



**MINISTÉRIO PÚBLICO
PORTUGAL**

PROCURADORIA-GERAL DA REPÚBLICA

GABINETE CIBERCRIME

Nota Informativa

**CIBERCRIME:
DENÚNCIAS RECEBIDAS
2020**

8 de janeiro de 2021

ÍNDICE

A. O CONTEXTO - CIBERCRIME	4
B. O PROCESSO DE RECEBIMENTO DE DENÚNCIAS	4
C. AS DENÚNCIAS RECEBIDAS	5
D. CRIMINALIDADE MAIS FREQUENTE	8

CIBERCRIME: DENÚNCIAS RECEBIDAS 2020

A. O CONTEXTO - CIBERCRIME

1. Dentro da genérica expressão *cibercrime* incluiu-se comumente um conjunto muito heterogéneo de tipos legais de crime. Primordialmente, é o caso dos ilícitos descritos na Lei do Cibercrime¹ (Lei nº 109/2009). Mas é também o caso de muitos outros crimes, quer incluídos no Código Penal², quer em diversas outras fontes legais avulsas³. Neste contexto, a quantificação estatística do cibercrime não é fácil, uma vez que, como se disse, além dos crimes informáticos clássicos, o conjunto abrange 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 brutal.

As estatísticas da Justiça, em geral, catalogam os ilícitos segundo os tipos legais de crime (por exemplo burlas, crimes contra a honra, crimes contra o direito de autor), não considerando autónoma ou separadamente aqueles que ocorrem *online*. O existente sistema de estatísticas da Justiça não está concebido de forma a permitir aperceber a dimensão numérica (estatística) da complexa realidade que se tem classificado como cibercriminalidade.

¹ Falsidade informática, dano informático, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido.

2. Por isso, não é fácil aperceber, 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

3. Com a finalidade de permitir aos cidadãos contactar com o Gabinete Cibercrime, está ativo, desde 2012, o endereço eletrónico cibercrime@pgr.pt. No início de 2016 passaram expressamente a aceitar-se também queixas da prática de crimes relacionados com a atividade do Gabinete.

Não estando ainda disponível a 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. Na verdade, as mensagens desta natureza, encaminhando denúncias relevantes para efeitos de processo penal, têm uma expressão numérica persistentemente crescente. Após a

² Designadamente a burla informática e a pornografia infantil.

³ Por exemplo, os ilícitos criminais relacionados com a proteção de dados pessoais.

eclosão da pandemia da COVID-19, na primavera de 2020, esta via de comunicação assumiu ainda mais importância.

4. O Gabinete Cibercrime não tem atribuições de direção da investigação criminal. Por esse motivo, estabeleceu-se um entendimento informal com o Departamento de Investigação e Ação Penal de Lisboa, fixando os parâmetros de um procedimento experimental de recebimento e encaminhamento destas denúncias para este 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 recebimento de queixas por correio eletrónico não consegue ainda dar resposta.

5. 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.

Na verdade, 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 apresentar 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 de forma muito vaga ou genérica. Também estas não são encaminhadas para inquérito.

6. Importa ainda referir que uma parte importante destas últimas denúncias, não 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 mensagem 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

7. Como se demonstrará de seguida, 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 aumentaram de forma excecional, designadamente durante a eclosão da pandemia da COVID-19.

8. No decurso do ano de 2020 foram recebidas pelo Gabinete Cibercrime 544 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 138). Das denúncias, 40 delas vieram a ser remetidas para a Polícia Judiciária, no quadro que acima se referiu.

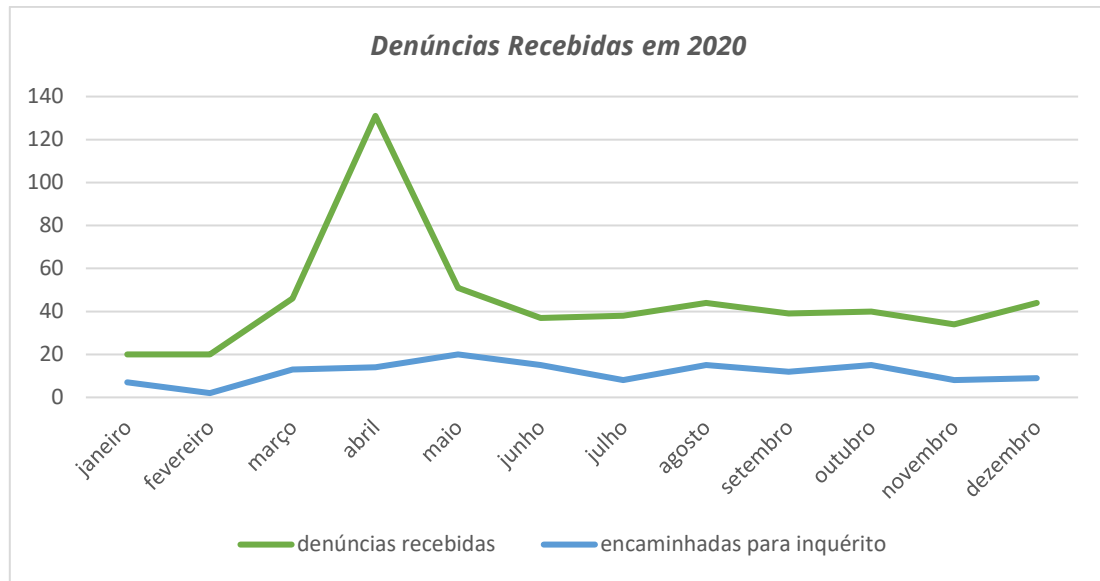
⁴ Ocasionalmente, as denúncias são remetidas para outros Departamentos de Investigação e Ação Penal, noutras comarcas, caso se aperceba liminarmente que os factos

denunciados ocorreram na área geográfica de outra comarca, que não na de Lisboa.

Denúncias Recebidas em 2020

mês	denúncias recebidas	encaminhadas para inquérito
janeiro	20	7
fevereiro	20	2
março	46	13
abril	131	14
maio	51	20

junho	37	15
julho	38	8
agosto	44	15
setembro	39	12
outubro	40	15
novembro	34	8
dezembro	44	9



9. A análise do número de denúncias recebidas no decurso do ano de 2020 suscita **quatro observações principais. A primeira observação** respeita ao período de eclosão da pandemia da COVID-19, no início da primavera de 2020: **nos meses de março a maio de 2020 foi recebido um número excepcionalmente elevado de denúncias**, se comparados com os restantes meses do ano.

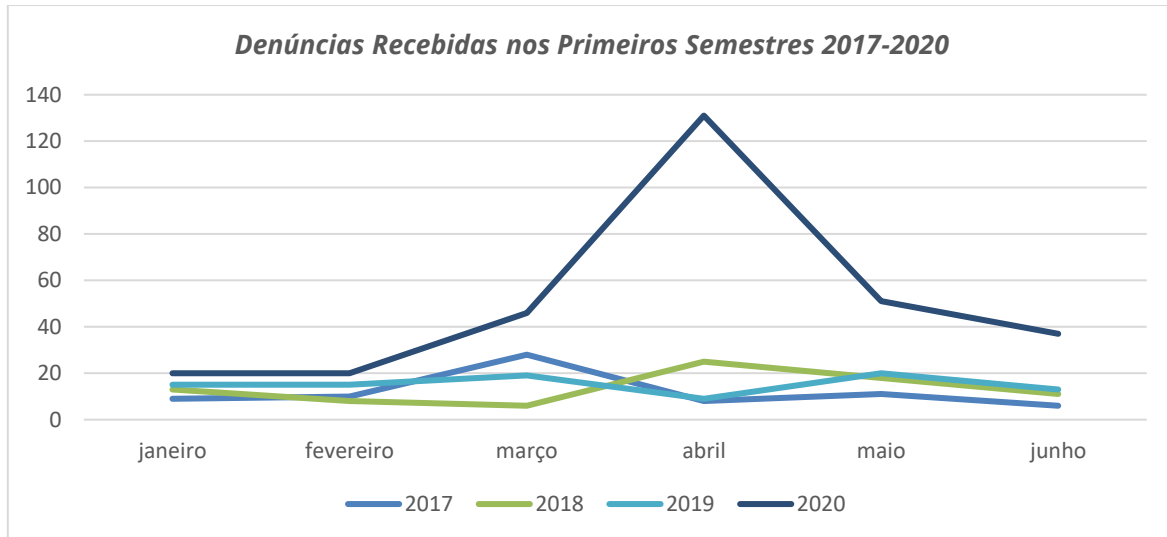
Por exemplo, em março de 2021 foram recebidas 46 denúncias, enquanto nos meses de janeiro e fevereiro tinham sido recebidas 20 (em termos percentuais, este aumento foi portanto de 230%). Por sua vez, em abril foram recebidas 131 denúncias, valor que, em relação ao mês de

março significa um aumento de 284%, mas se comparado com valores de janeiro e fevereiro representa um acréscimo de 650%. Durante o mês de maio, o número de denúncias regressou aproximadamente à dimensão de março (51 denúncias em maio, contra 46 em março).

10. Anote-se que esta conclusão, que sublinha o aumento excepcional de denúncias nos meses de março a maio de 2020, é corroborada pela análise dos valores dos correspondentes meses dos anos anteriores. Na tabela e no gráfico que seguem descrevem-se as denúncias recebidas apenas nos primeiros semestres dos anos de 2017 a 2020.

Denúncias Recebidas nos Primeiros Semestres 2017-2020

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



11. Os números constantes da tabela e visualmente representados no gráfico permitem claramente reforçar a conclusão que acima se formulou: comparadas com as de meses homólogos de anos anteriores, as denúncias recebidas durante os meses de março a maio de 2020 atingiram valores excepcionalmente elevados – sobretudo, as denúncias recebidas durante o mês de abril.

12. A **segunda observação** principal que se suscita é a de que, **ultrapassado o período excepcional de eclosão da pandemia**, passaram a ser recebidas denúncias com grande **regularidade e estabilidade**, em números rondando as 40 denúncias mensais. Esta foi aliás uma tendência que se manteve até ao final do ano de 2020.

Com efeito, como resulta do quadro que acima ficou, onde se descreveram as denúncias recebidas em 2020, nos meses de junho a dezembro foram recebidas 276 denúncias. Novembro de 2020 foi o mês em que se registaram menos (34 denúncias), enquanto agosto e dezembro foram aqueles em que se receberam mais (44 denúncias em ambos). Em termos percentuais médios, estes valores correspondem a 39,4 denúncias por mês.

13. Estas razões conduzem à **terceira observação** suscitada por estes dados: de

forma estável e persistente, as denúncias de cibercrime eram, no final do ano de 2020, o dobro daquelas que ocorriam no início do ano. Ou seja, de forma genérica pode dizer-se que **durante o ano de 2020, as denúncias de cibercrime duplicaram.**

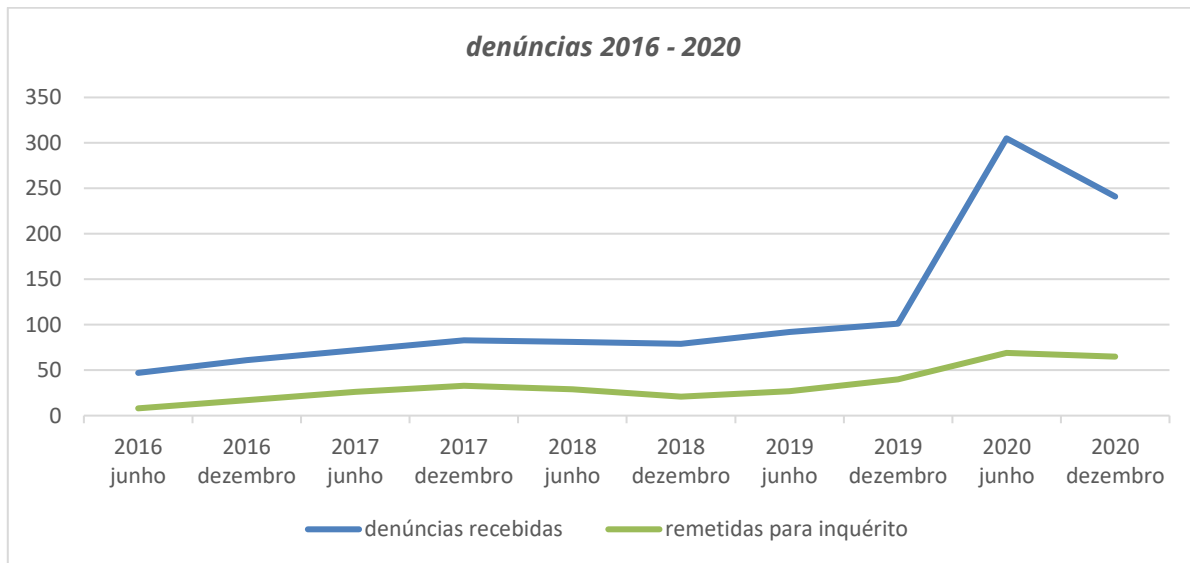
Com efeito, como acima se referiu, a partir de junho de 2020 foram mensalmente recebidas denúncias que, embora variando, rondaram as 40 denúncias por mês. Ora, em cada um dos meses de janeiro e fevereiro apenas foram recebidas 20 denúncias. Estes valores, do início do ano, são consistentes com os que se registaram no ano anterior, de 2019. Com efeito, no segundo semestre de 2019 foram recebidas 102 denúncias, correspondendo a uma média mensal de 17 denúncias. Já no período de outubro a dezembro de 2019 foram recebidas 60 denúncias – portanto, uma média mensal de 20, tal como ocorreu em janeiro e fevereiro de 2020. Como se viu, no segundo semestre de 2020, a média mensal rondou as 40 denúncias.

14. Uma **quarta observação** resulta da comparação dos valores das denúncias registadas em 2020 com as que se receberam nos anos anteriores. Como já se referiu, o Gabinete Cibercrime recebeu em **2020 muitíssimo mais denúncias do que em todos os anos anteriores.**

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 que a leitura seja mais rigorosa. 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 - 2020

Ano	denúncias recebidas	denúncias encaminhadas para inquérito
2016	108	25
2017	155	59 ⁵
2018	160	50 ⁶
2019	193	67
2020	546	138



15. 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.** De 2016 (108 denúncias) para 2017 (155 denúncias), registou-se uma subida de 144%. Foi mais tímida 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, um ano ímpar, o aumento no número de denúncias foi excecional: o número de denúncias superou em muito as dos anos anteriores, como já se referiu.

D. CRIMINALIDADE MAIS FREQUENTE

16. 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 dar origem a dados estatísticos rigorosos, mas certamente permite que delas se infiram as grandes linhas do cibercrime que vitima os portugueses.

defraudações na utilização da aplicação de pagamentos MBWAY

17. Ao longo do ano de 2020, um dos fenómenos criminosos que mais motivou denúncias, foi o das defraudações na utilização da aplicação de pagamentos MBWAY. Trata-se de um fenómeno que persistiu durante todo o ano, atingindo milhares de vítimas em todo o território nacional e causando às mesmas, no seu conjunto, um prejuízo que não está quantificado e dificilmente o será na sua globalidade, mas

⁵ Embora 20 destas 59 denúncias encaminhadas tenham sido remetidas para junção a um inquérito já existente.

⁶ Embora 13 destas 50 denúncias encaminhadas tenham sido remetidas para junção a um inquérito já existente.

seguramente de muitas centenas de milhares de euros, senão mesmo na ordem dos milhões de euros.

Por razões de eficácia na investigação e, sobretudo, por razões de prevenção geral, o Gabinete Cibercrime emitiu um **Alerta Cibercrime a 8 de abril de 2020**, sobre a utilização fraudulenta da aplicação MBWAY. Pela enorme expressão deste fenómeno criminal, foi emitida pela Procuradora-Geral da República a **Instrução n.º 1/20, de 27 de maio de 2020**, contendo diretrizes tendo em vista a coordenação da atividade do Ministério Público a este respeito.

phishing

18. Outros dos fenómenos mais frequentes do ano de 2020 foi o do *phishing*. Multiplicaram-se ao longo do ano campanhas de *phishing* muito agressivas, sobretudo por terem sido especificamente desenhadas para atingir vítimas em Portugal. Na primeira metade do ano identificaram-se sobretudo campanhas de *phishing* bancário, que muito se intensificaram aquando da eclosão da pandemia. Tais campanhas alargaram-se a muitos outros alvos, dissimulando planos criminosos que usaram (de forma abusiva) a imagem de entidades públicas e privadas portuguesas, como os CTT, a Autoridade Tributária ou a EDP, entre muitas outras.

Foram denunciadas muitas campanhas de *phishing* visando obter as credenciais de acesso a contas de correio eletrónico e a contas bancárias. Porém, muitas outras das campanhas que foram denunciadas tinham especificamente- em vista a obtenção de dados de cartões de crédito das vítimas. A persistente repetição e a intensidade destas campanhas induzem que se trata de uma atividade criminosa muito lucrativa.

Aliás, em paralelo foram também denunciadas ao Gabinete Cibercrime muitas situações de movimentos bancários ilegítimos, efetuados sem o conhecimento dos titulares das contas e, sobretudo, situações de uso abusivo dos dados

de cartões de crédito, nomeadamente para efetuar compras *online*.

Durante o ano de 2020, o Gabinete Cibercrime emitiu um **Alerta Cibercrime de 14 de abril** sobre mensagens eletrónicas fraudulentas, entre outras, referindo mensagens de *phishing*. Emitiu ainda diversos alertas sobre campanhas de *phishing* especificamente direcionadas: o **Alerta Cibercrime de 13 de fevereiro** (sobre *phishing* dirigido a utilizadores da aplicação Outlook Web App), o **Alerta Cibercrime de 13 março** (sobre *phishing* dirigido a clientes do banco Crédito Agrícola), o **Alerta Cibercrime de 17 de março** (sobre *phishing* dirigido a clientes do Banco Millennium BCP), o **Alerta Cibercrime de 16 de março** e o **Alerta Cibercrime de 15 de maio**, (ambos sobre *phishing* dirigido a clientes da EDP e a titulares de cartões de crédito).

ransomware

19. Também se pode inferir que as iniciativas de *ransomware* são lucrativas, porque se têm vindo a repetir – e deram origem a muitas denúncias, ao longo do ano. Neste caso particular, as vítimas parecem ter sido mais institucionais (pessoas coletivas, pequenas e médias empresas, por exemplo) do que pessoas singulares. Associada a esta prática, mas muito menos expressiva, mas também por vezes denunciada, persistiu ao longo de 2020 a difusão de outro *malware*, para além do *ransomware*.

O Gabinete Cibercrime emitiu um **Alerta Cibercrime de 14 de abril de 2020** sobre mensagens eletrónicas fraudulentas, entre outras, referindo mensagens genericamente contendo *malware*.

CEO fraud

20. Igualmente visando sociedades ou outras unidades económicas, foram denunciadas muitas situações de chamada "*CEO fraud*", técnica de engenharia social pela qual se pretende induzir em erro a estrutura empresarial, levando-a a efetuar pagamentos a terceiros (os criminosos), que se fazem passar

por autênticos fornecedores ou parceiros de negócio da empresa. Foram efetuadas muitas denúncias deste tipo por entidades 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 sobre contas bancárias estrangeiras.

burlas online

21. Conjuntamente com as defraudações com a aplicação MBWAY, as burlas *online* parecem ter sido o fenómeno de cibercriminalidade que terá provocado mais prejuízo económico aos portugueses. Foram denunciadas inúmeras formas de burla, com utilização de diversas plataformas *online* legítimas.

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). Este mesmo formato de engano ocorre também, e com igual frequência, quanto a automóveis.

Foram igualmente frequentemente denunciadas situações de pequenas burlas – pequenas, quanto ao valor económico envolvido –, sobretudo na venda de vestuário, ou calçado, ou equipamento desportivo ou de lazer. Tais burlas têm ocorrido, além das plataformas habituais de venda legítima, mais frequentemente nas redes sociais (e designadamente no Facebook e no Instagram). A técnica usada é repetida: criação de contas em que se disponibilizam produtos para venda e são efetivamente vendidos e pagos pela vítima, mas nunca entregues. Desta forma, são burladas muitas vítimas num espaço muito curto de tempo, após o que as contas são subitamente encerradas, sem que mais nada se saiba quanto ao seu titular.

Também se denunciaram, com alguma expressão, fenómenos desta natureza

relacionados com páginas específicas na Internet, pretendendo ilegitimamente imitar as páginas originais e oficiais de marcas internacionais de vestuário ou calçado.

burlas com relacionamentos e com criptomoedas

22. Durante o ano de 2020 foram também denunciados dois tipos de fenómenos fraudulentos que, existindo antes, se intensificaram significativamente. Um deles, foi o das burlas relacionadas com relacionamentos pessoais e emocionados estabelecidos, à distância, pela Internet, com desconhecidos (por exemplo supostos militares da ONU em serviço no Iraque, e similares). Nalguns casos, estas burlas provocaram prejuízos de dezenas de milhares de euros às vítimas.

O outro, foi o das burlas com transações sobre criptomoedas. Multiplicaram-se ao longo do ano as denúncias de páginas fraudulentas na Internet cujos gestores, depois de convencerem as vítimas a realizar promissores investimentos em negócios sobre aqueles ativos, desapareceram.

burlas com páginas web falsas

23. Também se denunciaram 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.

divulgação de dados privados e fotografias

24. A violação da privacidade e a divulgação *online* de dados pessoais (ou fotografias) motivou também muitas das queixas recebidas. Nalguns casos, numericamente não muito significativos, cidadãos denunciaram o acesso

não autorizado, por terceiros deles desconhecidos, a contas de email ou do Facebook. Por altura da eclosão da pandemia este fenómeno foi mais frequente quanto a sessões ou aulas em videoconferência. Este fenómeno deixou de ter expressão com o incremento (que foi muito rápido), da *literacia* quanto às regras de segurança a observar no uso das diversas plataformas de comunicação por via de videochamada.

Muito mais frequente foi, ao longo do ano, a divulgação não autorizada de fotografias. De entre os casos denunciados, os mais insidiosos (e algo frequentes), consistiram 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.

stalking e sextortion

25. Ainda neste campo, foram denunciadas algumas situações de perseguição com uso das tecnologias, ou *stalking*.

Foram denunciadas situações, igualmente com alguma expressão, de *sextortion*, com 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.

Persistiu em 2020, mais intensamente na primeira metade do ano, uma atividade criminosa paralela a esta, muitíssimo frequente no ano anterior, de 2019, de extorsão por via de mensagens de correio eletrónico remetidas de forma massiva, sob a ameaça de revelação de dados pessoais e imagens.

O Gabinete Cibercrime emitiu um **Alerta Cibercrime de 14 de abril de 2020** sobre mensagens eletrónicas fraudulentas, entre outras, referindo mensagens visando a extorsão por correio eletrónico.

discurso de ódio

26. No decurso do ano de 2020 emergiu um número significativo de denúncias em que se

reportavam factos traduzindo manifestações do chamado discurso de ódio. Tais denúncias dão conta, 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. Em geral, tais 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

27. Outro dos temas que emergiu nas denúncias recebidas durante o ano de 2020 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.