



**MINISTÉRIO PÚBLICO
PORTUGAL**

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

Nota Informativa

**CIBERCRIME:
DENÚNCIAS RECEBIDAS
2021**

25 de janeiro de 2022

ÍNDICE

A. O CONTEXTO – CIBERCRIME	3
B. O PROCESSO DE RECEBIMENTO DE DENÚNCIAS	3
C. AS DENÚNCIAS RECEBIDAS	5
D. CRIMINALIDADE MAIS FREQUENTE	9
<i>phishing</i>	9
<i>phishing</i> – dados de cartões de crédito	9
burlas <i>online</i>	10
burlas com páginas “falsas”	11
burlas com criptoativos e outros produtos financeiros	12
burlas em relações pessoais	12
CEO <i>fraud</i>	12
ataques informáticos	13
falsas chamadas da Microsoft	13
divulgação de fotografias e outra informação pessoal	14
<i>stalking</i> e <i>sextortion</i>	14
discurso de ódio online	14
violação de direito de autor	15
crimes contra a honra	15
defraudações na utilização da aplicação de pagamentos MBWAY	15

CIBERCRIME: DENÚNCIAS RECEBIDAS 2021

A. O CONTEXTO - CIBERCRIME

1. Comumente, inclui-se na expressão *cibercrime* um alargado conjunto muito heterogéneo de tipos legais de crime. Além dos ilícitos descritos na Lei do Cibercrime¹ (Lei nº 109/2009) assim acontece também com muitos outros crimes, quer incluídos no Código Penal², quer em diversas outras fontes legais avulsas³.

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 ditos *clássicos*, mas na verdade, esta realidade criminal abrange também crimes tão diversos como burlas em plataformas de vendas *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, em geral, 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. Além desta vertente comunicacional geral, a partir do início de 2016, esta linha de comunicação passou também a aceitar 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

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.

criminais remetidas por correio eletrónico, consequência da crescente digitalização da sociedade. Na verdade, as mensagens desta natureza, encaminhando denúncias relevantes para efeitos de processo penal, têm uma expressão numérica persistentemente crescente. Após a eclosão da pandemia da COVID-19, no início de 2020, esta via de comunicação assumiu ainda mais importância.

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, pois, atribuições funcionais de direção da investigação criminal, nos termos do Código de Processo Penal – não lhe é legalmente permitido, portanto, 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 Público⁴. 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. 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 não o são.

Ainda que traduzam indicadores importantes da realidade do cibercrime, muitas das denúncias recebidas não reúnem elementos ou condições suficientes para abertura formal de uma investigação. 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 sob anonimato, ou 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.

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. Durante o ano de 2021 esta possibilidade ocorreu com muito mais frequência.

C. AS DENÚNCIAS RECEBIDAS

8. As denúncias de *ciber crimes* 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, designadamente após a eclosão da pandemia resultante da COVID-19. Em 2021, o aumento foi ainda mais expressivo do que tinha sido em 2020: entre 1 de janeiro e 31 de dezembro de **2021 foram recebidas 1160 denúncias** – durante todo o ano de **2020 tinham sido recebidas 544**.

De uma forma genérica pode dizer-se que, desde 2019, de ano para ano, **as queixas recebidas mais que duplicam o número das denúncias do ano anterior**.

Denúncias em 2019:

193

Denúncias em 2020:

544

Denúncias em 2021:

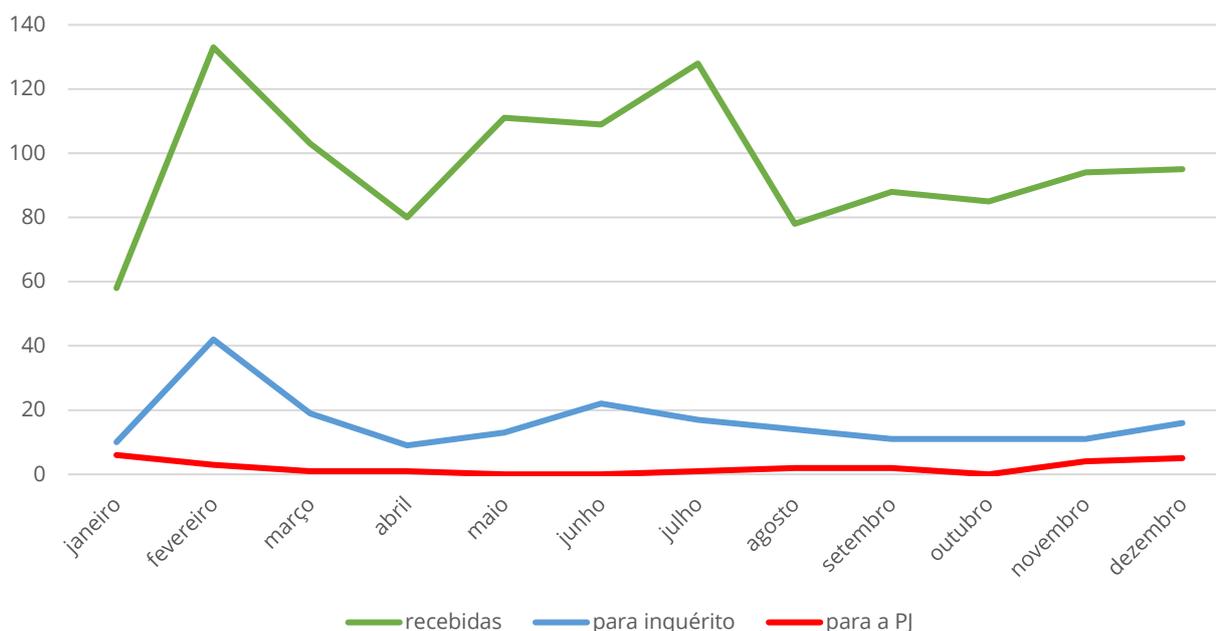
1160

9. No decurso do ano de 2021 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 195)** ou para a **Polícia Judiciária (que foram 25)**, nos moldes que acima se referiram.

denúncias recebidas em 2021

mês	denúncias recebidas	encaminhadas para inquérito	encaminhadas para a PJ	mês	denúncias recebidas	encaminhadas para inquérito	encaminhadas para a PJ
janeiro	58	10	6	julho	128	17	1
fevereiro	133	42	3	agosto	78	14	2
março	103	19	1	setembro	87	11	2
abril	80	9	1	outubro	85	11	0
maio	111	13	0	novembro	93	11	4
junho	109	22	0	dezembro	95	16	5

denúncias recebidas em 2021



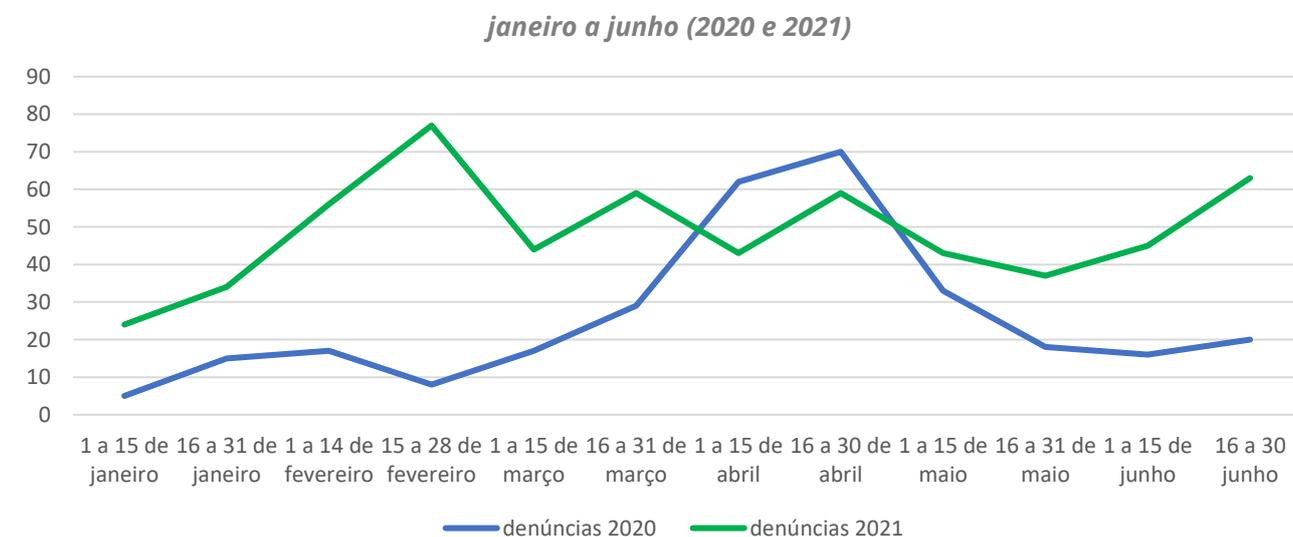
10. A análise do conjunto das denúncias recebidas no ano de 2021 revela, antes de mais, que se **mantém a tendência de consistente subida**: as denúncias recebidas no mês de dezembro (95 denúncias recebidas de 1 a 31 de dezembro de 2021) estão próximo do dobro das recebidas no mês de janeiro (58 denúncias recebidas de 1 a 31 de janeiro de 2021). Esta é uma tendência que vem já do ano de 2020. Como resulta da nota⁵ respeitante a esse ano, em janeiro de 2020 foram recebidas 20 denúncias, enquanto no mês de dezembro de 2020 foram recebidas 44.

11. Tal como se salientou na nota referente ao primeiro semestre de 2021⁶, a análise por períodos de quinze dias mostra ainda um outro aspeto extremamente relevante: tal como ocorreu em 2020, **nos períodos de confinamento decorrentes da pandemia de 2021 as denúncias aumentaram extraordinariamente**.

Recorda-se que, em 2020, tinha havido um aumento muito expressivo das denúncias recebidas entre março e maio, meses durante os quais foi imposto o confinamento obrigatório dos cidadãos aos seus domicílios.

Agora, em 2021, sucedeu o mesmo, em particular no mês de fevereiro, altura em que vigorou um novo confinamento obrigatório. É esta a conclusão que se alcança do gráfico que segue, que ilustra os *picos* de denúncias de abril de 2020 e de fevereiro de 2021. Quanto a este último período, entre 1 e 28 de fevereiro foram recebidas 133 denúncias, enquanto em janeiro tinham sido recebidas apenas 58 (portanto mais 229%). Em março foram recebidas 103 denúncias (portanto apenas 77% das denúncias recebidas em fevereiro).

Nos períodos de confinamento decorrentes da pandemia, em 2020 e 2021, as denúncias aumentaram extraordinariamente.



12. Como já se referiu, da mesma forma que sucedera no ano de 2020⁷, no decurso de 2021, o Gabinete Cibercrime recebeu muitíssimo mais denúncias do que em todos os anos anteriores, desde 2016. Salientou-se já que, desde 2019, em cada ano que passa, têm sido recebidas **mais que o dobro das denúncias que tinham sido recebidas no ano imediatamente anterior**.

⁵ https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_2020.pdf.

⁶ https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_de_cibercrime-22-07-2021.pdf.

⁷ https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_2020.pdf.

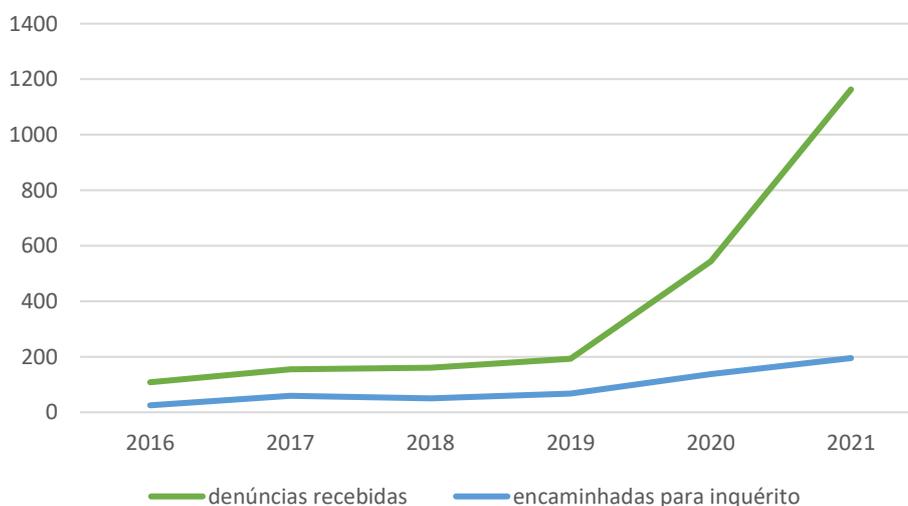
É certo que, quer em 2020, quer em 2021, como se adiantou acima, em momentos mais críticos da pandemia o número de denúncias de cibercrime foi muitíssimo mais elevado do que no resto do ano. Porém, não pode concluir-se que esse aumento de cibercriminalidade esteja apenas associado à pandemia: **embora a pandemia possa ter impulsionado o aumento deste tipo de criminalidade, esta tendência crescente afigura-se constante e consistente.** No quadro que vai de seguida e no gráfico que se lhe segue indicam-se as denúncias recebidas em cada ano, desde 2016. Descrevem-se também, em ambos, aquelas denúncias que, de entre o conjunto total, foram encaminhadas para inquérito, em cumprimento dos critérios acima referidos.

Independentemente dos picos, durante os períodos de confinamento decorrentes da pandemia, a cibercriminalidade tem aumentado todos os anos de forma constante e consistente.

denúncias 2016 - 2021

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

denúncias 2016 - 2021



13. Estes números revelam uma progressão constante e persistente do número de denúncias recebidas no decurso da última meia década: embora ocorram oscilações de mês para mês, ao longo do ano, registou-se sempre, **de um ano para outro, sem exceções, um aumento do número de denúncias.** De 2016 (108 denúncias) para 2017 (155 denúncias), registou-se uma subida de 144%. 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 118 %). Quanto a 2020 e 2021, como já se referiu, o aumento no número de denúncias foi excecional e superou em muito os dos anos anteriores. Assim, **de 2019** (193 denúncias) **para 2020** (544 denúncias), **o aumento foi de 288%**, enquanto **de 2020** (544 denúncias) **para 2021** (1160 denúncias), **o aumento foi de 213%**.

14. Este aumento das denúncias recebidas repercutiu-se naturalmente no número das denúncias remetidas para abertura de inquérito: durante o ano de **2021** foram **remetidas para investigação criminal 195 das denúncias** recebidas pelo Gabinete Cibercrime. Delas, o DIAP de Lisboa recebeu 158, sendo as restantes 37 distribuídas por outras comarcas do país. Recorda-se que em 2019 tinham sido remetidas para abertura de inquérito 67 denúncias (num conjunto total de 193 denúncias), número que subiu para 113 em 2020 (do total de 544 denúncias). Ou seja, **em apenas dois anos** (desde o final de 2019 até ao final de 2021), o número de **denúncias remetidas para investigação** passou para valores cerca de **três vezes maior**.

Sem prejuízo do incremento, em absoluto para o triplo, das denúncias remetidas para investigação, a leitura destes números é menos impressionante em termos relativos. É que, em **2019** foram remetidas para investigação **34,7 %** das denúncias (67 em 193), enquanto em **2020** foram remetidas **25,36 %** (138 em 544), sendo em **2021** remetidas apenas **16,81 %** (195 em 1160). Portanto, a subida anual do número de denúncias foi mais acelerada do que a subida do número daquelas que foram remetidas para investigação.

Três fatores principais são a razão deste menor crescimento percentual anual.

15. Por um lado, desde 2020 passaram a ser remetidas para a Polícia Judiciária (como mera informação operacional, sem que haja lugar a abertura de inquérito) algumas das denúncias que, pela sua tipologia, em anos anteriores eram remetidas ao DIAP – reduzindo assim o volume destas últimas. De seguida vai melhor explicar-se este aspeto.

Por outro lado, tiveram um enorme aumento o número de denúncias que se reportam a participações já anteriormente efetuadas pelo denunciante noutra sede. Também vai pormenorizar-se este vetor, de seguida.

Por último, um número muitíssimo expressivo das denúncias recebidas refere-se a criminalidade de massa, isto é, a crimes perpetrados pelos mesmos agentes contra um grande número de vítimas. São designadamente os casos do *phishing* bancário e do *phishing* para obtenção de dados de cartões de crédito, praticados por via da remessa de mensagens de correio eletrónico para um enorme número de potenciais vítimas. Em 2021 (tal como já acontecera em 2020) foram recebidas mais que uma centena de denúncias deste tipo de atuação criminosa, como melhor se descreverá mais abaixo. Como é sabido, os inquéritos direcionam-se para a identificação dos factos criminosos e do agente do crime. Neste caso concreto, está em causa em primeira linha quem expediu as mensagens criminosas – decorrentemente, portanto, o inquérito visando investigar estes factos englobará potencialmente um grande número de vítimas (ou dito de outra forma, um grande número de denúncias). Neste contexto, nomeadamente quando são denunciadas situações já anteriormente referenciadas, não se dá início a uma nova investigação quando é recebida cada uma das novas denúncias. Se o fosse, multiplicar-se-ia o número de denúncias remetidas para investigação de factos porventura coincidentes.

16. Como já se referiu, algumas das denúncias recebidas foram encaminhadas para a Polícia Judiciária, de acordo com a estratégia adotada e que acima se descreveu. Tratou-se sempre de casos em que eram denunciados factos reveladores de possível prática de crime. Porém, apenas em função da denúncia, por razões diversas, não havia necessariamente motivo para ser aberto um inquérito.

Assim aconteceu, por exemplo, em situações em que os denunciadores, apesar de quererem fazer chegar ao Ministério Público informação sobre práticas criminais, não manifestaram pretender exercer o direito de queixa. Ou então, por exemplo, situações em que vagamente se denunciou existirem práticas criminosas na Internet, sem se referenciar cabalmente tal prática. Ou então, por exemplo, denúncias

feitas com anonimato ou que não continham suficiente informação que permitisse identificar os factos criminosos ou os seus autores.

Em suma, adotando os critérios que acima se referiram, não se encaminharam para investigação, antes se remetendo para a Polícia Judiciária, denúncias que não reuniam condições para abertura de inquérito, mas que, ainda assim, continham informação relevante para a atividade daquele órgão de polícia criminal, por respeitarem a eventuais investigações em curso, ou por permitirem melhor identificar procedimentos ou fenómenos criminosos. Como já acima se referiu, durante o ano de 2021, neste contexto foram remetidas para a Polícia Judiciária 25 denúncias.

17. Por outro lado, ainda neste âmbito, importa referir o número significativo das denúncias não encaminhadas para inquérito por se referirem a outras participações, já antes entregues pelos denunciantes, por outras vias (quer diretamente noutros departamentos ou serviços do Ministério Público que, sobretudo, em órgãos de polícia criminal). Havendo já inquérito instaurado e a decorrer sobre os mesmos factos denunciados ao Gabinete Cibercrime, não havia motivo legal para que se remetesse a denúncia para abertura de nova investigação. No ano de 2021 assim ocorreu com 36 das denúncias recebidas.

D. CRIMINALIDADE MAIS FREQUENTE

18. 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 centenas de denúncias não pode ser interpretada como se fossem dados estatísticos rigorosos, mas certamente permite que delas 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 durante o ano de 2020 foi diferente daquela que ocorreu em 2021. Será também seguramente diferente da que 2022 revelará.

phishing

19. Como já acima se adiantou, um dos fenómenos criminais que continuou a motivar um grande número de denúncias em 2021 foi o do *phishing*. Continuam a multiplicar-se, de forma regular, campanhas de *phishing* especificamente dirigidas a vítimas em Portugal (bancos portugueses). Por essa razão, foi divulgado o **Alerta Cibercrime de 29 de setembro de 2021**. Já nos primeiros dias de 2022 veio ainda a ser emitido, sobre a mesma matéria, o **Alerta Cibercrime de 13 de janeiro de 2022**.

Por razões que já acima se explicaram, a generalidade das denúncias recebidas a este respeito não foi especificamente encaminhada para a abertura de inquérito.

phishing – dados de cartões de crédito

20. O mesmo sucedeu quanto à específica modalidade de *phishing* dirigido à obtenção ilícita de dados de cartões de crédito. Esta modalidade, pouco expressiva em anos anteriores, evoluiu ao longo do ano de 2021. Gradualmente, este tipo de prática criminosa passou a visar mais intensamente dados de cartões de crédito, tornando-se assim na mais frequente forma de *phishing*. A adoção de reforçadas medidas de segurança no acesso *online* a contas bancárias levou os agentes do crime a procurar induzir as vítimas a facultar-lhes os dados dos seus cartões de crédito.

Como acontece com o clássico *phishing* bancário, o processo criminoso passa pela expedição de mensagens (sobretudo de SMS ou WhatsApp, mas também de email), de forma indiscriminada, para destinatários escolhidos de forma aleatória.

O resto do processo varia. Foram identificadas campanhas em que foi utilizado o argumento enganoso de que a vítima iria ser reembolsada de quantias (por exemplo, pela AT – Autoridade Tributária ou pela EDP – Energias de Portugal, entre outras). Noutros casos, muitíssimo frequentes, o processo criminoso passou pela solicitação do pagamento de uma “pequena taxa”, relacionada com uma encomenda dirigida à vítima. Este processo expandiu-se muito significativamente, abusando do enorme incremento, durante o ano, das compras à distância, *online*.

Em todas estas situações o propósito dos agentes do crime foi o de solicitar à vítima que introduzisse os dados do seu cartão de crédito (o nome do titular, o número do cartão, a respetiva data de validade e ainda o código de segurança) numa página falsa, por eles gerida.

Foram emitidos o **Alerta Cibercrime de 25 de março de 2021**, o **Alerta Cibercrime de 12 de agosto de 2021** e o **Alerta Cibercrime de 27 de setembro de 2021** a este respeito.

Ao longo de 2021 este fenómeno registou uma enorme expansão, tornando-se no **mais expressivo de todos** aqueles que foram denunciados. Deu origem a 167 denúncias, correspondentes a **14,39 %** do total das 1160 denúncias recebidas.

burlas online

21. Em 2021, tal como sucedera já em 2020, o comércio eletrónico desenvolveu-se em grande velocidade, consoante os consumidores foram procurando, por esta via, ultrapassar as restrições à circulação e ao acesso físico ao comércio. Em paralelo a este desenvolvimento, surgiram práticas criminosas com ele relacionadas. As burlas em compras *online* expandiram-se, tornando-se num dos fenómenos de cibercriminalidade mais frequente, provocando um grande prejuízo económico efetivo aos portugueses. Durante este ano de 2021 foram identificadas e denunciadas inúmeras formas de burla, relacionadas com vendas através de diversas plataformas *online* legítimas. Da mesma forma, foram identificadas burlas com vendas nas redes sociais (designadamente no Facebook e no Instagram). A técnica utilizada, quer nas plataformas de vendas, quer nas redes sociais, foi idêntica e repetida: os agentes do crime criavam contas específicas para disponibilizar produtos para venda, que efetivamente eram pagos pelas vítimas, mas nunca entregues. Em ambas as situações (plataformas de vendas ou redes sociais) conseguiam defraudar um grande número de vítimas num espaço curto de tempo, após o qual as contas eram subitamente encerradas, sem que mais nada se soubesse quanto ao seu titular.

22. Na sua generalidade, todas estas situações específicas 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. Além disso, como a generalidade das vítimas pagou as suas compras com recurso a cartões de crédito, os respetivos dados ficaram na posse dos criminosos, que assim os passaram a poder utilizar abusivamente.

Este fenómeno criminoso assumiu uma **grande e progressiva expansão** ao longo do ano. As participações desta natureza vieram a corresponder a **21 % das denúncias que foram remetidas para abertura de inquérito**. No seu conjunto (denúncias remetidas para investigação e denúncias não remetidas), aquelas em que se denunciavam **burlas praticadas online corresponderam a 6 % (70) de todas as recebidas**. É, portanto, a julgar pelo sinal indicador que resulta das denúncias recebidas pelo Gabinete Cibercrime, um dos fenómenos mais frequente de

O *phishing* para obtenção fraudulenta de dados de cartões de crédito foi o fenómeno de cibercrime mais denunciado.

As burlas em compras *online* continuam a ser a parcela das denúncias que dá origem a mais investigações.

cibercriminalidade, apenas ultrapassado pelo *phishing* para obtenção de cartão de crédito, que já acima se descreveu.

burlas com páginas “falsas”

23. No segundo semestre de 2021 foi recebido um relevante número de denúncias de páginas “falsas” na Internet – páginas *web* que pretendem imitar 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.

24. 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 **2021** foram sinalizadas ao DIAP de Lisboa, para **abertura de inquérito, 28 das 45 denúncias recebidas** a este respeito – algumas das denúncias correspondiam a páginas já anteriormente sob investigação. Este foi o **segundo conjunto mais numeroso de participações encaminhado para inquérito**, apenas superado pelo das burlas *online*. Verificou-se ainda uma particular incidência deste fenómeno no final do ano, em dezembro, época em que muitos consumidores fazem mais compras.

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.

25. 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 exame.

No segundo semestre do ano surgiram também denúncias de páginas *online* que permitiam aos utilizadores, por si mesmos e apenas por si, sem qualquer intervenção de autoridades públicas, emitir um falso Certificado Digital COVID da UE, sem qualquer verificação ou confirmação dos respetivos requisitos.

Neste contexto, durante 2021, foram encaminhadas para investigação **10 denúncias**.

26. Embora com menor expressão numérica que o fenómeno anterior, continuaram em 2021 a ser recebidas denúncias de um fenómeno criminoso com grande impacto nas vítimas: o das burlas *online* no mercado imobiliário. Esta prática criminosa traduz-se na difusão de enganosas propostas de arrendamento de imóveis que não existem (ou que existindo, não pertencem ao anunciante, nem estão disponíveis para arrendamento). Apesar de, aparentemente, este fenómeno estar a ser menos expressivo do que já foi no passado, ainda assim foram recebidas 10 denúncias deste tipo de crimes (3 das quais foram encaminhadas para investigação). Verificou-se uma particular frequência de denúncias

nos meses de agosto e setembro, altura em que muitos estudantes universitários procuram alojamento nas cidades para onde se deslocam.

burlas com criptoativos e outros produtos financeiros

27. O ano de 2021 ficou marcado pela enorme expansão da oferta de investimentos em criptomoedas e também no chamado mercado forex. Alguma desta oferta, muito visível e ruidosa na Internet, revelou-se ser criminosa e não ter outro propósito que não o de burlar aqueles a quem se dirigia.

Tiveram enorme expansão as ofertas fraudulentas, na Internet, de negócios com investimentos em criptoativos.

Naturalmente, em consequência, surgiu um grande número de denúncias a elas associadas. Em geral, reportaram a existência de páginas fraudulentas na Internet cujos gestores, depois de convencerem as vítimas a realizar promissores investimentos em negócios sobre aqueles ativos, encerraram as páginas *web* e desapareceram, sem devolverem o dinheiro investido pelas vítimas. Foi a este respeito emitido o **Alerta Cibercrime de 2 de maio de 2021**.

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 a 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 sendo carregada apenas para uma plataforma *online* que, subitamente, foi encerrada, deixando assim as vítimas com muito pouca informação comprovativa da burla que sofreram.

Por este motivo, apenas uma pequena parte das denúncias reunia condições para ser encaminhada para abertura de investigação. Todavia, no contexto geral das denúncias recebidas, aquelas que se referiam a burlas relacionadas com este tipo de investimento assumiram uma dimensão muito significativa: foram recebidas **38 denúncias** por este motivo, o qual é assim, dentro das denúncias que não foram encaminhadas para investigação, o segundo grupo mais numeroso (apenas superado pelas denúncias de *phishing* para obtenção de dados de cartões de crédito).

burlas em relações pessoais

28. Intensificaram-se durante o ano de 2021 as 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 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 o ano de 2021 foram recebidas pelo Gabinete Cibercrime **10 denúncias** deste tipo, com particular incidência no período do verão (agosto e setembro). As vítimas são, todas elas, senhoras de meia-idade e, nalguns casos, sofreram prejuízos de dezenas de milhares de euros.

CEO fraud

29. Também ocorreu e causou relevantes prejuízos patrimoniais em Portugal, durante o ano de 2021, o fenómeno conhecido como *CEO fraud*, ou *BEC (business email compromise)*, técnica de engenharia social pela qual os criminosos induzem em erro uma 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.

Este tipo de denúncias (que foram **14** durante o ano), correspondeu a 6,6 % das que foram remetidas para abertura de inquérito.

ataques informáticos

30. As denúncias respeitantes a crimes informáticos, ou *cibercrimes* em sentido estrito, 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*) ou acessos ilegítimos a sistemas informáticos. Porém, o fenómeno criminoso mais denunciado, neste conjunto, é o do *ransomware*.

Todas as **13 denúncias** recebidas relatando ataques informáticos foram encaminhadas para investigação criminal. Uma boa parte delas referia-se a ataques a pequenas e médias empresas.

31. Foram, porém, recebidas outras denúncias remetidas por indivíduos (pessoas singulares), relatando crimes de acesso ilegítimo. Em geral, este tipo de acesso ilegítimo visou contas de correio eletrónico, ou contas de redes sociais tituladas pela vítima e legitimamente acedidas por terceiros.

Foram recebidas 8 denúncias deste tipo, todas elas encaminhadas para abertura de inquérito.

falsas chamadas da Microsoft

32. Um dos fenómenos que mais se expandiu durante o ano de 2021 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 por chamadas telefónicas fraudulentas em que, de forma astuciosa e enganosa, 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 acesse 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, acesse à sua conta de *homebanking*. Noutros casos referenciados, o “atacante” afirmou conseguiu 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).

33. Foram recebidas durante o ano **28 denúncias** deste tipo, com particular incidência nos **meses de outubro a dezembro**. Foi, a este propósito, emitido o **Alerta Cibercrime de 3 de novembro de 2021**.

Estas chamadas telefónicas não têm origem em Portugal – muitas delas têm origem em países distantes, como a Índia e ou a Nigéria, ou outros, com quem a cooperação judiciária é mais difícil ou demorada – e 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.

divulgação de fotografias e outra informação pessoal

34. A violação da privacidade e a divulgação *online* de dados pessoais (ou fotografias) continuou a motivar muitas das queixas recebidas. Tais denúncias incidiram sobretudo sobre o uso não autorizado de fotografias, por exemplo na criação de perfis ou contas em páginas de encontros ou de anúncios de prostituição, associando-se a esses perfis fotografias íntimas e dados verdadeiros das vítimas. Durante 2022 foram recebidas **27 denúncias** relatando factos desta natureza.

stalking e sextortion

35. Em território próximo do fenómeno a que imediatamente acima se aludiu, durante 2021 foram denunciadas ao Gabinete Cibercrime algumas situações (**7 denúncias**, das quais 5 foram encaminhadas para investigação criminal) de perseguição com uso das tecnologias, ou ***stalking***.

Foram denunciadas situações, igualmente com alguma expressão (**21 denúncias**), de ***sextortion***, ou exigência de quantias sob pena de divulgação de imagens íntimas, geralmente de natureza sexual. Este fenómeno ocorreu sobretudo com **vítimas** que, ***online***, travaram conhecimento **com pessoas desconhecidas**.

36. 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.

As denúncias deste tipo recebidas revelam que se trata de ações provenientes de múltiplos agentes, independentes uns dos outros que, replicando os vários modos de atuar, prosseguem interesses individuais, de lucro ilegítimo.

Sobre este fenómeno foi emitido o **Alerta Cibercrime de 11 de fevereiro de 2021**, atualizando a informação anteriormente veiculada pelo **Alerta Cibercrime de 23 de janeiro de 2019**.

discurso de ódio online

37. Continuaram a ser recebidas em 2021 algumas denúncias (em número pouco expressivo, de 6) em que se reportavam factos traduzindo manifestações do chamado discurso de ódio: sobretudo de textos e comentários em redes sociais, em que se incitava ao ódio, à violência, ou ainda à discriminação, por motivos raciais ou étnicos.

Quase todas estas denúncias foram **encaminhadas para abertura de inquérito**, embora nalguns casos tivesse havido dúvidas sobre a qualificação jurídica dos factos em causa.

violação de direito de autor

38. Outro dos temas que emergiu das denúncias recebidas durante o ano de 2021, embora em número muito pouco expressivo (**apenas 4 denúncias**) foi o da violação de direito de autor. Nenhuma das diversas denúncias recebidas se reportava aos clássicos abusos nesta matéria (designadamente à chamada “pirataria” de audiovisual) – pelo contrário, incidiam sobre violações de direitos da propriedade intelectual relacionadas com a economia digital.

crimes contra a honra

39. O Gabinete Cibercrime tem recebido recorrentemente denúncias reportando crimes contra a honra, sobretudo referentes a publicações em redes sociais.

Pela natureza do ilícito em causa (e pelas exigências processuais penais associadas à mesma), o procedimento adotado é o de informar os denunciadores 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). Durante 2021 foram recebidas **14 denúncias** deste tipo.

defraudações na utilização da aplicação de pagamentos MBWAY

40. Como se reportou em notas anteriores, respeitantes a 2020⁸ e ao primeiro semestre de 2021⁹, naqueles períodos de tempo, um dos fenómenos criminosos que mais motivou denúncias foi o das defraudações na utilização da aplicação de pagamentos MBWAY. Este fenómeno atingiu milhares de vítimas em todo o território nacional, causando prejuízos muito avultados. A este respeito foi até publicado um **Alerta Cibercrime a 8 de abril de 2020**.

Entretanto, foram desenroladas diversas operações policiais visando este tipo de criminalidade, com realização de detenções, às quais os *media* deram muita visibilidade. Talvez por isso, o fenómeno tem vindo a diminuir. No primeiro semestre de 2021 ainda surgiram numerosas denúncias a este respeito, mas no segundo semestre do ano os casos foram bastante menores (**apenas 11 denúncias**).

⁸ https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_2020.pdf.

⁹ https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_de_cibercrime-22-07-2021.pdf.