embora menos acentuada: durante o **primeiro semestre** foram recebidas **1363 denúncias** – no período correspondente do ano de 2020 foram recebidas 305 denúncias, no de 2021 foram recebidas 594 e no de 2022, 852 denúncias. Entre o primeiro semestre de 2022 e o correspondente período de 2023 registou-se um **aumento de 59,97%** no número de denúncias.

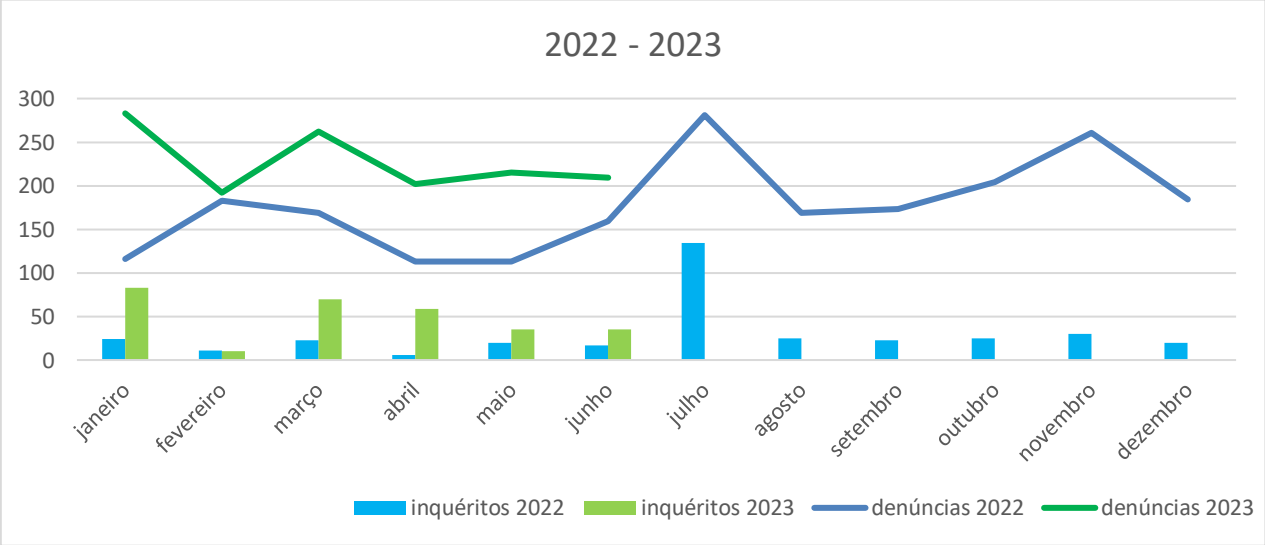
9. Como se referiu e melhor se descreve no quadro e no gráfico que seguem, entre janeiro e junho de 2023, foram recebidas pelo Gabinete Cibercrime 1363 denúncias. Também ali se discriminam aquelas denúncias que vieram a ser **encaminhadas para abertura de inquérito** (que foram **292**).

[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.

Comparativamente, apresentam-se os correspondentes dados de 2022 (de ambos os semestres). Quanto a 2023, do conjunto de todas as denúncias, 14 delas vieram a ser remetidas para a Polícia Judiciária, nos moldes que acima se referiram.

Denúncias Recebidas em 2022 e 2023 (primeiros semestres)

	denúncias recebidas		**encaminhadas para inquérito**	
	2022	**2023**	**2022**	**2023**
janeiro	116	283	25	83
fevereiro	182	192	11	10
março	169	262	23	70
abril	113	202	6	59
maio	113	215	20	35
junho	159	209	17	35
total 1º semestre	**852**	**1363**	**102**	**292**
julho	281		134	
agosto	169		25	
setembro	173		23	
outubro	204		25	
novembro	261		30	
dezembro	184		20	
total do ano	**2124**		**359**	



10. Observou-se alguma variação, de mês para mês. Porém, mesmo naqueles meses em que ocorreram menos denúncias, ainda assim, registaram-se números muito superiores aos de qualquer dos meses do mesmo semestre do ano anterior.

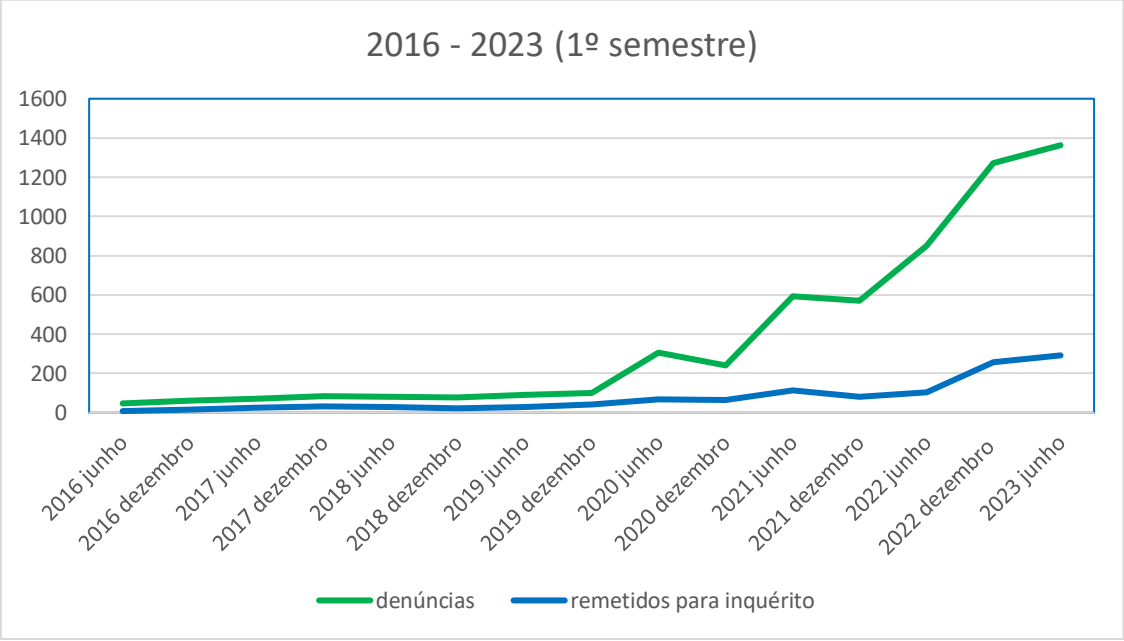
as denúncias do primeiro semestre de 2023 ultrapassam em muito as do mesmo semestre do ano anterior (correspondem a 159,97%)

11. Os números constantes da tabela seguinte, visualmente representados no gráfico que se lhe segue, revelam igualmente uma clara progressão do

cibercrime, de ano para ano, renovada neste semestre. Como tem resultado dos números registados em anos anteriores, a progressão do cibercrime é constante e consistente.
No quadro que vai de seguida, indicam-se as denúncias recebidas em cada ano, desde 2016. No gráfico, os valores inscritos dividem-se por semestres, para que melhor se aperceba a dimensão deste primeiro semestre de 2023. 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 - 2023

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	2124	359
2023 **(apenas o 1º semestre)**	1363	292



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

13. Numericamente, as denúncias recebidas por via do endereço cibercrime@pgr.pt representam apenas uma pequena parcela do conjunto total das denúncias de cibercriminalidade apresentadas pelos cidadãos ao Ministério Público. Por essa razão, a informação recolhida destes já milhares de denúncias não gera dados estatísticos rigorosos. Porém, sendo uma amostra transversal, 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 semestres anteriores foi diferente daquela que ocorreu no primeiro semestre de 2023 e será também seguramente diferente da que o segundo semestre revelará.

14. Já se referiu que o primeiro semestre de 2023 revelou um aumento do número de denúncias recebidas e também um aumento daquelas que foram remetidas para inquérito. Como se disse, neste período de tempo foram recebidas pelo Gabinete Cibercrime 1363 denúncias, das quais 292 vieram a ser **encaminhadas para abertura de inquérito** – portanto, **21,42% das denúncias**. No equivalente semestre de 2022, tinham sido recebidas 852 denúncias, das quais 102 foram encaminhadas para inquérito (portanto, 11,97%).

15. Este aumento de denúncias remetidas para inquérito resultou, entre outros fatores, do surgimento de algumas campanhas criminosas específicas. Assim, logo no mês de janeiro surgiu uma campanha criminosa que afetou muitas vítimas, centrada numa plataforma *online* que, recrutou pessoas para que supostamente visualizassem filmes, com o objetivo de fazer subir o respetivo "rating". Supostamente, tais pessoas seriam pagas por cada visualização. Afinal, verificou-se que todo este negócio era criminoso e fraudulento, acabando as pessoas recrutadas por ser burladas em valores de milhares de euros. Este fenómeno foi denunciado ao Gabinete Cibercrime e as respetivas participações vieram a dar origem a 51 investigações.

O "PHISHING" CONTINUA A SER UM FENÓMENO MASSIVO

16. Numericamente, no primeiro semestre de 2023, 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 cartões bancários de pagamento das vítimas. O tradicional *phishing* dirigido às contas bancárias tem vindo a ser dirigido, quase integralmente, a dados de cartões de crédito[5]. Esta evolução tem com certeza origem no reforço das medidas de segurança de acesso às contas de *homebanking*, designadamente com a implementação de múltiplos fatores de autenticação.

a tipologia criminosa mais denunciada foi a do *phishing*: 209 casos no primeiro semestre de 2023

17. Porém, o modelo da atuação criminal permaneceu inalterado: continua a passar pela remessa de milhares de mensagens eletrónicas. Ao contrário do que acontecia no passado, em vez do *email*, os agentes criminosos passaram a utilizar mais o WhatsApp. O propósito manteve-se: induzir as vítimas a aceder a páginas *falsas*, por si geridas, onde são incentivadas a introduzir os dados dos seus cartões de crédito.
No passado, foram muito utilizadas mensagens que referiam enganosamente que existiam quantias a ser reembolsadas. Neste semestre, este tipo de mensagens deixou de se verificar. Passaram a predominar as mensagens que solicitavam o pagamento de uma "pequena taxa", relacionada com uma encomenda dirigida à vítima e, sobretudo, as mensagens em que apenas se pedia a autenticação do titular do cartão, com todos os dados do mesmo.

18. Ao longo do semestre, estas denúncias de *phishing* (**209 casos**) constituíram o conjunto mais numeroso do total das denúncias recebidas pelo Gabinete Cibercrime, correspondendo a **15,33 % do total** das 1363 denúncias recebidas. É um número expressivo, mas ainda assim menor que aquele que

[5] Durante o primeiro semestre de 2023 apenas foram denunciados três casos de phishing especificamente visando as credenciais de acesso a bancos.

se registou no correspondente semestre de 2022, período no qual foram recebidas 292 denúncias de *phishing*, num universo total de 852 (portanto, correspondendo a 29,9% de todas as denúncias recebidas). Esta tendência, de diminuição relativa das denúncias de *phishing*, tinha já sido anotada no segundo semestre de 2022.
No passado, foram emitidos vários **Alertas Cibercrime** a este respeito, disponíveis **aqui**. Já neste primeiro semestre de 2023, foram emitidos, também a este propósito, o **Alerta Cibercrime de 5 de julho de 2023** e o **Alerta Cibercrime de 3 de julho de 2023**. No semestre anterior tinham sido emitidos os Alertas Cibercrime de **10 de outubro de 2022** e de **29 de setembro de 2023**.

19. Recorda-se que nesta área, das fraudes relacionadas com os cartões de bancários de pagamento, após novembro de 2021 o legislador nacional redesenhou o modelo incriminatório, passando 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.
Tal como acontecera já em semestres anteriores, em consequência desta alteração legislativa foram recebidas várias participações relacionadas com o uso abusivo de dados de cartões: a totalidade das 13 denúncias recebidas foram remetidas para investigação. Todas elas se reportavam ao **uso abusivo de dados de cartões**, por agentes desconhecidos, em compras na Internet.

20. 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*.

OCORREM CADA VEZ MAIS BURLAS EM NEGÓCIOS *ONLINE*

21. Todos os indicadores apontam no sentido de que o comércio eletrónico se desenvolve persistentemente 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.

os *burlões* "migraram" para o ambiente *online* e para as plataformas digitais de compra e venda

22. Durante o primeiro semestre de 2023 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 em 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, "desaparecendo" e nada mais se sabendo dele.

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.

No primeiro semestre de 2023 foram **remetidos para inquérito 41 denúncias** em que se relatam factos desta natureza (correspondentes a **14,04 %** do total das 292 **denúncias remetidas para investigação**). Este número supera o do correspondente semestre de 2022, no qual tinham sido remetidas para inquérito 35 denúncias.
Quanto a muitas outras denúncias de factos do mesmo teor, não foram encaminhadas para investigação por facultarem escassa informação ou, por de qualquer outra forma, não reunirem requisitos para esse efeito (sendo os denunciantes informados do direito, que sempre existe, de apresentarem queixa formal).

burlas no mercado imobiliário

24. Economicamente, uma das formas mais lesivas das burlas *online* é a que tem ocorrido no mercado imobiliário. 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 primordiais 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.
Durante o primeiro semestre de 2023 foram recebidas 11 denúncias desta natureza. A este respeito foi emitido o **Alerta Cibercrime de 12 de julho de 2023.**

burlas com criptoativos

25. É também economicamente muito significativo o valor das fraudes relacionadas com investimentos em criptoativos.
Anotou-se durante este semestre, como nos anteriores, uma grande expansão da oferta de investimentos em criptoativos, particularmente por via de plataformas criminosas, que não têm qualquer outro propósito senão o de burlar terceiros. Surgem na Internet (e rapidamente desaparecem) páginas supostamente correspondentes a entidades que aceitam e gerem investimentos desta natureza (supostos *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 cripto ativos têm provocado prejuízos patrimoniais muitíssimo avultados

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.

26. Entre janeiro e junho de 2023 foram recebidas pelo Gabinete Cibercrime **33 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 estes motivos, somente uma pequena parte das denúncias (6 delas) reunia condições para dar origem à abertura de investigação.

burlas com páginas "*falsas*"

27. Tal como já aconteceu no ano anterior, neste primeiro semestre de 2023 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.

28. 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.

29. 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.

30. 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.
Entre janeiro e junho de 2023, foram encaminhadas para **abertura de inquérito as 42 denúncias** recebidas a este respeito – representando **14,38 %** do total das **denúncias remetidas**.

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

31. Tal como vem sucedendo desde a eclosão da pandemia COVID-19, em 2020, outro dos fenómenos criminosos que motivou muitas denúncias no primeiro semestre de 2023, 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 vítimas, embora se note,

tal como nos semestres anteriores, diminuição daquelas que efetivamente são enganadas pelos agentes criminosos. Há com certeza mais conhecimento e mais sensibilidade geral para este tipo de atuação criminosa. Por isso, na generalidade, os cidadãos que reportaram este tipo de prática afirmaram que não foram enganados, porque se aperceberam daquilo que estava a ocorrer e não cederam 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.

32. Este procedimento criminoso não é uma mera burla clássica, pela qual um vendedor desonesto engana um comprador. Trata-se de um procedimento mais complexo e sofisticado. Neste caso, o criminoso não vende enganosamente um bem a um terceiro: pelo contrário, apresenta-se como comprador e, recorrendo a processos fraudulentos mais rebuscados leva a vítima, que é vendedora de um bem, a fazer-lhe pagamentos, mesmo sabendo que está a vender um bem e não a comprá-lo.
Neste primeiro semestre de 2023, ainda se registaram **30 denúncias** por tentativas de defraudação com utilização da aplicação **MBWAY**. Como se trata, em geral, de situações de crime de burla, de natureza semipública e, por outro lado, a generalidade das vítimas não foi enganada pelo processo criminoso, muito poucas delas foram encaminhadas para inquérito.

33. Tem-se, porém, observado que, gradualmente, os métodos fraudulentos relacionados com os enganos sobre a aplicação MBWAY, evoluíram para novas formas de defraudação. Os criminosos continuam a procurar convencer os vendedores de produtos *online* a pagar-lhes quantias, mas utilizando outros argumentos.
Mantém-se o modelo de abordar um vendedor, logo que este disponibiliza um bem para venda numa qualquer legítima plataforma *online*. Do mesmo modo, o criminoso manifesta vontade de comprar aquele bem sem o ver, sem saber qual é o respeito estado de conservação e sem discutir o seu preço. Estabelece todos os contactos sempre e apenas por via de mensagens de WhatsApp, por vezes com evidentes erros de linguagem, indiciando ter sido usado um tradutor automático (parecendo, portanto, que o criminoso não fala português). De seguida, este agente criminoso informa que vai 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, informa ainda que a empresa transportadora afinal exigia que seja feito um seguro, a pagar pelo vendedor – mas que o mesmo será reembolsado pelo comprador.

34. Nos casos identificados em que o vendedor acedeu a pagar antecipadamente essa quantia, correspondente a um suposto seguro, 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, que não foi buscar.
A este respeito foi emitido o **Alerta Cibercrime de 11 de maio de 2023**.

AUMENTARAM AS INICIATIVAS CRIMINOSAS FRAUDULENTAS POR VIA DE COMUNICAÇÕES

falsas convocatórias policiais

35. Surgiu em 2022, ganhando relevante intensidade, uma modalidade de burla *online*, que permaneceu muito ativa no primeiro semestre de 2023, a qual passa pela expedição de milhares 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. Durante o primeiro semestre de 2023 foram recebidas **92 denúncias** deste tipo de crime – no período correspondente do ano de 2022 tinham sido recebidas 53 denúncias.
As mensagens deste tipo são muito rudimentares e os documentos anexos também. Referem recorrentemente nomes de autoridades nacionais, tais como a Procuradora-Geral da República, ou o Diretor Nacional da Polícia Judiciária, ou o Diretor Nacional da Polícia de Segurança Pública. Não se afiguram, em geral, nada 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.
Em todo o caso, nenhum dos denunciantes referiu ao Gabinete Cibercrime ter efetivamente transferido as quantias exigidas, não tendo por isso ficado patrimonialmente lesado. Por estas razões, a generalidade das mensagens de correio eletrónico recebidas não foi encaminhada para abertura formal de inquérito.
A este respeito foi emitido, já no semestre anterior, o **Alerta Cibercrime de 30 de agosto de 2022**, cuja atualidade se mantém plenamente válida.

37. No final de 2022 tinha surgido uma variante do fenómeno criminal que acaba de descrever-se, a qual veio a assumir crescente frequência ao longo do primeiro semestre de 2023 e se tornou muitíssimo presente no fim do semestre. Nesta nova modalidade, a abordagem às vítimas foi feita pela realização massiva de **chamadas telefónicas**, para destinatários indiscriminados, os quais são informados de que o seu documento nacional de identificação foi relacionado com **criminalidade internacional grave**, motivo pelo qual foi já emitido um mandado de detenção em seu nome.
Nesta abordagem, por métodos ardilosos, o criminoso leva a vítima a facultar-lhe os seus dados de identificação e também bancários, com o propósito de a convencer a transferir quantias monetárias para contas que lhe indica. Já após o fim do primeiro semestre de 2023 veio a ser emitido a este respeito o **Alerta Cibercrime de 18 de agosto de 2023**.

supostos pagamentos de eletricidade em falta

38. Já em anos anteriores tinham sido denunciadas campanhas criminosas de expedição de mensagens escritas que, alegando estar em dívida um pagamento de dívida respeitante a fornecimento de eletricidade, levavam as vítimas a efetuar pagamentos não devidos, aos agentes criminosos.
No **primeiro semestre de 2023 foram recebidas 186 denúncias deste teor**, embora a generalidade dos denunciantes tenha referido que não efetuou qualquer pagamento. Não obstante, em 86 destes casos, as denúncias foram encaminhadas para investigação, a qual se concentrou parcelarmente no DIAP de Lisboa.
A enorme difusão deste fenómeno criminoso motivou a emissão do **Alerta Cibercrime de 23 de março de 2023**.

o fenómeno conhecido como "*olá mãe, olá pai*"

39. 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 intensificaram-se durante o primeiro semestre de 2023, durante o qual foram recebias **33 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. 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 5 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 (o mais expressivo pagamento identificado foi de 4000 euros).
A expansão deste tipo de burla levou à emissão do **Alerta Cibercrime de 3 de maio de 2023**.

falsos telefonemas da Microsoft

40. Outro dos fenómenos que continuou a ser denunciado no primeiro semestre de 2023 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 com o seu computador: em geral, refere-se que o computador está infetado com um vírus, ou foi atacado por *hackers*. Depois, é informada de que existe solução, sendo foi "conduzida" a instalar *software*, normalmente de origem maliciosa. 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*.

41. Trata-se de chamadas telefónicas que não têm origem em Portugal, provindo de países 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, em geral não se encaminharam estes casos para investigação criminal.

42. Entre janeiro e junho de 2023 foram recebidas 6 denúncias desta natureza – muito menos que as 47 que foram recebidas no período correspondente do ano de 2022. Anota-se assim uma clara quebra desta prática criminosa, aliás já identificada na parte final do ano de 2022.

"CEO fraud"

43. Também continuaram a ser denunciados ao Gabinete Cibercrime burlas do tipo "*CEO fraud*", ou "*business email compromise*", técnica de engenharia social pela qual criminosos pretendem 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 2023 foram recebidas pelo Gabinete Cibercrime **17 denúncias** desta natureza, todas elas encaminhadas para investigação. Anota-se que, durante todo o ano de 2021, tinham sido recebidas 14 denúncias deste tipo. Por sua vez, apenas no primeiro semestre de 2022, tinham sido recebidas 10 denúncias. Afigura-se, portanto, que este fenómeno criminoso está em expansão.

SUBSISTEM OS CLÁSSICOS CRIMES NAS REDES

44. 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, poe vezes, com repercussão pública. A parte mais significativa destas denúncias relatou ataques de *ransomware* e de acesso ilegítimo.
Muito mais numerosas 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.

45. Todavia, ainda assim, de entre as denúncias recebidas por este canal de comunicação (a linha cibercrime@pgr.pt), no primeiro semestre de 2023, foram remetidos para investigação 5 casos de *ransomware* e 9 de acesso ilegítimo.

divulgação de dados privados e fotografias íntimas

46. Continuaram a ser recebidas, como tem ocorrido desde 2016, denúncias em que se relata violação da privacidade e divulgação *online* de dados pessoais. 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 utilização da imagem de vítimas em anúncios de prostituição, associando-se aos anúncios os dados verdadeiros daquelas vítimas – o processo comummente referenciado como *revenge porn*.

47. 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.

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 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. Neste semestre, este tipo de denúncias, foi menos expressivo que no passado, totalizando 21 queixas – no conjunto do ano de 2022 tinham sido

recebidas 50 denúncias desta natureza. Agora, no primeiro semestre de 2023, apenas foram encaminhadas para inquérito 3 delas.

discurso de ódio *online*, crimes contra a honra

49. Estes fenómenos criminógenos foram muito significativos no passado. Vieram, porém, a perder expressão significativa. Todavia, no primeiro semestre de 2023, registaram-se algumas denúncias, sobretudo de crimes contra a honra (17 denúncias).

Pela natureza do ilícito em causa (e pelas exigências processuais penais associadas à mesma), o procedimento adotado tem sido sempre 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).