MISCELLANEA

DEZ 2022 — Nº17
REVISTA SEMESTRAL
GRÁTIS

APAV

FICHA TÉCNICA

REVISTA MISCELLANEA
Nº REGISTO ERC: 127611 – DEZEMBRO 2022

PROPRIETÁRIO
APAV | ASSOCIAÇÃO PORTUGUESA DE APOIO À VÍTIMA
NIPC: 502 547 952

DIRETORA
ROSA SAAVEDRA

FOTOS
JÚLIA PAVIN

DESIGN EDITORIAL
RITA CASTELO BRANCO

IMPRESSÃO E ACABAMENTO
PUBLIREP - PUBLICIDADE & REPRESENTAÇÕES LDA. | RUA PARTICULAR
APM ARMAZÉM Nº 6 | 2790-192 CARNAXIDE

TIRAGEM
50 EXEMPLARES

ESTATUTO EDITORIAL
DISPONÍVEL ONLINE EM BIT.LY/ESTATUTOEDITORIAL_MISCELLANEA

SEDE DE REDAÇÃO E SEDE DO EDITOR
RUA JOSÉ ESTEVÃO 135-A | 1150-201 LISBOA | PORTUGAL

CONTACTOS
+351 21 358 79 00 | APAV.SEDE@APAV.PT | WWW.APAV.PT

NOTA:
Foi dada liberdade aos/às autores/as dos artigos que constam do presente número da Revista MISCELLANEA APAV para redigi-los, ou não, ao abrigo das normas do Acordo Ortográfico da Língua Portuguesa, tendo cada um/a optado individualmente

ÍNDICE

EDITORIAL

ADMIRÁVEL MUNDO NOVO

Neste número especial da *Miscellanea* abordamos o mundo virtual, o ciberespaço, a cibersegurança e o cibercrime, sobretudo na perspectiva das vítimas e da vitimação. O mundo virtual, sendo virtual, não é, nunca é, neutro nem inócuo. Têm as matérias do ciberespaço muitas vezes grande e decisiva importância na vida real de todos e cada um de nós.

Mesmo com uma cultura de cibersegurança, impacta-se na vida, na liberdade, na honra e no património das pessoas e na actividade e na reputação das empresas, positiva e negativamente e, algumas vezes mesmo, muito negativa e gravemente.

O cibercrime e a vitimação é e deve ser objecto de análise e sobretudo de intervenção adequada e imediata. E essa ponderada análise e pronta intervenção não deve apenas ocorrer na vertente preventiva e patrimonial, mas igualmente nas perspectivas imprescindíveis de eliminar ou diminuir o seu potencial destrutivo e de violação dos direitos e sobretudo dos direitos fundamentais.

Afirma-se, por isso, a igual valia das vertentes da prevenção e da afirmação simbólica do direito e dos direitos, do sancionamento, da repressão ou da censura da *patologia*, ou seja, de comportamentos por acção e por omissão típicos, ilícitos, culposos e puníveis, e da importância da *terapêutica*, isto é da salvaguarda cautelar, da eliminação, sustação ou da reparação efectiva de violações de bens pessoais e materiais.

O furto de identidade, o seu *modus operandi* e a necessidade de prevenção não podem descurar a efectiva e pronta protecção da vítima quando se consuma. O cumprimento dos deveres e a concretização das responsabilidades exige a possibilidade de sindicância. E essa sindicância só existirá com um efectivo direito à informação dos ofendidos e dos lesados e com um correspondente direito à acção que seja efectivo.

Essa abordagem prática é essencial, porque, por mais prevenção que se tente e faça, os riscos abstractos depressa passam a perigos concretos e estes a efectivos danos pessoais e materiais. E deve haver respostas concretas das entidades e das autoridades sob pena de responsabilidades partilhadas e de responsabilização conjunta.

Em matéria de apoio aos cidadãos e de informação clara e atempada dá-se a conhecer a Linha Internet Segura. Até porque aumentam as abusivas *violações de privacidade online*, prolifera a ilícita *divulgação de fotografias e dados pessoais*, multiplicam-se os *acessos ilegítimos*, praticam-se inúmeras *sabotagens informáticas*, cresce exponencialmente o *phishing*, grassam as *burlas em compras na internet* e alastram as *fraudes relacionadas com cartões de crédito*.

Felizmente existem meios de reacção, procedimentos próprios e profissionais do foro, autoridades, especialistas e técnicos a quem recorrer, instrumentos de reacção esses de que se pode lançar mão para responder ao aumento de criminalidade, limitar danos e procurar a reparação ou a recuperação de activos, aumento de criminalidade que também ocorreu potenciadamente no pico da pandemia, na sequência dos confinamentos e do aumento de usos dos meios cibernéticos.

Nesse contexto e na evolução dos últimos anos, aumentaram igualmente as *burlas em compras e vendas* e, em número e sofisticação, fenómenos criminosos como os decorrentes de métodos de ataque de *Backdoors*, de *DoS*, de *Spoofing*, etc., ou de esquemas de *CEO fraud*, de *Technical Assistance Scam*, de *Sextortion* e de *Bullying* ou de *Stalking digital*…

Infelizmente se instrumentos legais e processuais existem, muitas vezes não funcionam, ou porque não são suficientemente eficazes e eficientes; e outras tantas porque não são sequer conhecidos ou prontamente operacionalizados. Há que alterar a cultura de inércia e os paradigmas.

Tratam-se nesta revista também matérias de natureza substantiva ou processual, abordando-se realidades sociológicas e tipos de criminalidade em especial, tal como a que se consubstancia no ciberterrorismo e em violência ou agressões *online* entre a população juvenil, elencando-se vários outros crimes e a necessária gestão na prevenção de riscos e de resposta às crises e incidentes, discutindo-se a controvérsia da licitude ou ilicitude na obtenção de prova por meio da infiltração digital, captura ou monitorização encoberta *online* de dados informáticos.

É todo um *admirável mundo novo*. Com virtualidades, benefícios, escolhos, desafios e perigos. Conheçamo-los um pouco melhor. Urge, pois, estudar, regular, formar, sensibilizar, comunicar e… agir.

NOTAS BIOGRÁFICAS

BERNARDO
PEREIRA GONÇALVES

É jurista, licenciado pela Faculdade de Direito da Universidade Católica Portuguesa (Escola de Lisboa), instituição onde actualmente frequenta o Mestrado Forense, com especialização em Direito e Processo Penal. Frequentou o Curso de Especialização em Direito Penal, Económico, Internacional e Europeu da Faculdade de Direito da Universidade de Coimbra.

CARLOS
PINTO DE ABREU

É advogado especialista em Direito Criminal e representou a Ordem dos Advogados na Unidade de Missão para a Reforma Penal. Foi docente universitário e membro da Comissão de Fiscalização do Centros Educativos e da Comissão de Acompanhamento do Sistema de Vigilância Electrónica.

CAROLINA
ESTEVES SOARES

Doutoranda em História, especialidade em História Moderna, na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa. É técnica de Apoio à Vítima na APAV desde 2017, sendo agora técnica da Linha Internet Segura e analista certificada pela INHOPE.

GONÇALO
GAGO DA CÂMARA

Advogado. Mestre em Direito Penal pela Faculdade de Direito da Universidade de Lisboa.

INÊS
PEREIRA DE MELO

É advogada, licenciada pela Faculdade de Direito da Universidade de Lisboa e pós-graduada em Direito Fiscal. Exerce sobretudo nas áreas do direito criminal e do direito fiscal e é docente no Instituto para o Desenvolvimento Social. Tem trabalhado em áreas de violência doméstica e em processos de crimes de ódio.

JOANA
MARTINS

Licenciada e mestre em Criminologia pela Faculdade de Direito da Universidade do Porto. Atualmente trabalha como *KYC Vetting Analyst* na Natixis em Portugal. Tem como áreas de interesse o cibercrime, a criminalidade económico-financeira e o crime organizado.

MANUEL
PEDROSA DE BARROS

É consultor em Segurança das Comunicações, Cibersegurança, Protecção da Privacidade e dos Dados Pessoais, nos aspectos técnicos de aplicação da legislação nacional e europeia. Foi Director de Segurança de Comunicações da Autoridade Nacional de Comunicações; membro activo de diversos grupos internacionais (UE, ENISA, OCDE, UIT) e nacionais (Comissão Instaladora do Centro Nacional de Cibersegurança, Futuro do SIRESP, Incêndios Florestais, Avisos à População, Conselho Gestor do Sistema de Certificação Eletrónica do Estado, Estrutura Nacional de Segurança, GMDSS).

PEDRO
VERDELHO

Magistrado do Ministério Público desde 1990, é Diretor do Gabinete Nacional de Coordenação na área do Cibercrime, da Procuradoria-Geral da República. Anteriormente, desempenhou funções de investigação criminal, entre outras, na área dos crimes informáticos. Foi docente do Centro de Estudos Judiciários (na área penal). Além disso, representa Portugal em diversos organismos internacionais na área do cibercrime.

RICARDO
ESTRELA

Licenciado em Direito pela Faculdade de Direito pela Universidade de Lisboa. Trabalha na APAV desde 2016. É gestor da Linha Internet Segura. Representa a APAV nas redes internacionais INSAFE e INHOPE.

JÚLIA
PAVIN

Julia Pavin é uma fotógrafa brasileira em busca das mais diversas expressões artísticas, por meio de campanhas publicitárias, editoriais e retratos.

01.

CIBERESPAÇO CIBERSEGURANÇA E CIBERCRIME

CARLOS PINTO DE ABREU
E BERNARDO PEREIRA GONÇALVES

I.

Vivemos actualmente numa sociedade de informação que nasceu ao abrigo das novas tecnologias e revolucionou as relações sociais, económicas e jurídicas de um modo que, há algumas décadas, seria inimaginável. No entanto, agora não é necessário recorrer à imaginação para verificar o impacto profundo que a galopante evolução tecnológica tem tido na sociedade, isto é, não há sector da nossa vida que não tenha sido afectado pelo fenómeno da informatização. Desde a defesa nacional, à actividade científica, passando pela actividade económica, pela saúde e a educação, todos os aspectos da nossa vida foram, com efeito, invadidos pela informática.

II.

Toda a informação (v.g., notícias, comunicações, dados de utilizadore de acesso, dados bancários, etc.) existe num espaço virtual – o ciberespaço – onde ocorre uma comunicação permanente entre redes compostas pelos mais variados aparelhos e dispositivos, tais como satélites, computadores, telemóveis, televisões e eletrodomésticos. Por outras palavras, qualquer aparelho com uma ligação à Internet é uma linha desta vasta rede que cobre o globo. Torna-se, por isso, evidente que este universo de informação se encontra em constate expansão, sendo cada vez melhores, menores e em maior número os equipamentos com esta particularidade. Na esteira do alargamento deste universo, surgem diversas oportunidades, mas também diversos desafios.
Por um lado, está aberto o caminho não só para uma maior democratização da informação – alcançável devido à redução dos custos de produção e à optimização da gestão de informação e à crescente disseminação e utilização de sistemas informáticos[1] – como também para o reforço da eficácia e da eficiência nas mais variadas áreas (v.g. direito, gestão, medicina, política, indústria militar, educação, comunicações, segurança e operações de socorro).
Por outro, torna-se absolutamente necessário evitar o erro, o abuso, a dispersão, o excesso, a inutilidade, a futilidade, a desactualização e a manipulação da informação. Além disso, cumpre salvaguardar a privacidade e a protecção de dados pessoais e de dados íntimos, e encontrar uma resposta adequada ao anonimato (que em certos casos é desejável e benéfico e noutros indesejável e prejudicial). É fundamental investir em meios técnicos especializados, bem como proteger as infraestruturas críticas e a integridade das redes de modo a garantir a operacionalidade.

III.

Tal como nos restantes domínios da vida, são dispersas e múltiplas as fontes e ameaça (v.g., desastres naturais, avarias, negligência humana, dolo, etc.), no entanto, no que respeita ao ciberespaço, os ataques intencionais levados a cabo por acessos não autorizados ou através de actos de sabotagem encerram percentagem significativa do perigo. Embora seja inquestionável que a evolução tecnológica permitiu um incremento da qualidade de vida dos cidadãos, também resultou na criação de novas formas de lesar direitos e de prejudicar interesses alheios, tanto individuais como colectivos. Surgiu assim a criminalidade informática, e começaram a estudar-se e a regular-se o cibercrime, o ciberterrorismo, a ciberespionagem e o fenómeno do *hacktivismo*. O número de ataques registados, dirigidos tanto a empresas como a pessoas individuais, tem vindo a aumentar nos últimos anos[2],

1. Devido, não só à redução dos seus custos de produção, ao aumento exponencial da velocidade de processamento e à miniaturização, como também ao decréscimo das dificuldades da sua utilização.

2. Veja-se, a título de exemplo, o Relatório Anual de Segurança Interna 2020 (disponível em www.portugal.gov.pt/pt/gc23) que, apesar de registar, em geral, um decréscimo de participações criminais, registou um aumento concreto de 26.8% relativamente à participação de crimes informáticos.

facto que veio evidenciar a importância e a perigosidade das crises informáticas desta natureza e de alguns dos métodos de ataque utilizados[3].

IV.

Segundo se tem vindo a entender[4], a criminalidade informática pode ser entendida em sentido amplo, abrangendo condutas em que o sistema informático é apenas um de vários meios para a prática de um determinado crime[5] ou, em sentido estrito, compreendendo apenas as condutas em que a "informática" aparece como um elemento do tipo legal de crime ou como bem jurídico protegido[6]. E no que toca ao cibercrime, importa ter presentes dois diplomas legais essenciais.
Em primeiro lugar, a Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), que além de estabelecer disposições penais, materiais[7] e processuais, estabelece também disposições relativas à cooperação internacional em matéria penal, e relativas e à recolha de prova em suporte eletrónico. No domínio da lei em causa também as pessoas colectivas e entidades equiparadas são susceptíveis de responsabilidade criminal, nos termos do artigo 9.º [8].

Relativamente à obtenção de prova digital, são estabelecidas algumas medidas especiais: a preservação expedita de dados, a revelação expedita de dados de tráfego e a injunção para apresentação de dados ou concessão de acesso a dados[9].
Além da supra referida Lei do Cibercrime, também o Código Penal prevê alguns crimes[10] relevantes neste particular domínio. Importa ainda ter em conta outros normativos relevantes, tais como o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 (Regulamento Geral sobre a Protecção de Dados); a Lei n.º 46/2018, de 13 de Agosto (Regime Jurídico da Segurança do Ciberespaço) e o respectivo Decreto-Lei 65/2021, de 30 de Julho; a Lei n.º 32/2008, de 17 de Julho (Lei da Conservação de Dados); a Lei n.º 58/2019, de 8 de Agosto (Lei da Protecção de Dados Pessoais); a Lei n.º 16/2022, de 16 de Agosto (Lei das Comunicações Eletrónicas)[11]; a Lei n.º 41/2004, de 18 de Agosto (Protecção de Dados Pessoais e Privacidade nas Telecomunicações); o Decreto-Lei n.º 252/94, de 20 de Outubro (Regime de Protecção Jurídica dos Programas de Computador); e o Decreto-Lei n.º 122/2000, de 4 de Julho (Regime de Protecção Jurídica das Bases de Dados).

V.

Dada a multiplicidade de riscos de ataque informático e a extrema dificuldade de reparação dos seus danos, o foco essencial no que toca à cibercriminalidade, em especial no domínio empresarial, prende-se com uma lógica de prevenção, que passa pelo investimento na cibersegurança, pela formação dos funcionários, habilitando-os a identificar sinais de perigo e a reagirem de forma imediata, e pela elaboração de protocolos de defesa e de planos de acção e de reacção.
Veremos que tal é insuficiente.
O esforço para a antecipação dos possíveis cenários de ataque pode ser crucial para que seja dada uma resposta pronta e eficaz, adequada a evitar as consequências mais gravosas de um ataque. Se, pelo contrário, não for dada uma resposta apropriada, tal pode potenciar os efeitos danosos.
A contenção de danos é o objectivo primário de qualquer vítima de um ataque informático.
Posteriormente, há que analisar tanto as causas como os efeitos dos incidentes, e elaborar novos procedimentos de modo a melhorar os métodos de resposta e reduzir o risco de eventos futuros causadores de danos. Mas é essencial prever mecanismos de assunção de responsabilidades.
Importa ainda, para garantir o sucesso da cibersegurança, assegurar o cumprimento de todas as obrigações legais, nomeadamente ao nível do tratamento e protecção de dados e das infraestruturas, e actuar sempre com base na cooperação com todas as partes envolvidas, desde clientes às diversas entidades nacionais e internacionais directa ou indirectamente responsáveis pela segurança informática, tais como o Ministério Público e os Órgãos de Polícia Criminal, o Centro Nacional de Cibersegurança, as Autoridades Reguladoras, as Ordens Profissionais, a Rede Nacional CSIRT, a EUROPOL, a INTERPOL, a EUROJUST e, agora, a Procuradoria Europeia.
O ciberespaço é uma realidade recente, que se encontra em constante mutação e representa inúmeros desafios.
As vantagens são múltiplas, mas os perigos também. O cibercrime representa um sério problema de segurança que pode afectar toda e qualquer pessoa, causando danos potencialmente irreparáveis.
A tecnologia possibilita ataques anónimos, transnacionais, com consequências muito gravosas.

Assim, no que diz respeito à cibersegurança, a prevenção, a cooperação e a formação são elementos-chave para minimizar os riscos inerentes ao mundo informatizado em que hoje vivemos; mas que não prescindem da acção imediata, adequada e inteligente.

3. Tais como o *phishing*, que se traduz na tentativa de obter ilicitamente credenciais de acesso a sistemas informáticos.
4. V. Venâncio, Pedro Dias, Lei do Cibercrime Anotada e Comentada, Coimbra Editora, 2010.
5. Por exemplo, um crime de injúria, p.e.p. no artigo 181.º do Código Penal, praticado com recurso a um computador.
6. Como acontece, por exemplo, nos artigos 3.º a 8.º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro).
7. Nomeadamente, artigos 3.º (Falsidade informática); 3.º-A e seguintes, relativos à contrafacção de cartões ou outros dispositivos de pagamento, incluindo moedas virtuais; 4.º (Dano relativo a programas ou dados); 5.º (Sabotagem informática); 6.º (Acesso ilegítimo); 7.º (Intercepção ilegítima); 8.º (Reprodução ilegítima de programa protegido).
8. Que remete para o regime de responsabilização previsto no artigo 11.º do Código Penal.
9. Previstas nos artigos 12.º, 13.º e 14.º, respectivamente.
10. Nomeadamente, nos artigos 193.º (Devassa por meio da informática); 194.º (Violação de telecomunicações); 221.º (Burla informática e nas comunicações); 225.º (Abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento).
11. Que entrará em vigor a 14 de Outubro de 2022, revogando a Lei 5/2004, de 10 de Fevereiro.

02.

CIBERCRIME EM TEMPO DE PANDEMIA: – ALÉM DA COVID, PORTUGAL TAMBÉM FOI ATINGIDO PELO CIBERCRIME!

PEDRO VERDELHO

1 Para quem não tenha formação jurídica, o cibercrime é uma nebulosa de contornos muito pouco definidos, que conjuga crime com o ambiente cibernético. Para o mais apurado e rigoroso dos juristas é difícil encontrar, para lá deste conceito vago, uma melhor e mais rigorosa definição científica de cibercrime, com a qual logre convencer os seus pares.
Ambos concordarão num aspeto: as realidades que integram aquela difusa nebulosa chegaram para ficar, expandem-se a uma velocidade visível ao mais nu dos olhos de qualquer observador, atingindo um muito crescente número de vítimas.
Chegam diariamente às autoridades públicas denúncias de violações de privacidade *online*, de divulgação de fotografias e dados pessoais, de quebras de funcionamento de sistemas informáticos, de acessos ilegítimos, de burlas em compras na Internet e fraudes relacionadas com cartões de crédito ou com supostos investimentos mirabolantes, entre muitas outras.
São fenómenos de uma criminalidade sem rosto, perpetrada por criminosos que, muito longe, em países e até continentes distantes, se escondem por detrás da opacidade de ecrãs e atuam a partir de locais insuspeitados pelas vítimas. Estas, mais que em relação a outras criminalidades, sentem-se impotentes e indefesas perante os cibercriminosos.
É, pois, muito relevante que a *Miscellanea APAV* entre neste novo espaço digital, explicando-o e alertando potenciais vítimas para atuações criminosas, dando pistas àqueles a quem compete dar-lhes apoio.

2 O Gabinete Cibercrime da Procuradoria-Geral da República é um gabinete de coordenação nacional da atividade do Ministério Público que, pela natureza das suas funções, acompanha a evolução dos fenómenos cibercriminosos que mais vitimizam os cidadãos. Recebe anualmente centenas de denúncias de vítimas de cibercrime, que encaminha para os Departamentos de Investigação e Ação Penal do Ministério Público nas comarcas do país. A circunstância de ter ação de âmbito nacional permite-lhe ter uma visão englobante de todos estes fenómenos.
Na prática judiciária, é habitual referenciar-se este genérico universo do cibercrime como um conjunto homogéneo de ilícitos penais, que inclui, naturalmente, os crimes contra a disponibilidade, integridade e confidencialidade dos sistemas de informação, descritos na Lei do Cibercrime – Lei nº 109/2009 (designadamente a falsidade informática, o dano informático, a sabotagem informática, o acesso ilegítimo e a interceção ilegítima), mas também os crimes de burla informática e de pornografia infantil (incluídos no Código Penal). Porém, pelo meio em que surgem e pelas formas como se manifestam, também é habitual agregarem-se às manifestações de cibercrime diversos outros tipos de ilícito, chamados *online*, como as burlas em plataformas de vendas online, ou a divulgação ilícita de fotografias e outros dados pessoais, ou os crimes contra a honra, ou ainda a difusão e pornografia infantil ou os crimes contra o direito de autor.

3 O Gabinete Cibercrime monitoriza estes fenómenos criminosos a partir das denúncias que recebe por via de correio eletrónico. Tais denúncias, que no ano de 2021 superaram as mil e cem, não correspondem a todas aquelas que são apresentadas ao Ministério pelos diversos canais. Todavia, pela sua expressão numérica são consideradas uma amostra muito significativa das mesmas.

4 Uma primeira nota importa sublinhar a este respeito. Desde que passou sistematicamente a monitorizar-se este tipo de denúncias, em 2016, tem-se verificado um constante e persistente aumento do número das mesmas. Isto é, todos os anos, de ano para ano, os portugueses são crescentemente vítimas de fenómenos de cibercriminalidade.
Nos anos mais recentes, de 2020 e 2021, o aumento dos casos (e, portanto, das vítimas) de cibercriminalidade foi excecional: desde o final de 2019, de forma consistente, de ano para ano, as queixas mais que têm duplicado as do ano anterior.
Importa ainda registar que após a eclosão da pandemia da COVID–19, no início de 2020, a progressão do número destes fenómenos foi muito maior. Além disso, nos períodos de confinamento obrigatório dos cidadãos aos seus domicílios, decorrentes da pandemia (quer em 2020, quer em 2021) as queixas por crimes na área da cibercriminalidade aumentaram de forma ainda mais expressiva, de modo extraordinário.
Não obstante, embora em momentos mais críticos da pandemia o número de casos tenha sido muitíssimo mais elevado, não pode concluir-se que esse aumento de cibercriminalidade esteja apenas associado à situação pandémica. Embora a pandemia possa efetivamente ter impulsionado o aumento deste tipo de criminalidade, esta tendência crescente, que já antes se afigurava constante e consistente, voltou a revelar essa tendência com o aligeiramento das restrições associadas à COVID.

5 Uma das mais marcadas características associadas à criminalidade *online* é a da sua evolução permanente – não apenas evolução numérica, de crescimento, mas também de diversificação.
Os métodos criminosos vão-se sucedendo, surgindo, desenvolvendo-se em massa e depois desaparecendo, consoante o conhecimento público dos mesmos se difunde e as medidas tecnológicas de segurança os vão conseguindo enfrentar. Apesar disso, algumas das técnicas usadas pelos cibercriminosos vão persistindo no tempo, sofisticando-se, para contornar as medidas defensivas adotadas.
Esta é uma nota importante, porque o exercício que vai de seguida fazer-se, de análise da cibercriminalidade de que são presentemente vítimas os portugueses, pode vir a ficar rapidamente desatualizado: as experiências passadas mostraram que a realidade do crime *online* observada durante o ano de 2020 foi diferente daquela que se mostrou em 2021.
A evolução anotada ao longo deste último ano permite desde já afirmar que o cenário que se revelará ao longo do ano de 2022 será também seguramente diferente.

6 Um dos fenómenos cibercriminosos que mais tem vitimizado os portugueses é o do *phishing*. Esta expressão é o nome dado um processo criminoso ardiloso, que tem em vista obter ilicitamente credenciais de acesso de outrem (nome de utilizador, *passwords*…) a contas *online* (podem ser contas de *email*, contas bancárias, contas em redes sociais, contas em serviços *online* ou outras).
Normalmente, os criminosos começam por remeter milhares de mensagens (de email, de SMS ou mesmo de *WhatsApp*) para destinatários desconhecidos.
Conseguem os contactos dos mesmos em listagens ilegalmente obtidas, por exemplo, disponíveis na *darknet*.
Em tais mensagens, os criminosos incitam a vítima a aceder a uma página *web*, onde deverão inserir as suas credenciais de acesso. Porém, o *link* disponibilizado pela mensagem

não corresponde à autêntica página do banco, ou do serviço de *email*, mas antes a uma página falsa, gerida pelos próprios criminosos. Desta forma, se a vítima introduzir ali as suas credenciais de acesso estará a facultá-las ao criminoso, que depois poderá fazer uso das mesmas, acedendo ao seu *email*, à sua conta bancária, ou a outros serviços que subscreva *online*.

7 Numericamente, o *phishing* foi um dos motivos mais significativos de denúncia por crimes *online* em 2021. Durante este ano continuaram a multiplicar-se, de forma regular, campanhas de *phishing* especificamente dirigidas a vítimas em Portugal (bancos portugueses). A generalidade dos bancos de Portugal viu assim surgir clones das suas páginas *online*, produto de ação criminosa.
Muitas vítimas portuguesas, enganadas por este ardil, facultaram assim a criminosos as suas credenciais de acesso a contas bancárias.
A frequência desta prática criminosa tem levado os bancos a reforçar as medidas de segurança no acesso *online* a contas bancárias, designadamente introduzindo mais e novos modos de autenticação.

8 Ainda mais frequente que esta modalidade, foi a prática de *phishing* destinado à obtenção ilícita de dados de cartões de crédito.
Aliás, esta variante foi a mais frequentemente denunciada pelas vítimas portuguesas, correspondendo a quase 15% dos casos reportados.
O modo de atuar dos criminosos é similar, mas mais dissimulado.
Tal como sucede no *phishing* bancário, nesta modalidade o processo também começa com a remessa indiscriminada de mensagens para milhares de destinatários. Tais mensagens apelam sempre à urgência no acesso a um *link*. Esse *link* aponta para uma página falsa, gerida pelos criminosos onde, de forma ardilosa, as vítimas são induzidas a introduzir todos os dados dos seus cartões de crédito.

9 Nalguns casos, as páginas falsas alegam pertencer a bancos, referindo ainda que tais bancos pretendem atualizar os seus dados.
Noutros, muito frequentes, os sites alegam pertencer a serviços postais, alegando falsamente carecer dados dos cartões de crédito para entregar uma determinada encomenda.
Noutros ainda, os sites alegam pertencer a prestadores de serviços públicos (eletricidade, por exemplo) ou à administração fiscal, informando falsamente a vítima de que tem um reembolso para receber, necessitando, para esse efeito, de facultar os dados do seu cartão de crédito.

10 Têm sido recorrentemente identificadas, nos últimos meses, sucessivas campanhas de *phishing* desta natureza, abusando das imagens de entidades como a AT – Autoridade Tributária, ou a EDP – Energias de Portugal, ou ainda os CTT – Correios.
A expansão deste modelo de prática criminosa foi enorme após a eclosão da pandemia da COVID-19, a qual teve associado, também, um enorme aumento das compras *online* e, por conseguinte, da necessidade de utilização, pelas vítimas, de serviços de pagamento *online*.
Com efeito, em muitíssimas situações, o processo criminoso passou pela solicitação do pagamento de uma "pequena taxa", relacionada com uma encomenda dirigida à vítima. Este detalhe era credível para muitas vítimas, uma vez que, efetivamente, tinham procedido a compras à distância, *online*.

11 Aliás, a área do comércio eletrónico tem sido terreno fértil para várias outras manifestações de cibercriminalidade.
Trata-se de uma realidade em imensa expansão, desenvolvendo-se de forma particularmente expressiva durante as restrições à circulação e ao acesso físico ao comércio, resultantes da pandemia.
Todavia, esta tendência crescente manteve-se após o levantamento daquelas medidas restritivas.
Por este motivo, esta área passou a ser atrativa para a criminalidade que, progressivamente passou a entranhar-se nas compras e vendas *online*.
As burlas em compras e vendas têm vindo a expandir-se, tornando-se num dos fenómenos de cibercriminalidade mais frequente, provocando um grande prejuízo económico efetivo aos portugueses.

12 Existem burlas em compras e vendas nas diversas plataformas *online* legítimas, as quais são assim abusivamente aproveitadas pelos criminosos para os seus propósitos ilícitos. Da mesma forma, existem burlas em compras e vendas efetuadas por via das redes sociais.
Em ambos os casos, os criminosos usam a técnica de criar contas específicas para disponibilizar produtos para venda: disponibilizam bens para venda, em geral por um preço muito vantajoso; aceitam o legítimo pagamento de múltiplos compradores de boa-fé e, após receberem os valores da compra encerram subitamente a sua conta sem que seja possível serem de novo contactados.
Em geral, com a disponibilização de um só anúncio, ou de um só produto, os criminosos conseguem defraudar

um grande número de vítimas num espaço muito curto de tempo. Depois, encerram as contas, abrindo subsequentemente outras contas para dar continuidade à sua atuação criminosa.

13 Como se disse, este tipo de criminalidade tem atingido muitíssimas vítimas em Portugal, causando muitos prejuízos às mesmas. Embora o produto de cada venda fraudulenta nunca seja muito elevado (em geral, raramente ultrapassando as dezenas de euros), pelo enorme número de vítimas que esta atuação efetivamente tem atingido, o seu significado económico é muito relevante.
Este fenómeno é, como se disse, numericamente muito expressivo, sendo daqueles que deu mais origem a queixas de vítimas portuguesas (apenas superado pelo *phishing*).

14 Os meses mais recentes (segundo semestre de 2021) revelaram a massificação de uma forma mais agressiva e lesiva de defraudação em compras e vendas *online*: a criação de páginas falsas de marcas de roupa, calçado ou equipamento desportivo. Multiplicaram-se na Internet páginas supostamente correspondentes a marcas conhecidas no mercado, muito semelhantes às mesmas, mas geridas por criminosos, com intuitos fraudulentos. Tais páginas são anunciadas em redes sociais e noutras páginas na Internet, para captarem mais visitas. Reproduzem, copiando, o aspeto e os conteúdos das autênticas páginas das marcas em causa, procurando convencer quem as visita a efetuar compras *online* por via delas. Com esse propósito, estas páginas falsas anunciam sempre grandes promoções, saldos ou enormes descontos (com frequência de 70 ou 80% do preço de base, a terminar no próprio dia). Por outro lado, estas páginas nunca indicam qualquer forma de contacto com os respetivos responsáveis e, em geral, apenas permitem o pagamento das compras com cartão de crédito.

15 Em Portugal têm sido reportadas inúmeras páginas falsas, que vão surgindo e desaparecendo, para dar lugar a outras, exatamente iguais, mas em local diferente (portanto, com um *link* diferente). Têm sido muitas as vítimas a queixarem-se de terem comprado bens em páginas que vieram a verificar ser deste tipo – bens esses que, apesar de pagarem (com cartão de crédito), naturalmente nunca receberam.
Tal como acontece com as contas do *Facebook* ou *Instagram* abertas com intuitos fraudulentos também estas páginas falsas acabam por provocar um grande número de vítimas num espaço muito curto de tempo, após o qual, com frequência, o respetivo *URL* é bloqueado.

16 Além das falsas páginas de marcas de roupa, de marcas de 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.

17 As falsas páginas de hotéis ou de alojamento local são particularmente nocivas para as vítimas: em geral, são páginas fraudulentas que aceitam reservas para alojamento, como se se tratasse da autêntica página do alojamento em causa. Cobram o serviço por antecipação, em geral por via de cartão de crédito. Portanto, a vítima tem muita dificuldade em reaver o valor em que foi burlada. Por outro lado, normalmente, a vítima é confrontada com o crime apenas no momento em que chega ao alojamento, para gozar as suas férias, ficando muitas vezes numa situação vulnerável: sem alojamento e sem dinheiro para pagar outro alojamento.

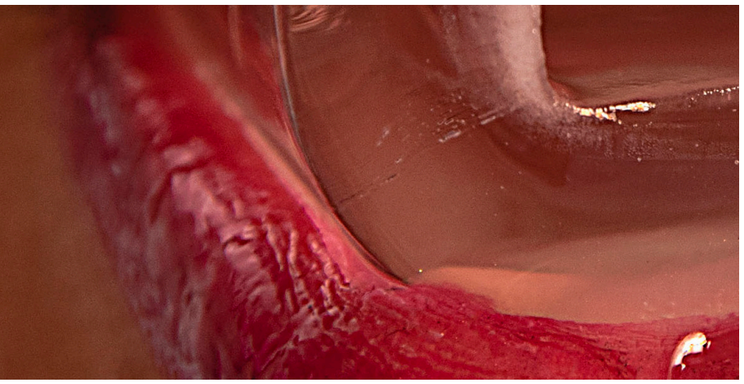
18 Outra forma muito incisiva de burla por via de páginas falsas traduz-se na criação de falsas páginas de venda de equipamento médico de proteção (máscaras, luvas, gel desinfetante...). Estas páginas *web* surgiram abundantemente após a eclosão da pandemia e normalmente as vítimas que procuram são empresariais: aceitam encomendas de equipamento em grande quantidade, com frequência no valor de milhares de euros.

19 Também tem vindo a multiplicar-se a criação de falsas páginas na Internet de natureza institucional, isto é, de páginas que procuram imitar as autênticas páginas de instituições publicas ou páginas que prestam serviços públicos.
Foram já há vários anos identificadas páginas que alegam prestar serviço nas áreas dos registos públicos, prometendo, por exemplo, facultar, mediante um pagamento, certidões de nascimento, ou certidões do registo predial. Foi até identificado um conjunto de páginas que prometia divórcios *online*, disponível 24 horas por dia. Ou um conjunto de páginas que prometia remeter para casa dos interessados a carta de condução, sem que fosse necessário frequentar aulas ou fazer qualquer exame.

20 No segundo semestre do ano de 2021 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 COVD da UE, sem qualquer verificação ou confirmação dos respetivos requisitos. Portanto, permitiam a quem visitasse estas páginas gerar falsos documentos públicos.

21 Todas estas páginas, fingindo ser páginas de serviços públicos ou imitando as autênticas páginas de instituições públicas, tal como as falsas páginas de marcas comerciais, surgem e vão sendo bloqueadas, dando origem a novas páginas com novos *URL*, alojadas noutro fornecedor de serviços em nuvem, numa mutação muito difícil de reprimir com eficácia antes de que produzam vítimas.

22 Dando continuidade ao que se observou em anos anteriores, os tempos recentes revelaram ainda, embora com menor expressão do que já teve, um fenómeno fraudulento com grande impacto nas vítimas: o das burlas *online* no mercado imobiliário.
Trata-se de uma prática criminosa que passa pela difusão enganosa de propostas de arrendamento de imóveis que não existem (ou que existindo, não pertencem ao anunciante, nem estão disponíveis para arrendamento). Sob o pretexto de assinatura de um contrato firme, o burlão sugere à vítima o pagamento de uma quantia correspondente a rendas antecipadas – uma vez pagas estas rendas antecipadas, o criminoso desaparece, não mais sendo possível contactá-lo.
Em Portugal esta atividade é mais intensa nos meses de agosto e setembro, altura em que muitos estudantes universitários procuram alojamento nas cidades para onde se deslocam.

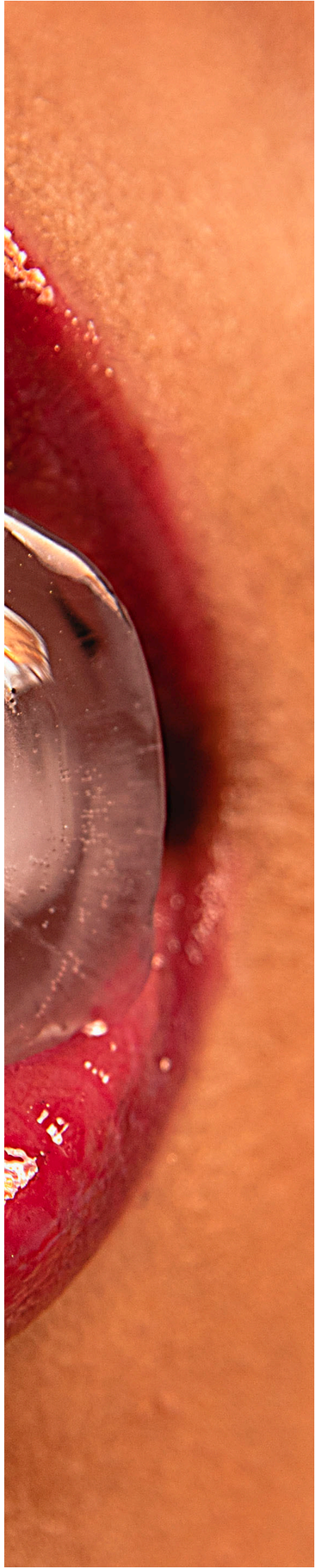


23 Os criptoativos impuseram-se e tornaram-se uma realidade presente em muitas facetas da vida: são repositório de valor em tempo de crise, moeda de troca, investimento, apenas para referir facetas correntes e permitidas.
A estagnação económica de anos recentes, com muito baixas taxas de juro, tornou os criptoativos apelativos, por permitirem obter alguma rentabilidade – sem prejuízo, claro, do enorme risco que um tal investimento significa.
Passou assim a haver uma enorme oferta deste tipo de ativos.
Rapidamente se percebeu que alguma desta oferta, muito visível e ruidosa na Internet, é criminosa e não tem outro propósito que não o de burlar aqueles a quem se dirige. Muitos têm sido os portugueses que são vítimas deste tipo de burla: em geral, acedem a 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 por aquelas.
Neste tipo de burla a credulidade é um fator essencial: as vítimas invariavelmente entregam o seu dinheiro, para supostamente realizarem investimentos, a pessoas que não conhecem, nem viram nunca, com quem apenas falaram por telefone, ou até apenas por mensagens escritas.

24 Este é também o cenário de fundo de um outro tipo de burlas com grande expressão, perpetradas num contexto de relacionamento amoroso à distância, exclusivamente *online*.
Na Internet abundam plataformas cujo propósito é o de estabelecer o contacto entre pessoas que buscam um relacionamento pessoal ou íntimo com outras pessoas. Por outro lado, as diversas redes sociais são regulamente usadas pelos seus utilizadores para exporem as suas vidas e as respetivas venturas e desventuras. Estas realidades têm sido aproveitadas por redes criminosas pouco escrupulosas que, nas plataformas de relacionamento e nas redes sociais, identificam pessoas que lhes pareçam sozinhas ou carentes. Procuram contactá-las e aproximar-se das mesmas, com o propósito de irem contruindo uma relação à distância. Normalmente, os alvos são senhoras de meia-idade que vivem sozinhas. Os criminosos identificam-se como homens igualmente sozinhos, cidadãos europeus ou norte-americanos em missão de risco no estrageiro (por exemplo, supostos militares da ONU em missão no Iraque, ou supostos comandantes de navios a navegar em alto mar, ou supostos médicos em serviço em zonas de conflitos militares).
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 que têm sido 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.
Ano após ano, progressivamente, este tipo de criminalidade tem causado sérios prejuízos patrimoniais às vítimas, nalguns casos de dezenas de milhares de euros.

25 Igualmente dá origem a muito relevantes prejuízos patrimoniais em Portugal o fenómeno conhecido como *CEO fraud*, ou *BEC* (*business email compromise*).
É um modelo criminoso muito sofisticado, que recorre à chamada engenharia social: em breves termos, por via de ardilosas mensagens de correio eletrónico, os criminosos induzem em erro membros de uma estrutura empresarial, levando-os a efetuar pagamentos a terceiros (os próprios criminosos), que normalmente 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. Atuam sempre contra vítimas de outros países.
Em Portugal foram identificadas como vítimas empresas estrangeiras, que foram enganosamente induzidas a efetuar pagamentos para contas bancárias de bancos em Portugal.
Do mesmo modo, foram identificadas sociedades comerciais portuguesas que ardilosamente foram levadas a efetuar pagamentos com destino a contas bancárias estrangeiras.

26 É igualmente da engenharia social que se socorrem os criminosos para perpetrarem o tipo de burla conhecida na gíria internacional como *technical assistance scam* e mais referenciado em Portugal como "falsas chamadas da Microsoft". Este tipo de fraude passa pela realização, pelos criminosos, de chamadas telefónicas durante as quais tentam convencer as vítimas, de forma astuciosa e enganadora, 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.
Normalmente, os criminosos identificam-se como técnicos do apoio informático da Microsoft, referindo ter solução para o problema encontrado.
Têm ocorrido casos em que a vítima é convencida a instalar *software* – naturalmente de origem maliciosa, podendo danificar, roubar dados, encriptar ou até mesmo inutilizar o sistema. Noutros casos é sugerido à vítima que aceda a uma determinada página na Internet e aí introduza os dados do seu cartão de crédito. Ou ainda que partilhe o seu ecrã com o criminoso e que, mantendo o ecrã partilhado, aceda à sua conta de *homebanking*.
Portanto, em suma, este método visa permitir aos criminosos aceder a meios de pagamento das vítimas, ficando assim em posição de os virem a utilizar, mais tarde, em seu proveito.



27 É também o intuito de lucro que incentiva os criminosos à prática daquilo que no jargão ciber policial tem sido conhecido como *sextortion*. Trata-se de um fenómeno massificado de coação, em que os agentes criminosos, por via de mensagens de correio eletrónico, que mandam para milhares de destinatários, tentam convencer vítimas a pagarem-lhes quantias monetárias (invariavelmente em *bitcoins*), sob a ameaça de divulgação pública de dados, imagens ou informações pessoais das mesmas.
Nestas tentativas massificadas o criminoso explora o desconhecimento e o receio da vítima, que não conhece e da qual não tem qualquer informação.

28 Diferente deste fenómeno, mas igualmente referido com frequência como *sextortion*, é a exigência de quantias sob pena de divulgação de imagens íntimas, geralmente de natureza sexual, em casos individuais (isto é, em casos em que o criminoso apenas está a chantagear uma vítima específica – e não a expedir mensagens em massa, como no fenómeno anterior).
Este tipo de situação ocorre sobretudo quando o criminoso e a vítima se conhecem e mantiveram no passado uma relação pessoal ou íntima. Muitas vezes este fenómeno ocorre com vítimas que, *online*, travaram conhecimento com pessoas desconhecidas, a quem mandaram imagens ou gravações de vídeo suas.

29 Nas franjas deste tipo de criminalidade, sobretudo económica, visando o lucro, existem outros tipos de práticas criminosas, designadamente animada por propósitos pessoais ou egoísticos. Todas elas têm uma expressão numérica mais reduzida, embora ocorram regularmente em Portugal.

30 É o caso, por exemplo, das situações de *stalking*, ou perseguição com uso das tecnologias. Ocorre em geral num quadro de relacionamento pessoal (melhor: em geral, de rotura de relacionamento pessoal), entre a vítima e o agressor.

31 Mas é também o caso, embora pouco expressivo, de manifestações do chamado discurso de ódio. Ocorre, entre outras formas, com a publicação de textos ou comentários em redes sociais, ou mesmo em órgãos de comunicação social, em que se incita ao ódio, à violência, ou ainda à discriminação, por motivos raciais ou étnicos. Mas ocorre também com atitudes ou iniciativas especificamente dirigidas a vítimas concretamente identificadas e visadas.

32 São também específicas e identificadas as vítimas de uma forma de cibercriminalidade de franja, mas significativa, que é a divulgação *online* de fotografias ou outra informação pessoal ou íntima.
Existem manifestações menos graves deste fenómeno, por exemplo de uso não autorizado de fotografias das vítimas, ou por exemplo na criação de perfis ou contas falsas, em redes sociais, com fotografias ou outras informações das vítimas assoiadas.
Outras manifestações são mais gravosas. É o caso da divulgação de fotografias íntimas das vítimas, ou da publicação de anúncios em páginas de encontros ou de prostituição, associando-se a esses anúncios fotografias íntimas e dados verdadeiros das vítimas.

03.

VITIMAÇÃO POR FURTO DE IDENTIDADE *ONLINE*

JOANA MARTINS

Introdução

O desenvolvimento da tecnologia e da Internet levou não só a que novos crimes surgissem, mas, também, permitiu que outros se estendessem para o mundo *online*, como é o caso do furto de identidade *online*. Além disso, com a chegada da pandemia de Covid-19, inevitavelmente, a dependência do ciberespaço para a realização de diversas atividades diárias aumentou. Consequentemente, também os ciberofensores se deslocaram para o contexto digital na procura de oportunidades criminais com efeitos nefastos para as vítimas.

Nesta senda, o presente trabalho pretende dar atenção científica a este fenómeno que é a vitimação por furto de identidade *online*. Para o efeito, será apresentada a definição de cibercrime, o seu enquadramento legal e, também, o impacto da pandemia no mesmo. Posteriormente, será feita uma revisão teórica sobre este objeto de estudo, nomeadamente no que concerne à delimitação conceptual, *modus operandi* através do qual é perpetrado e, ainda, será discutida a importância de algumas variáveis individuais (*e.g.*, género, idade, estatuto socioeconómico e educação) que a literatura tem apontado como determinantes da vitimação por esta ofensa em específico. Por fim, será abordada a importância da prevenção deste fenómeno.

Cibercrime

Definição

Este inegável progresso da Internet e consequente transferência de atividades de rotina para o ciberespaço a partir dos anos 90 do século XX, desencadearam o desenvolvimento do que muitos autores denominam como cibercrime (Guedes *et al.*, 2021) que, hoje, já não se trata de um facto negável (Correia, 2021). A grande problemática relacionada com o cibercrime diz respeito à sua conceptualização pois, apesar de os autores concordarem que este é um dos grandes desafios criminais da atualidade, não há uma definição que seja universalmente aceite (Yar, 2006; Fafinski *et al.*, 2010). Esta dificuldade conceptual advém do rápido desenvolvimento tecnológico, das divergências existentes nas diferentes legislações e da existência de múltiplos atores, públicos e privados, envolvidos na regulação e controlo do cibercrime (William & Wall, 2013). Não obstante se verificar que existem múltiplas expressões para designar a prática de ofensas no contexto digital (*e.g.*, crime informático, crime digital e crime relacionado com computadores), neste artigo será adotado o termo cibercrime, abarcando o conjunto de ofensas que partilham uma característica, que é o facto de serem cometidas através de um computador e de tecnologia, como a Internet.

Em Portugal, Venâncio (2011, p. 17) apresenta uma definição de cibercrime segundo uma perspetiva jurídica, categorizando os cibercrimes em sentido amplo e sentido estrito. Nas palavras do autor:

"em sentido amplo (…) a criminalidade informática englobará toda a panóplia de atividade cibercriminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios. Em sentido estrito, entendemos nós que a criminalidade informática abarcará apenas aqueles crimes em que o elemento digital surge como parte integradora do tipo legal ou mesmo como o seu objeto de proteção."

Já ao nível internacional, segundo Wall (2007), é possível identificar diferentes tipos de cibercrimes de acordo com a mediação tecnológica. Em primeiro lugar, podem reconhecer-se os crimes tradicionais que utilizam os computadores como mera assistência, como acontece, por exemplo, com as fraudes bancárias e com o furto de identidade *online*. Estas ofensas têm um elevado impacto, uma vez que, mesmo que a Internet seja removida continuarão a persistir, dado que os ofensores vão apenas mudar a forma como os cometem. Por outro lado, identificam-se os crimes convencionais para os quais o aparecimento da Internet criou oportunidades globais, isto é, permitiu que o crime praticado tenha um impacto mais vasto e até mesmo global. Neste caso, o computador não é o instrumento principal da atividade, mas o meio de realização de prova assume a forma digital (*e.g.*, tráfico de droga; Grabosky, 2004). Por último, identificam-se os verdadeiros cibercrimes, ou seja, aqueles que são fruto da própria Internet e não existiriam sem ela (*e.g.*, *hacking*). Para

além disto, Wall (2007) acrescenta que os cibercrimes se podem definir de acordo com as ofensas cometidas e, neste sentido, distinguir-se-iam três tipos, nomeadamente, i) crimes contra a integridade dos computadores, como o *hacking* e os vírus; ii) crimes assistidos por computadores, como as fraudes; e iii) crimes relacionados com o conteúdo dos computadores, como a distribuição de pornografia. Outra distinção muito acolhida na literatura científica é a de Furnell (2002) e que tem como critério principal o papel desempenhado pela tecnologia. Neste sentido, o autor distingue as ofensas focadas no computador e as ofensas assistidas pelo computador. As primeiras englobam os crimes que têm como alvo a própria infraestrutura eletrónica. Já as segundas abarcam os crimes que já existiam antes da Internet, mas que agora encontram uma nova via para serem cometidos.

Enquadramento legal

Para além da delimitação conceptual do conceito de cibercrime, também se tem procurado enquadrar legalmente as ofensas que ocorrem no ciberespaço. Efetivamente, verifica-se ao nível europeu que existe uma tentativa de harmonização legal em relação ao cibercrime. Contudo, apesar dos esforços, ainda não se encontra um acordo em função das singularidades de cada sistema legal e jurídico (Yar, 2006). Ao nível nacional, a intervenção é feita através do Código Penal (CP) e através da Lei do Cibercrime - Lei nº 109/2009, de 15 de setembro.

Relativamente à Lei do Cibercrime, no artigo 11º, encontra-se uma definição que diz respeito à criminalidade informática e cuja definição alude a todos os atos em que "o computador serve como meio para atingir um objetivo criminoso ou em que o computador é alvo simbólico desse ato ou em que o computador é objeto do crime". Para além disso, esta lei é igualmente aplicável às situações em que os crimes são cometidos por meio de um sistema informático ou em relação aos quais se verifique a necessidade de recolher prova em suporte eletrónico. Já ao nível do direito penal português, há uma intervenção nesta matéria ao nível do CP para proteção do fim criminoso e dos bens jurídicos visados. Ademais, o cibercrime não se reduz ao CP, estende-se à Lei nº 46/2018, de 13 de agosto, que transpõe uma diretiva do parlamento e conselho europeu, e que visa estabelecer o regime jurídico da segurança no ciberespaço.

Apesar do marco legal da cibercriminalidade em Portugal ser a Lei do Cibercrime, a regulamentação deste fenómeno não se limita a esta lei. Quanto ao sistema judiciário português, mais concretamente na competência da Polícia Judiciária, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica é a unidade operacional especializada que dá resposta à cibercriminalidade, tendo como principais missões a prevenção, detenção e investigação deste fenómeno (Decreto-Lei n.º 81/2016, de 28 de novembro). Quanto ao Ministério Público, foi criado o Gabinete do Cibercrime[1] que tem como missão a coordenação, a formação de magistrados, a interação com o setor privado e com os órgãos de política criminal e, eventualmente, o acompanhamento de determinados processos. Já o Centro Nacional de Cibersegurança (CNCS)[2], funciona no âmbito do Gabinete Nacional de Segurança, e tem como principais linhas de ação a sensibilização para comportamentos mais seguros e responsáveis no ciberespaço; a disseminação de alertas, orientações e boas práticas; a produção de conhecimento sobre o estado da cibersegurança em Portugal; e, por fim, exerce competências de regulação e supervisão dos setores de atividade económica (Decreto-Lei nº 136/2017, de 6 de novembro). Através do serviço CERT.PT[3] (Equipa de Resposta a Incidentes de Segurança Informática Nacional), o CNCS realiza uma efetiva coordenação nas respostas aos variados incidentes que afetam o ciberespaço, coordenando a resposta com as entidades da Administração Pública, operadores de infraestruturas críticas, operadores dos serviços essenciais e prestadores de serviços ao nível digital.

Em súmula, apesar do cibercrime ser um fenómeno que ocorre ao nível transnacional e que não conhece barreiras geográficas (Dias, 2012), é possível constatar que se têm procurado criar leis e instâncias de controlo exclusivamente dedicadas a este fenómeno que é a cibercriminalidade. Para além disso, como será visto de seguida, a pandemia de Covid-19 demonstrou precisamente a necessidade de regulação e repressão deste fenómeno.

1. Criado por um Despacho do Procurador-Geral da República, a 7 de dezembro de 2011.
2. Lei Orgânica do Gabinete Nacional de Segurança, Decreto-Lei nº3/2012, de 16 de janeiro.
3. *https://www.cncs.gov.pt/pt/certpt/*, acedido em maio de 2022.

Impacto da Covid-19 na cibercriminalidade

No ano de 2020, a Organização Mundial de Saúde declarou a doença do novo coronavírus como uma emergência de saúde pública internacional. Naturalmente, tal fenómeno causou mudanças radicais na vida da população mundial (Horgan *et al.*, 2020), levando à construção de um "novo normal" (Collier *et al.*, 2020). Perante as mudanças a que se assistiam, foram várias as instituições e organizações que alertaram para a possibilidade do aumento da prática de cibercrimes. Em Portugal, em 2020, o Gabinete do Cibercrime da Procuradoria-Geral da República registou um aumento gradual e persistente das queixas recebidas, sendo que as situações mais reportadas foram as fraudes através do *Mbway*, fraudes através do *e-mail* ou mensagens que continham *malware*, *phishing* e extorsão via *e-mail* (Gabinete do Cibercrime, 2020). Já no ano de 2021, o mesmo gabinete, registou mais denúncias por tentativas de *phishing*, fraude *online* e fraudes relacionadas com criptoativos. Para além destes dados, os relatórios demonstram que, independentemente do facto de o maior número de denúncias se registar durante os períodos de confinamento, há uma ampliação consistente e progressiva do cibercrime nos últimos anos (Gabinete do Cibercrime, 2021). Outra fonte importante de informação, o Relatório de Riscos e Conflitos de 2021, demonstra que as tentativas de *phishing*, *smishing*, infeção por *malware* e fraude por *Mbway*, foram as ameaças mais prevalentes durante o ano de 2020 (Observatório de Cibersegurança, 2021). Para além dos relatórios nacionais e internacionais que se têm desenvolvido para perceber qual o efeito da pandemia nos diversos cibercrimes, começam, também, a surgir investigações empíricas. No Reino Unido, Buil-Gil e colaboradores (2021), concluíram

que os cibercrimes mais prevalentes durante a pandemia de Covid-19 foram as fraudes relacionadas com as compras *online* e leilão e, ainda, o *hacking* de redes sociais e do *e-mail*. Nos Estados Unidos, Payne (2020) encontrou uma situação semelhante, na medida em que, nos primeiros três meses de 2020, as denúncias mais prevalentes estavam relacionadas com fraudes e, consistentemente, Lallie e colegas (2021), observaram que os ciberataques se tornaram mais frequentes durante a pandemia. Por fim, na investigação de Collier e colaboradores (2020) foi possível observar que os ataques de negação de serviço aumentaram de forma substancial após a adoção das medidas de confinamento.

Em suma, não se pode negar que a pandemia de Covid-19 teve um forte impacto na prevalência e incidência de alguns cibercrimes. Por esse motivo, e perante a ausência de informação sobre as tendências específicas do furto de identidade *online*, este estudo procura contribuir para o crescimento científico sobre esta ofensa e, para tal, será agora realizada uma revisão teórica acerca deste objeto de estudo.

Furto de Identidade *Online*

Definição

O furto de identidade, uma ofensa eminentemente tradicional, ganhou uma nova vida com a chegada a Internet, passando a ser cometida com maior frequência. O desenvolvimento tecnológico e da Internet permitiu o acesso a um elevado número de informações de carácter pessoal e financeiro (Smith, 2011), colocando em causa a ciberidentidade. Esta ciberidentidade tem sido definida como "o conjunto de elementos físicos, fisiológicos, psíquicos, económicos, culturais e sociais de um utilizador, constantes na Internet, que correspondem à identidade real da pessoa", ou seja, a ciberidentidade pode ser entendida como uma extensão da identidade pessoal na Internet e, qualquer ato atentatório do direito à ciberidentidade será, à partida, ilícito (Silva, 2014, pp. 16-17). Por sua vez, Roberts e colaboradores (2013) consideram que o termo identidade *online* representa o conjunto de informações pessoais que deveriam

ser intransmissíveis. Para Hille e colaboradores (2015) a identidade da pessoa é constituída pela informação pessoal e financeira combinadas. Posto isto, para Reyns (2013), o furto de identidade é um termo utilizado para categorizar vários crimes que envolvam o uso fraudulento de informações pessoais de um certo indivíduo para fins criminosos e, ainda, sem o seu consentimento. A esta ideia, Solove (2002) acrescenta que o ofensor obtém as informações pessoais e utiliza-as de várias maneiras fraudulentas para se fazer passar pela vítima ou para gerar informações falsas sobre a mesma. Esta aquisição da identidade pode ocorrer com recurso a diferentes meios e o uso da informação obtida pode ser utilizada para distintos fins, nomeadamente, para o cometimento de outros crimes (Newman & McNally, 2005) conforme será visto adiante.
Por fim, para Saunders e Zucker (1999), o furto de identidade *online* consiste no uso, de forma ilícita, dos dados identitários de outra pessoa (*e.g.*, nome, data de nascimento, número do cartão de crédito) para perpetrar fraudes económicas ou para se fazer passar pela vítima na Internet. Assim, tendo por base as diferentes definições apresentadas, é possível observar que há elementos que são consensuais em todas, desde logo, o facto das informações pessoais e financeiras serem utilizadas de forma fraudulenta e, ainda, a utilização dessas mesmas informações sem conhecimento e consentimento prévio da vítima.
Em Portugal, o furto de identidade teve, outrora, qualificação penal pela Lei nº 12/91, de 21 de maio, Lei da Identificação Civil e Criminal, mais precisamente no seu artigo 38º, postulava que:
"Quem induzir alguém em erro, atribuindo, falsamente, a si ou a terceiro, nome, estado ou qualidade que por lei produza efeitos jurídicos, para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem será punido com prisão até 2 anos ou multa até 100 dias, se o facto não constituir crime mais grave".

Anos mais tarde, esta lei foi revogada e substituída pela Lei nº 33/99, de 18 de maio, fazendo com que o mencionado artigo 38º deixasse de existir. Segundo Silva (2014), nos tempos que correm, perante a ausência de uma norma que regule este fenómeno, o uso da identidade alheia tem relevância em termos penais quando da mesma se procura obter algum benefício ilegítimo ou prejudicar a pessoa cuja identidade foi furtada. Assim, as situações em que a utilização da identidade de outrem parece ter relevância ocorrem (1) quando há cometimento do crime de uso de documento de identificação alheio (art. n.º 261º CP), (2) perante o cometimento do crime de falsificação de documentos (art. n.º 256º CP), (3) quando se comete o crime de falsificação de estado civil (art. n.º 248º CP), (4) na prática do crime de falsas declarações (art. n.º 348º-A CP) e, por fim, (5) quando através da usurpação, é causado um prejuízo económico a outra pessoa (*e.g.*, crime de burla, n.º 217º e seguintes, CP).
Para além da delimitação conceptual do conceito de furto de identidade *online*, importa aludir ao *modus operandi* através dos quais esta ofensa pode ser perpetrada e, para tal, descrevem-se de seguida, algumas das técnicas mais utilizadas pelos ciberofensores.

Modus operandi

Existem técnicas cada vez mais complexas que se vão aprimorando e facilitam a concretização do furto de identidade *online*, sendo evidente que as técnicas empregadas pelos ciberofensores se vão alterando à medida que a tecnologia evolui (Wang & Huang, 2011). Desta forma, o furto pode ser perpetrado com recurso ao *hacking*, ao envio de *software* malicioso, *phishing*, *smishing* e *pharming*.
Para simplificar a compreensão destas estratégias, definem-se, conceptualmente, cada uma delas.
Relativamente ao *hacking*, Antunes e Rodrigues (2018, p.105) definem-no como a "realização de atividades ilícitas de invasão e acesso ilegítimo a sistemas informáticos de instituições, empresas ou particulares, com vista à recolha de informações sobre o seu funcionamento".
No ordenamento jurídico português, o *hacking* é punido com o crime de "Acesso ilegítimo" na Lei do Cibercrime no seu artigo 6º. No fundo, o *hacking* traduz-se pelo acesso não autorizado a um dado sistema informático e pelo uso da manipulação, sabotagem ou espionagem (Singh, 2007), sendo que esta é uma técnica utilizada com sucesso por parte dos cibercriminosos na perpretação do furto de identidade *online* (Roberts *et al.*, 2013).
O furto da informação digital pode, também, ser consumado com recurso a *softwares* maliciosos. Estes são programas introduzidos nos sistemas informáticos de forma encoberta, tendo como objetivo comprometer a confidencialidade, integridade ou a disponibilidade dos dados da pessoa, das aplicações ou do sistema operativo.
Tendo em conta esta definição, pode-se concluir que é um conceito geral que engloba diferentes tipologias e formas de propagação do *software* malicioso, nomeadamente vírus no computador, cavalos de Troia[4] e *spyware*. Uma vez instalado no sistema informático da vítima, quer seja individual, quer seja coletiva, pode recorrer-se, por exemplo, a técnicas de *pharming* para furtar informações pessoais e/ou financeiras (Reyns, 2015).
Ao nível da engenharia social, o *phishing* é assistido pelo computador (Wall, 2007) e o objetivo é confundir os utilizadores da Internet para que forneçam informações confidenciais, nomeadamente, credenciais para aceder a determinado serviço (*e.g.*, banco *online*). Note-se que estas tentativas são efetuadas através do envio de *e-mails*, mensagens instantâneas ou serviços de *chat*, por remetentes aparentemente legítimos, combinadas com o redireccionamento para páginas *web* fraudulentas onde é feito o pedido das informações confidenciais (Reyns, 2015; Reyns & Henson, 2016; Antunes & Rodrigues, 2018). Por sua vez, o *smishing* é uma técnica similar ao *phishing* só que, neste caso, as mensagens são enviadas pelo telemóvel através de mensagens de texto (Williams, 2016).
Por norma, as tentativas de *phishing* são autonomizadas e realizadas em massa de forma a atingir o maior número de pessoas possível (Leukfeldt, 2014). Outra técnica utilizada para o cometimento do furto de identidade *online* é o *pharming* que, apesar de ser similar ao *phishing*, é mais complexa, devido ao facto de utilizar estratégias de *malware* para perpetrar o *phishing*.
Na prática, há uma apropriação ou usurpação do nome de domínio ou *URL* de uma página *web* legítima, redirecionando os utilizadores dessa mesma página para outra página fraudulenta na qual é solicitada a informação pessoal (Antunes & Rodrigues, 2018). Assim, num primeiro momento é instalado um vírus ou programa malicioso no dispositivo da vítima e, de seguida, no momento em que a vítima utiliza o *website*, os seus dados podem ser furtados, sendo difícil detetar que tal está a acontecer (Brody *et al.*, 2007).

Determinantes individuais do Furto de Identidade *Online*

Nos últimos anos, a Criminologia tem-se focado no estudo das dimensões individuais (e.g., características sociodemográficas) que podem influenciar a probabilidade de vitimação por furto de identidade *online*, nomeadamente o género, a idade e o estatuto socioeconómico. Assim sendo, serão agora apresentados os resultados de algumas investigações empíricas que têm sido realizadas acerca destes determinantes.
No que concerne ao género, Holt e Turner (2012), assim como Reyns (2013), chegaram à conclusão de que os homens têm mais probabilidade de serem vítimas de furto de identidade *online*. Na mesma linha, Alshalan (2006) descobriu que o género tem um efeito na vitimação *online*, sendo os homens mais vitimados do que as mulheres, avançando com a explicação de que os homens, nesta investigação, despendem mais tempo *online* do que as mulheres, o que, no ponto de vista deste investigador, pode aumentar o nível de exposição ao risco e, consequentemente, aumentar a vitimação dos homens.
Quanto à idade, no estudo de Williams (2016) e Harrell (2015), foram os mais jovens e os adultos de meia-idade a reportarem níveis mais elevados de vitimação por furto de identidade *online*. Contrariamente, na investigação desenvolvida por Reyns (2013) os indivíduos mais velhos apresentaram maior risco de vitimação por furto de identidade *online*. Mais recentemente, no estudo desenvolvido por Bunes e colaboradores (2020), observou-se que os indivíduos com idades compreendidas entre os 39 e os 73 anos demonstraram um maior risco para a maioria dos tipos de furto de identidade incluídos no estudo, o que, para os autores, pode ser o reflexo da capacidade económica e dos padrões de consumo dessa geração.
Relativamente ao estatuto socioeconómico, são várias as investigações, que observam que quem tem rendimentos mais altos apresenta maior risco de se tornar vítima (Reyns, 2013; Reyns & Henson, 2015; Bunes *et al.*, 2020). Segundo Reyns (2013), tal pode dever-se ao facto dos indivíduos com mais rendimentos fazerem mais compras *online* e, consequentemente, exporem mais os seus dados pessoais e financeiros, aumentando o risco de serem furtados. Na mesma linha, para Bunes e colaboradores (2020), indivíduos de estatutos socioeconómicos mais elevados e com níveis de educação mais altos apresentam maior poder aquisitivo e possuem mais dispositivos com ligação à Internet que transferem e armazenam informações, o que pode comprometer os dados de natureza pessoal e financeira. Já no estudo de Williams (2016) o estatuto social está associado à vitimação, pois indivíduos com estatutos baixos e altos apresentavam níveis de vitimação mais elevados, ao passo que, indivíduos de classe média, apresentavam baixas taxas de vitimação por furto de identidade *online*. Por fim, nas investigações de Leukfeldt e Yar (2016) ou van Wilsem (2013) nenhuma das variáveis individuais explicou a vitimação por furto de identidade *online*.

4. Programas maliciosos executáveis, desenvolvidos com o objetivo de entrar no sistema de uma rede ou sistema informático. Reside num sistema como sendo um ficheiro benigno, contudo quando o utilizador o abre é executado e desenvolve uma ação maliciosa (Hoque *et al.*, 2014).

Prevenção

Tendo em conta os impactos negativos provocados pelo furto de identidade *online* torna-se fundamental conhecer integralmente este fenómeno para que seja possível prevenir futuras vitimações de forma eficaz.

Na perspetiva de Dias (2012) a prevenção do cibercrime deve ser feita através da sensibilização, nomeadamente, através de seminários, campanhas públicas ou privadas, quer sejam dedicados à generalidade da população, quer sejam dedicados a um pequeno grupo de pessoas.

No decorrer destas dinâmicas de sensibilização, para a referida autora, deve alertar-se para os riscos e perigos característicos do ciberespaço e, ainda, deve procurar-se o ensino de técnicas de proteção *online*.

No que concerne ao furto de identidade *online*, embora não sejam implementadas muitas estratégias de prevenção, os investigadores têm feito um esforço para identificarem medidas eficazes. Um exemplo, é o contributo de Wang e Yuan (2006) sendo que estes autores dão primazia à educação. Assim sendo, acreditam que educar a população é uma estratégia eficaz para prevenir a exposição de dados pessoais e financeiros *online* e, como consequência, prevenir o furto de identidade. Com efeito, quanto mais os indivíduos tiverem consciência das ameaças e consequências desta ofensa, mais motivadas estarão na proteção dos seus dados. Na prática, os autores sugerem que as populações sejam educadas no sentido de não fornecer informações pessoais a estranhos; caso compre muito *online* poder criar um cartão bancário com menos quantias monetárias e utilizar somente para os pagamentos das compras; e, caso seja vítima desta ofensa, deve reportar logo a situação às autoridades e, ainda, às instituições bancárias de forma a minimizar as perdas (*e.g.*, cancelamento dos cartões). A estas medidas, Park e Vieraitis (2021) acrescentam que, quem foi vítima de furto de identidade, deve receber aulas educacionais que promovam a navegação segura na Internet. Complementarmente às medidas a adotar pelos cidadãos, também se podem identificar um conjunto de medidas de proteção que são conferidas pela própria tecnologia, ou seja, esta fornece recursos que tornam mais complexo o acesso a informações pessoais e financeiras, como por exemplo, através do uso de medidas biométricas. Esta biometria torna difícil, senão impossível, a personificação da identidade do outro (Wang & Yuan, 2006). No estudo de Carmel e Akila (2020), que procurou perceber se efetivamente o uso das medidas biométricas preveniam o furto de identidade *online*, concluiu-se que, perante a utilização daquelas medidas, o furto pode efetivamente ser prevenido.

Conclusão

Tendo em conta os elevados custos do cibercrime, as consequências danosas que o furto de identidade *online* provoca nas suas vítimas e, ainda, a tendência de aumento do cibercrime após a pandemia de Covid-19, é importante que se continue a investigar e a produzir conhecimento científico acerca dos fenómenos criminais que ocorrem no ciberespaço. Mais especificamente, deve ser produzido conhecimento acerca dos fatores de risco que contribuem para a vitimação *online* e devem ser desenvolvidas estratégias de prevenção eficazes que permitam que os utilizadores se sintam seguros quando navegam na Internet.

Referências

Alshalan, A. (2006). Cyber-crime fear and victimization: an analysis of a national survey. Mississippi: Mississippi State University.

Antunes, M., & Rodrigues, B. (2018). Introdução à Cibersegurança: a internet, os aspetos legais e a análise digital forense. Lisboa: FCA.

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, Pharming and Identity Theft. Academy of Accounting & Financial Studies Journal, 11(3).

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies, 23(sup1), S47-S59.

Bunes, D., DeLiema, M. & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. Preventive Medicine Reports, 17, 1-8.

Carmel, V. V., & Akila, D. (2020). A survey on biometric authentication systems in cloud to combat identity theft. J Crit Rev, 7(3), 540-547.

Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations. Scottish Institute for Policing Research.

Correia, A., (2021). Velhos crimes, novas ferramentas; novos crimes, novas ferramentas. In Guedes, I., e Gomes, A. (Eds.), Cibercriminalidade: novos desafios, ofensas e soluções (pp. 53-71). Pactor.

Dias, V. M. (2012). A problemática da investigação do cibercrime. Data Venia Revista Jurídica Digital, 1(1), 63-87.

Furnell, S. (2002). Cybercrime: Vandalizing the information society. Boston: Addison Wesley.

Grabosky, P. (2004). The global dimension of cybercrime. Global Crime, 6(1), 146-157.

Guedes, I., Moreira, S., e Cardoso, C. (2021). Cibercrime: conceptualização, desafios e perceções públicas. In Guedes, I., e Gomes, A. (Eds.), Cibercriminalidade: novos desafios, ofensas e soluções (pp. 3-23). Pactor.

Harrell, E. 2015. Victims of identity theft, 2014, Bureau of Justice Statistics, NCJ 248991.

Holt, T., & Turner, M. (2012). Examining risks and protective factors of on-line identity theft. Deviant Behavior, 308-323.

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications, 40, 307-324.

Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing, Journal of Criminal Psychology.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: a theoretical and empirical analysis. Deviant Behavior, 1-18.

Newman, G., & McNally, M. (2005). Identity theft literature review. Washington, DC: National Criminal Justice Reference Service.

Payne, J. L., Morgan, A., & Piquero, A. R. (2020). COVID-19 and social distancing measures in Queensland, Australia, are associated with short-term decreases in recorded violent crime. Journal of experimental criminology, 1-25.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. Journal of Research in Crime and Delinquency, 50(2), 216–238.

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. Journal of Financial Crime.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. International journal of offender therapy and comparative criminology, 60(10), 1119-1139.

Saunders, K. M., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. International Review of Law, Computers & Technology, 13(2), 183-192.

Silva, F. (2014). A usurpação da ciberidentidade. Dissertação de Mestrado. Escola de Direito. Universidade Católica do Porto.

Singh, P. (2007). Laws on Cyber Crimes. Jaipur: Book Enclave.

Smith, R. G. (2011). Identity theft and fraud. In Jewkes, Y., & Yar, M. (Eds.), Handbook of Internet Crime (pp. 273-301). Londres: Routledge.

Van Wilsem, J. (2013). "Bought it, but never got it." Assessing risk factors for online consumer fraud victimization. European Sociological Review, 29(2), 168-178.

Venâncio, P. D. (2011). Lei do Cibercrime: anotada e comentada. Coimbra Editora.

Wall, D. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. Police Practice and Research, 8(2), 183-205.

Wall, D. S., & Williams, M. L. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing. Policing and Society, 23(4), 409-412.

Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft. IEEE Security & Privacy, 4(2), 30-38.

Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft. IEEE Security & Privacy, 4(2), 30-38.

Williams, M. (2016). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. The British Journal of Criminology, 56(1), 21–48.

Yar, M. (2006). Cybercrime and Society. London: Sage Publications.

Relatórios consultados

Gabinete do Cibercrime (2020). Covid-19: Cibercrime em tempo de pandemia. Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/2020_06_01_cibercrime_em_tempo_de_pandemia.pdf (acedido em maio de 2022).

Gabinete do Cibercrime (2021). Cibercrime: denúncias recebidas 2021. Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime-25-01-2022.pdf (acedido em maio de 2022).

Observatório de Cibersegurança (2021). Relatório Cibersegurança em Portugal: Riscos e Conflitos 2021. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf (acedido em maio de 2022).

Leis consultadas

Código Penal;
Decreto-Lei n.º 81/ 2016, de 28 de novembro;
Decreto-Lei nº 136/2017, de 6 de novembro;
Lei n.º 109/2009, de 15 de setembro: Lei do Cibercrime;
Lei n.º 12/91, de 21 de maio: Lei da Identificação Civil e Criminal;
Lei nº 46/2018, de 13 de agosto.

04.

A TENDÊNCIA CRESCENTE NA *INTERNET* DOS DISCURSOS DE ÓDIO E DE INCITAMENTO AO ÓDIO E À DISCRIMINAÇÃO

INÊS PEREIRA DE MELO
E CARLOS PINTO DE ABREU

Com a evolução das tecnologias cada vez mais a *internet* se tornou num meio, não só de comunicação, mas de difusão de todo o tipo de discursos e conteúdos. Se, por um lado, a facilidade de comunicação traz inúmeras vantagens, por outro, tem-se verificado um aumento da prática de crimes perpetrados por este meio, mais a mais devido ao anonimato que as plataformas *online* conferem aos seus utilizadores.

Entre eles, cada vez mais se assiste a discursos de ódio e de incitamento ao ódio e à discriminação. Um exemplo contemporâneo da prática deste tipo de discurso reside na retórica difamatória e ultrajante utilizada pela Rússia para se referir à Ucrânia no contexto actual de guerra entre aqueles dois países.

Discursos de ódio sobre a comunidade LGBT também são cada vez mais frequentes num mundo que se quer cada vez mais tolerante e multicultural. Também a pandemia de Covid-19 que atravessámos fez aumentar exponencialmente os discursos de ódio espalhados um pouco por toda a internet e sempre escondidos atrás do anonimato conferido por um ecrã.

No Direito Europeu o discurso de incitação ao ódio define-se como a incitação pública à violência ou ao ódio em virtude de certas características, tais como a etnia, religião, nacionalidade ou cor. Nesta senda, o Conselho da Europa definiu o discurso de ódio como "*qualquer expressão que espalha, incita, promove ou justifica ódio racial, xenofobia, anti-semitismo ou qualquer outra forma de intolerância. Incluindo: intolerância causada por nacionalismo agressivo e etnocentrismo, discriminação e hostilidade contra minorias, migrantes e pessoas de origem estrangeira*".

Com o aumento dos discursos de incitação ao ódio têm as instituições europeias encetado diversos esforços no sentido de combater estas práticas tão nocivas para a comunidade. Há que destacar neste domínio a Decisão-Quadro 2008/913/JAI do Conselho, de 28 de Novembro de 2008[1], relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia que impôs aos Estados-Membros a tomada das medidas necessárias para punir "a incitação pública à violência ou ao ódio contra um grupo de pessoas ou os seus membros, definido por referência à raça, cor, religião, ascendência ou origem nacional ou étnica" (alínea a) do n.º 1 do artigo 1.º) e a apologia, negação ou banalização grosseira públicas de crimes de genocídio, crimes contra a Humanidade e de determinados crimes de guerra, cometidos contra um grupo de pessoas ou seus membros, definido por referência à raça, cor, religião, ascendência ou origem nacional ou étnica, quando esses comportamentos forem de natureza a incitar a violência ou o ódio contra esse grupo ou os seus membros (alíneas c) e d) do n.º 1 do artigo 1.º).

Também o Código de Conduta para a luta contra os discursos ilegais de incitação ao ódio em linha[2], promovido pela Comissão Europeia, pretende

1. Disponível em *https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008F0913*
2. Disponível em *https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_pt*

combater as supra referidas práticas discriminatórias. Este Código de Conduta foi, aliás, subscrito pelas redes sociais mais utilizadas no mundo e onde mais se verifica a existência deste tipo de discursos de ódio e discriminação, como o *Facebook*, *Twitter*, *Microsoft*, *Instagram*, *Google*, *Youtube*, *Snapchat*, *Dailymotion*, *Jeuxvideo.com* e *TikTok*, o que se mostra um grande passo no combate à prática deste tipo de crimes. A Decisão-Quadro 2008/913/JAI supra referida teve também, naturalmente, impacto nos ordenamentos jurídicos internos dos Estados Membros, estando, assim, em Portugal este tipo de crime descrito no n.º 2 do artigo 240.º do Código Penal como o acto de, através de meio de divulgação pública, provocar ou incitar a prática de actos de violência, difamação, injúria, ou ameaça a pessoas ou grupos de pessoas, nomeadamente em razão da sua etnia, nacionalidade, religião, género, orientação sexual ou deficiência, sendo punível, em abstracto, com pena de prisão de um a oito anos.

Estão excluídas do tipo de crime de discriminação e incitamento ao ódio as condutas que ocorram em privado, exigindo o nosso Código Penal que a conduta punível se realize em espaço de carácter público e se destine a ser divulgada, o que poderá suceder através de discursos orais ou publicados em sites públicos e passíveis de ser partilhados, de cartazes ou panfletos, de meios de comunicação social, de grafitis em espaços abertos, etc. A reforçar a ideia da exclusão deste tipo de crime das condutas que ocorram em privado, note-se que, ainda que a conduta seja punível quando partilhada em site da internet de livre acesso ao público, o mesmo já não sucede quando a partilha acontece em páginas de acesso restrito ou grupos fechados. Daqui decorre a concreta intenção do legislador de punir estes discursos apenas quando sejam públicos e destinados à divulgação.

Ainda no panorama nacional, também a Constituição da República Portuguesa consagra no n.º 2 do seu artigo 13.º que "ninguém pode ser privilegiado, beneficiado, prejudicado, privado de qualquer direito ou isento de qualquer dever em razão de ascendência, sexo, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual".

Não obstante este ser um tema cada vez mais actual e que gera uma preocupação crescente, tanto a nível dos Estados Membros, como a nível das Organizações Comunitárias e Internacionais, muito se fala na sua possível colisão com o direito à liberdade de expressão.

Nesta senda é de realçar, em primeiro lugar, o n.º 2 do artigo 20.º do Pacto Internacional sobre os Direitos Civis e Políticos[3] que consagra que "toda a apologia ao ódio nacional, racial ou religioso que constitua incitação à discriminação, à hostilidade ou à violência estará proibida por lei" e que tem servido de justificação à restrição do direito à liberdade de expressão.

Por outro lado, há que atentar no artigo 10.º da Convenção Europeia dos Direitos do Homem[4] que consagra o direito à liberdade de expressão e de opinião. O Tribunal Europeu dos Direitos Humanos tem entendido, no entanto, que este não é um direito absoluto, tendo afirmado em vários casos que "tolerância e respeito pela igual dignidade de todos os seres humanos constituem um dos fundamentos de uma sociedade democrática e plural. Sendo assim, por questão de princípio, considera-se necessário que certas sociedades democráticas penalizem e inclusive proíbam todas as formas de expressão que espalham, incitam, promovem ou justificam ódio baseado em intolerância (incluindo intolerância religiosa)". Por outro lado, tem o mesmo Tribunal Europeu invocado o artigo 17.º da Convenção Europeia dos Direitos do Homem, que consagra a proibição do abuso de direito, para considerar inadmissíveis as queixas por restrições à liberdade de expressão por entender que, nos casos concretos, o resultado do exercício do direito à liberdade de expressão atentava de tal forma contra os valores espelhados na Convenção que jamais poderia reclamar a sua protecção.

No entanto, situações existem sobre as quais as Nações Unidas consideram ilegítimas as restrições à liberdade de expressão por não pressuporem o incitamento à discriminação, mas o Tribunal Europeu dos Direitos do Homem tem vindo a considerar tratarem-se, ainda assim, de válidas restrições ao direito à liberdade de expressão. Um exemplo muito claro desta situação é o do negacionismo do Holocausto que tem vindo a ser punido pelos tribunais internos alemães com a validação do Tribunal Europeu dos Direitos do Homem.

1. Disponível em https://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf
4. Disponível em https://www.echr.coe.int/documents/convention_por.pdf
5. Disponível em https://www.ohchr.org/en/freedom-of-expression

Foi exactamente para ultrapassar as dúvidas sobre em que situações o discurso atinge o limiar do incitamento à discriminação ou em que situações o direito à liberdade de expressão está a ser ilegitimamente restringido que a ONU desenvolveu o Plano de Acção de Rabat[5], que se traduziu em critérios para avaliar o contexto, o autor do discurso, a sua intenção, o conteúdo do discurso, a extensão da difusão do discurso e a probabilidade de vir a causar danos.

Não obstante a União Europeia adoptar constantes mecanismos para combater o discurso de ódio e fazer diversas solicitações aos Estados-Membros no sentido de desenvolverem planos de acção nacionais contra o racismo nas suas diversas formas e concretamente sobre o incitamento ao ódio e à discriminação, entendemos ainda existir um grande percurso a percorrer, quer através de mecanismos judiciais, quer no que à educação das crianças, adolescentes e jovens diz respeito. Munindo-os de mecanismos que lhes permitam identificar e reivindicar os direitos humanos, podem aqueles reconhecer os seus próprios estereótipos e preconceitos, bem como os de terceiros, e contribuírem activamente para a mudança deste paradigma. No entanto, e no que ao panorama nacional diz respeito, cabe referir que existem poucos registos de denúncias deste tipo de crimes, seja por falta de confiança no sistema judiciário, porque os cidadãos alvo destas práticas se encontram indocumentados e, por isso, têm receio de recorrer à justiça, seja por uma questão de vergonha ou até mesmo de represálias ou por não saberem a quem e onde se devem dirigir para apresentar queixa ou denúncia de actos criminosos.

Ao facto de na grande maioria das vezes as vítimas não denunciarem este tipo de práticas acresce a circunstância de não serem raras as vezes em que queixas que denunciam crimes de ódio são menosprezadas à partida ou arquivadas à chegada, muitas vezes pelo simples motivo de serem apresentadas contra desconhecidos, sem que sejam feitas as diligências necessárias para averiguar a identidade do autor do mesmo, nomeadamente oficiando os servidores dos sites e redes sociais onde foram praticadas as condutas em causa para indicarem o IP do utilizador autor do crime. Prova disso é o facto de indicarem as estatísticas que, entre 2016 e 2020, terem sido abertos 161 inquéritos para investigação da prática do crime de discriminação e incitamento ao ódio e à violência e apenas 3 terem dado origem a acusação pelo Ministério Público.

Por este motivo, entendemos que antes de se procederem a alterações legislativas - como pretendia o Projecto de Lei n.º 922/XIV/2.ª com vista à alteração do artigo 240.º do Código Penal -, será necessário avaliar se os instrumentos normativos actualmente em vigor têm aplicação prática e munir os cidadãos de mecanismos que lhes permitam identificar, denunciar e ver efectivamente processados crimes de discriminação e incitamento ao ódio.

05.

A DEFESA DAS VÍTIMAS EXIGE INFORMAÇÃO E CLARA ATRIBUIÇÃO DE RESPONSABILIDADES

MANUEL BARROS

A defesa das vítimas exige informação e clara atribuição de responsabilidades

Responsabilidade e a responsabilização na decorrência de um incidente de segurança que afecte um sistema de informação detido e utilizado por uma pessoa individual ou por uma entidade colectiva.

No respeitante à responsabilidade problematizo obrigações da entidade cujo sistema foi afectado, enquanto quanto à responsabilização a perspectiva que adopto é a de quais são as possibilidades de terceiras partes poderem reclamar junto daquela entidade a defesa dos seus interesses, no caso terem sido lesadas nos seus legítimos direitos.

Importa abordar não só a pessoa detentora do sistema de informação que foi objecto do incidente de segurança, bem como a Autoridade ou Autoridades a quem a ocorrência é, por imperativo legal, reportada. E assegurar tal reporte aos lesados.

Quanto ao sistema de informação, necessariamente interligado a outros sistemas de informação por conexão à rede, refiro-me a equipamentos computorizados ou, dito de uma outra forma, dotados de microprocessador, de memória, de canais de ligação externa, de programas, incluindo um sistema operativo, os quais no seu conjunto controlam e determinam as funcionalidades e o desempenho do equipamento, mediante o controlo e gestão da informação processada, arquivada ou transmitida.

Nestes equipamentos incluo, entre outros, o tradicional computador de secretária, o computador móvel, o sistema de computadores de uma empresa ou de um organismo público, o telemóvel, o frigorífico inteligente, o equipamento robotizado, o automóvel dito inteligente por ter capacidade de condução autónoma, o *drone*, etc.

Julgo não haver qualquer dúvida de que estes sistemas de informação podem ser objecto de um incidente de segurança, incluindo um ciberataque, o qual pode constituir em determinadas circunstâncias um incidente de reporte obrigatório à Autoridade ou Autoridades Competentes ou até instrumento ou alvo de um cibercrime, caso em que estaremos perante a existência de cibervítimas.

Aproximando esta problemática numa perspectiva de uma ameaça e de um alvo é típico conduzir a análise subsequente à discussão de qual é o agente da ameaça, de qual é o vector de ataque, de qual é a superfície de exposição, de como pode ser feita a obtenção da evidência do ataque ou a atribuição ao atacante ou a concretização da prova. Para o caso que vos coloco não é essa a discussão que me interessa. O que me traz à liça decorre de saber ou de ter a capacidade de identificar questões que permitam clarificar quais devem ser as obrigações e a responsabilização de detentores de sistemas de informação afectados por incidentes de segurança perante terceiros e, sucessivamente, das Autoridades Competentes que, por aplicação da legislação, foram objecto de comunicação, reporte ou queixa, perante esses terceiros e o público em geral.

A informação estatística relativa à evolução registada, bem como às perspectivas futuras no respeitante a incidentes de cibersegurança, incluindo de cibercrime, que as Autoridades, nacionais e internacionais, bem como outras fontes, usualmente consideradas como credíveis, nos fazem chegar, são claras em termos do aumento crescente do número de ocorrências e da diversificação e sofisticação das suas causas.

Em conformidade verificamos ser cada vez maior o número de pessoas, individuais ou coletivas, cujo sistema foi afectado e, inclusivamente, pessoas cujos sistemas foram mais que uma vez afectados. Tudo com impacto, muitas vezes severo, para terceiros.

Sem prejuízo da necessidade do reforço contínuo do esforço de sensibilização e de preparação de e para o fenómeno ou fenómenos subjacentes pelas pessoas

afectadas e pelas Autoridades, julgo que importa sobretudo perceber o que pode e deve ser feito de forma a minimizar os impactos perante terceiros, incluindo o público em geral.
Para que tal seja possível é fundamental que a legislação, nomeadamente, ao fixar obrigações de adopção de medidas de segurança adequadas ao risco e de reporte às pessoas cujos sistemas foram afectados, bem como a condução das acções pelas Autoridades Competentes permitam estabelecer as condições de base para a criação e o desenvolvimento de um sistema claro e transparente de atribuição de responsabilidades. E de um sistema de informação obrigatória adequado a dar a conhecer eventos para o exercício de direitos daí decorrentes. Neste sentido importa recuperar algum histórico relevante.
Em 1992, os países membros da Organização para a Cooperação e o Desenvolvimento Económico (OCDE) adoptam as "Linhas Orientadoras para a Segurança dos Sistemas de Informação" substituídas em 2002, na sequência do ataque de 11 de Setembro de 2001 às Torres Gémeas de Nova Iorque, pelas "Linhas Orientadoras para a Segurança dos Sistemas e das Redes de Informação sob o lema "Para uma Cultura de Segurança", por sua vez e finalmente substituídas em 2015 pela Recomendação sobre a Gestão do Risco Digital para a Prosperidade Económica e Social, em vigor.

Cada um dos documentos referenciados apresenta um conjunto de princípios e guidelines que constituem o que, para os efeitos pretendidos, os membros da OCDE entenderam ser de recomendar que os países membros, mas não só, adoptem.

No respeitante à responsabilidade e à responsabilização existe em cada um deles um princípio específico que trata desta matéria, o qual se transcreve de seguida:

1992
ACCOUNTABILITY PRINCIPLE
The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2002
RESPONSIBILITY
All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

2015
RESPONSIBILITY
All stakeholders should take responsibility for the management of digital security risk.

They should act responsibly and be accountable, based on their roles, the context and their ability to act, for the management of digital security risk and for taking into account the potential impact of their decisions on others. They should recognise that a certain level of digital security risk has to be accepted to achieve economic and social objectives.

Similarmente, na 57.ª Assembleia Geral das Nações Unidas, em 2002, é adoptada a Resolução 57/239 – Criação de uma Cultura Global de Cibersegurança, a qual considera que para tal é requisito que todos os participantes adoptem um conjunto de nove elementos, entre eles, os seguintes:

RESPONSIBILITY
Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment.

A legislação estabelece genericamente, no âmbito de aplicação respectivo, que as pessoas detentoras dos sistemas: "devem adoptar as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam".

Verificando-se que os incidentes de segurança ocorrem e que, em consequência, há terceiros afectados é, a meu ver, por estes, legítimo questionar se a entidade detentora do sistema, embora tenha procedido ao reporte do incidente de segurança às Autoridades Competentes em conformidade com o disposto na legislação aplicável, terá eventualmente:

× procedido de forma gravemente negligente ou simplesmente descuidada à gestão do controlo de acessos ao sistema de que resultou a perda de controlo da segurança da informação pessoal à sua guarda,

× não procedido ou procedido tardiamente às actualizações aos programas residentes no sistema, incluindo aos componentes que asseguram a gestão da segurança da informação, não tendo seguido as orientações dos fabricantes de que resultou a ocorrência de um incidente de segurança por não ter sido eliminada uma vulnerabilidade a uma ameaça conhecida cuja solução estava disponível,

× procedido à aceitação de programas de fonte não verificada que alteraram drasticamente as funcionalidades do sistema de que resultou que o sistema autónomo passou a ter um comportamento fora do previsto,

× não procedido a uma completa e cuidada revisão a um incidente de segurança anteriormente ocorrido, não tendo por isso identificado e adoptado as medidas de segurança que impedissem a sua repetição.

Na sequência da recepção e tratamento dos reportes de incidentes de segurança, parece-me, adicionalmente, que a acção das Autoridades Competentes é fundamental para que a responsabilidade e a responsabilização das entidades detentoras de sistemas de informação, afectados por incidentes de segurança, perante terceiros sejam plenamente assumidas. E para isso é necessário que as vítimas sejam informadas.

Parece-me que deveria ser debatido qual o tipo de informação que as entidades cujos sistemas foram afectados e as Autoridades devem disponibilizar ao público em geral e, em particular, às vítimas de incidentes, para que seja melhorada a transparência quanto a uma adopção adequada e proporcional de medidas para gestão dos riscos que afaste ou que, em contrário, concretize, se assim for o caso, um comportamento negligente. E possa permitir o exercício de direitos de reparação ou de indemnização.

Parece-me, finalmente, que uma adopção plena do princípio da responsabilidade é necessária para que, em caso de cibercrime, se possam identificar quais são as vítimas e desenvolver as medidas de protecção adequadas a cada situação em específico.

Por último, em face da evolução patente do aumento da autonomização dos sistemas, da adopção em larga escala de soluções de inteligência artificial, da melhoria da conectividade e das capacidades de processamento e de armazenamento de informação dos sistemas, julgo ser de recomendar que haja um esforço de todos os participantes para que seja pronta, clara e transparente a informação a disponibilizar e para que possa ser, se for o caso, feita a atribuição de responsabilidades, nos termos da legislação aplicável e, em termos pedagógicos e de prevenção, e a concretização de qual é a acção, a avaliação e as recomendações das Autoridades Competentes, neste âmbito, e, se for o caso, também, qual a sua responsabilidade.

06.

INTERVIR NO DIGITAL: A LINHA *INTERNET* SEGURA

CAROLINA ESTEVES SOARES
E RICARDO ESTRELA

Segundo dados de um estudo publicado pela Pordata, em Portugal, em 2021, 99,7% dos jovens entre os 16 e os 24 anos, 98,4% das pessoas entre os 25 e 34 anos e 96,4% dos 35 aos 44 anos são utilizadores da internet. Existiam no mesmo ano em Portugal 14.390.340 telemóveis (Pordata, 2022).
A grande parte destes utilizadores não está sensibilizada e ainda menos alerta para os riscos que decorrem dessa utilização.
Assim, e sem pretender advogar contra a utilização da internet, consideramos urgente reforçar e investir no conhecimento e sensibilização por forma a proteger os seus muitos utilizadores. Nomeadamente avaliar os seus perfis digitais, reforçar a segurança e privacidade nos seus diversos dispositivos e nos inúmeros perfis detidos em lojas *online*, redes sociais, nuvens etc.
Como proposta a prazo, consideramos também urgente refletir, enquanto comunidade, sobre a forma como se pensa o papel da tecnologia e a sua utilização. Só através do reforço da literacia digital nos poderemos proteger e tornar a navegação na internet mais segura e compreender as consequências da sua utilização de forma mais consciente.

O papel e impacto da tecnologia no nosso quotidiano

Como já mencionamos, as estatísticas reveladas pela Pordata indicam que em 2021 existiam em Portugal 14.390.340 telemóveis, face aos 6.584 registados em 1990. Mostraram também que a maioria da população está conectada à internet. Dados publicados pela Eurostat confirmam esta realidade. Em 2021, quase nove em cada dez (89%) indivíduos na UE, com idades compreendidas entre os 16 e 74 anos, utilizaram a Internet (pelo menos uma vez nos três meses que antecederam a data do inquérito). Esta percentagem foi de pelo menos 95% em seis países, com os valores mais elevados registados na Dinamarca, Irlanda e Luxemburgo (todos 99%), seguidos pela Finlândia e Suécia (ambos 97%). A percentagem mais baixa foi registada na Bulgária (75%) (Eurostat, 2022).
Também em 2021, um outro estudo convocou pessoas de todo o mundo a contribuir com as suas perspetivas sobre a internet. A iniciativa contou com a participação de decisores políticos, académicos, bem como outros atores relevantes.
Neste estudo, foi destacado o fácil e rápido acesso, o volume de informação, acesso facilitado a serviços e atividades culturais e de lazer, a possibilidade de contacto à distância, oportunidades de emprego e negócio e a possibilidade de teletrabalho (Delicado, Estevens, Rowland, Truninger & Salgado, 2021).
O papel da tecnologia na habilitação e no envolvimento é evidente. Há uma ação à distância, feita sem contacto físico, requerendo menos tempo e esforço, automatizada em muitos aspetos.
O excesso de informação, notícias falsas e o isolamento são, em contraste, as desvantagens mais apontadas.
Este isolamento sendo um efeito do uso excessivo destas tecnologias (Delicado *et al.*, 2021). Já o impacto das redes sociais e destas na qualidade da democracia os resultados são ambíguos.
Esta ambiguidade está patente em muitas vertentes da tecnologia: esfera pública versos a esfera privada; acesso facilitado a informação versos a maior probabilidade dessa informação ser falsa ou enganadora; papel facilitador da internet no ativismo, na luta por causas sociais e de direitos humanos e a amplificação do espírito coletivo e de entreajuda versos a propagação do discurso de ódio. Uma luta constante entre a liberdade de expressão e a imposição de limites.
A fusão entre a nossa dimensão digital e física é mais evidente e está cada vez mais esbatida. Este processo de hibridização, de esbatimento das fronteiras entre o *online* e *offline*, o mundo real e o digital é visível "por exemplo, nas perceções sobre o que é uma identidade digital,

uma construção que incorpora informações e rastos deixados pelos indivíduos de forma voluntária e involuntária nas plataformas digitais que utiliza" (Delicado *et al.*, 2021, p.2).

*

É neste seguimento que nos pareceu pertinente explorar e refletir juntamente com o leitor conceitos como o de corpo digital, sombra digital, ou o de identidade digital, este último talvez mais conhecido.
A Eurostat revelou algumas estatísticas relativas à privacidade e proteção da identidade pessoal nos cidadãos dos Estados membros da União Europeia. E neste campo observaram algumas disparidades na forma como os utilizadores da Internet geriram o acesso às suas informações pessoais na Internet em 2021. Pouco menos de três quartos (73%) dos utilizadores da Internet da UE geriram o acesso à informação pessoal através da Internet, uma percentagem que variou entre apenas 56% na Roménia e 91% na Finlândia e nos Países Baixos. Os utilizadores da Internet da UE forneceram algum tipo de informação pessoal *online*, muitos deles empreendendo diferentes ações para controlar o acesso a esta informação pessoal na Internet. Apenas dois quintos (40%) limitaram o acesso ao seu perfil ou conteúdo em sítios de redes sociais (Eurostat, 2022).
Assim, ao leitor pedimos agora que reflita: quantas aplicações tem no seu *smartphone*? Estas aplicações têm a localização ativa? Autorizou o acesso aos seus contactos, câmara e microfone? Quantos perfis tem em redes sociais? Esses perfis estão públicos? Que informações privadas disponibiliza nestas redes? Quantas fotografias publica semanalmente? Essas fotografias são sempre suas ou também protagonizam os seus amigos, filhos, colegas? De onde consome a maioria da informação de que dispõe?
À medida que vamos criando os nossos perfis nas redes sociais, plataformas de emprego, fazendo *upload* de documentos, fotografias e vídeos ou fazendo comentários a notícias. À medida que vamos aceitando que as aplicações nos nossos telemóveis sigam a nossa localização, sigam as nossas pesquisas nos motores de busca e façam recomendações de produtos. À medida que aumentamos a nossa pegada digital estamos simultaneamente a criar um "eu" digital. Uma versão do nosso corpo ou da nossa identidade no mundo digital. Todos os dias criamos e deixamos mais pedaços de informação, que são armazenados, recolhidos e analisados. Estes vestígios/pegadas que deixamos podem dar a outros uma visão alargada da nossa vida. Fornecemos no mundo *online* mais informações do que estaríamos dispostos a partilhar na rua ou com colegas de trabalho. Estas versões podem também estar totalmente erradas, podem ser copiadas, mas já aqui voltamos.
Esta identidade digital pode ser observada de posicionamentos diferentes:
- A identidade que as plataformas, como a *Google*, criam. A confluência da nossa atividade *online* fornece dados constantes e com essa informação as empresas criam um perfil *online* que as norteia na adaptação dos seus produtos e que partilham com as agências publicitárias que as sustentam. Aqui o perfil é construído por outros e o papel do indivíduo nesta identidade digital é diminuto;
- A identidade que os próprios criam sobretudo através da forma como a pessoa se apresenta na internet, podendo espelhar a realidade dos próprios *offline*, ainda que não necessariamente.
- E finalmente, uma identidade digital que converge as construções do indivíduo e as das plataformas que este utiliza. "Essa identidade é algo construído a partir dos rastos deixados pelos indivíduos de forma voluntária e involuntária na internet, nas redes sociais, mas não só.
Neste caso os participantes falam em identidade construída com base nos dados que decidimos partilhar e que as plataformas nos solicitam e agregam" (Delicado, p.10).
A existência desta identidade digital já é reconhecida nas políticas da UE. O programa "Digital Identity for All Europeans" procura responder às necessidades dos cidadãos e, ao mesmo tempo, permitir um maior controlo dos mesmos às suas informações pessoais.

"We want a set of rules that puts people at the centre. Algorithms must not be a black box and there must be clear rules if something goes wrong. The Commission will propose a law to this effect next year. This includes control over our personal data which still have far too rarely today. Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality" (Leyen, 2020).

E se muitos de nós concorda ou reconhece pelo menos a existência de uma destas identidades, continua a existir uma perceção geral de que o mundo *online* está distante e que há uma fronteira evidente que o separa do mundo "real" ou físico. Uma consequência desta perceção é a não aplicação *online* das mesmas defesas e estratégias de segurança que aplicamos no nosso quotidiano "físico". A outra é considerarmos os crimes e ofensas que acontecem *online* menos gravosos do que aqueles que se passam na rua. Considerar a existência de violência em práticas virtuais acarreta muitas dificuldades, nomeadamente conceptuais. Porém, a literatura e discussões mais recentes parecem apontar para pertinência da utilização deste conceito em crimes que ocorrem *online* (Valente, Neris, Ruiz & Bulgarelli, 2016).

Qual é o trabalho da Linha Internet Segura?

Com este enquadramento explicar o trabalho e pertinência da Linha Internet Segura fica mais facilitado.
A Linha Internet Segura foi criada em 2019, fazendo parte de um consórcio coordenado pelo CNCS – Centro Nacional de Cibersegurança, que também envolve a FCT – Fundação para a Ciência e a Tecnologia, DGE – Direção Geral da Educação do Ministério da Educação, IPDJ - Instituto Português do Desporto e Juventude, a Fundação Altice e a Microsoft Portugal.
A Linha Internet Segura, é um apoio específico do Sistema Integrado de Apoio à Distância (SIAD) da APAV, que assegura o apoio anónimo e confidencial, relativo ao uso das tecnologias *online*, cobrindo todos os assuntos relativos à utilização das mesmas. A integração da Linha Internet Segura no SIAD assegura ainda uma resposta articulada com os serviços de proximidade da APAV.
Desde logo o trabalho desenvolvido dividiu-se maioritariamente em 3 dimensões: a *helpline*; a *hotline* e as ações de prevenção e sensibilização.
Helpline: As/Os utentes (vítimas ou denunciantes) podem chegar até nós por vias diferentes. Pela linha telefónica (800 219 090), pelo email linhainternetsegura@apav.pt ou pelo formulário disponível no nosso site. Ao recebermos esse formulário entramos depois em contacto com a/o utente pedindo mais informações de forma a traçar uma estratégia de segurança e tratarmos das diligências necessárias.
Se se tratar de casos em que foi publicado conteúdo, nomeadamente imagens íntimas, sem consentimento da pessoa numa rede social, agimos no sentido de garantir que a prova digital fica assegurada ao mesmo tempo que solicitamos a remoção do dito conteúdo. Para isso, temos feito o esforço de articulação com várias plataformas para tornar esse processo mais célere.
Desde a sua criação, a Linha Internet Segura tem feito um esforço para que o seu trabalho seja feito em rede, estabelecendo parcerias estratégicas com diferentes plataformas digitais, destacando-se aqui a mais recente parceria da APAV com duas associações sem fins lucrativos Inglesas: a *Revenge Porn Helpline* e *SWGfl*. Esta parceria estabelece a APAV como ponto de contacto do programa *"Stop Non Consensual Intimate Image Abuse"*.
Este programa permite às vítimas de divulgação não consensual de imagens e vídeos íntimos impedirem que este conteúdo seja partilhado nas plataformas *Facebook* e *Instagram*. Trata-se de uma ferramenta inovadora que permite às vítimas deste tipo de violência minimizarem a exposição da sua imagem, sem dependerem de terceiros.
A Linha Internet Segura sendo uma Linha de Apoio integrada na Associação Portuguesa de Apoio à Vítima (APAV) dispõe de Técnicas/os de Apoio à Vítima especializadas/os no apoio a pessoas que foram ou são vítimas de crimes praticados fazendo uso da Internet e estão disponíveis para ouvir, garantindo a confidencialidade e o respeito pela autonomia das/os suas/seus utentes prestando apoio psicológico, jurídico e social para lidar com as situações de vitimação. Nesse sentido, muitas/os utentes são depois encaminhadas/os para os Gabinetes de Apoio à Vítima da APAV mais próximos.
Hotline: A outra vertente de atuação da Linha Internet Segura é a sua vertente *Hotline*. A APAV é membro da International Association of Internet Hotlines (INHOPE), associação que agrega um conjunto de 50 *hotlines* espalhadas por 46 países em diferentes continentes, cuja missão é a remoção de conteúdo de abuso sexual de menores *online*. Algumas *Hotlines* como é o caso da *Hotline* Portuguesa têm um foco de atuação mais abrangente recebendo também denúncias de outro tipo de conteúdo ilegal como conteúdo *online* que faça apologia à discriminação e à violência.
A Linha Internet Segura já tem estabelecido com a Polícia Judiciária um protocolo de referenciação de situações relativas a abuso sexual de menores *online*. Este protocolo permite encaminhar situações que configurem crimes sexuais contra menores *online* de uma forma célere para a Unidade de Cibercrime e Criminalidade Informática da Polícia Judiciária, bem como permite a esta última referenciar vítimas para as estruturas de Apoio da APAV.
Prevenção e sensibilização: Finalmente, estes dois trabalhos convergem nesta terceira dimensão. Há uma necessidade constante de formação, atualização e investigação por parte das/os técnicas/os da Linha. Este trabalho e a experiência adquirida confere-nos uma posição privilegiada para prepararmos ações de sensibilização ou de formação junto da comunidade para uma utilização mais segura da Internet.

*

Em 2021, a Linha Internet Segura verificou um aumento nos contactos, denunciando formas de violência associadas à ameaça de partilha de conteúdo íntimo (Estatísticas Linha Internet Segura, 2021). Acrescido também do contínuo aumento da denúncia de conteúdos de abuso sexual de menores e de discurso de ódio *online*, quer a nível nacional quer mundial.
No que concerne ao material de abuso sexual de menores *online*, "a maior parte continua a ser o material autoproduzido por parte de crianças

e jovens, que muitas vezes é conseguido através de manipulação perpetrada por adultos", sendo depois esse conteúdo comercializado. Esta preocupação é partilhada também pela Europol, no seu mais recente relatório sobre Criminalidade *Online*.
A *sextortion*, a burla e o furto de identidade foram os crimes e outras formas de violência mais registados na dimensão *Helpline* em 2021, verificando-se uma subida acentuada das duas primeiras. Na dimensão *Hotline*, em 2021, houve um crescimento no número de registos, em 54%, mantendo-se o predomínio dos conteúdos de abuso sexual de menores. O número de imagens e conteúdos alojados em Portugal identificados a este respeito também aumentou (Relatório Cibersegurança em Portugal - Riscos e Conflitos, 2022).
Cada vítima/sobrevivente é impactada de alguma forma pela sua experiência. Esses impactos podem incluir danos significativos para a sua saúde física e mental, estatuto social e oportunidades económicas, e, em alguns casos, levam à morte. O impacto é dividido em cinco categorias: psicológico (por exemplo, vergonha, depressão ou medo); físico (por exemplo, automutilação, agressão ou prisão); funcional (por exemplo, mudar uma rota ou derrubar um perfil); económico (por exemplo, extorsão ou perda de rendimento ou oportunidades educacionais); e social (por exemplo, excluídos pela família, amigos ou colegas de trabalho).
Com isto em vista, tentamos garantir o suporte técnico, porém, o enfoque está em garantir que a vítima se sente apoiada e que tem um suporte. Procuramos, através do trabalho em rede, ser esse apoio, mesmo que nem sempre seja possível alcançar o desfecho desejado pela vítima.

*

A acessibilidade das tecnologias já mencionadas torna-as igualmente acessíveis aos perpetradores. Por natureza facilitam também a propagação e perpetuidade de textos e imagens, que se multiplicam e existem por muito tempo ou indefinidamente. Isso significa que o dano causado na vítima pode ser continuado e difícil de mensurar.
O comportamento ou motivação e a estratégia do perpetrador pode ser repetido com frequência variável e pode ser conduzido utilizando uma ou mais formas de tecnologia, em *posts* nas redes sociais, *uploads* em plataformas de entretenimento, mensagens encaminhadas por *WhatsApp* ou *Telegram*. Os perpetradores utilizam uma variedade de táticas tecnologicamente facilitadas e beneficiam muito das informações que cada um de nós deixa voluntariamente (Hinson, Mueller, O'Brien-Milne & Wandera, 2018, p.3).
Assim, fenómenos como Engenharia Social (Grassi *et al.* 2017) fazem sentido e são cada vez mais patentes.
O relatório de Junho de 2022 do Centro Nacional de Cibersegurança demonstra isso mesmo. As conclusões deste relatório apontam para "a persistência de algumas ameaças próprias do contexto de pandemia, como as ligadas à instrumentalização das fragilidades do fator humano, mas também o reforço de outras que têm grande capacidade de impacto, como o *ransomware* ou a exploração de vulnerabilidades" (Relatório Cibersegurança em Portugal - Riscos e Conflitos, 2022, p.3).
Os incidentes mais registados em Engenharia Social são os casos de *vishing*, *smishing* e *phishing* (todos pertencem à mesma família, usam as mesmas técnicas, mas por meios diferentes: telefonema, sms, *email*), seguido dos casos de *sextortion* ou divulgação não consensual de dados privados, fotografias. Em paralelo, encontram-se os casos de burlas *online* e burlas com páginas *web* falsas (Relatório Cibersegurança em Portugal - Riscos e Conflitos, 2022).

De que forma isto se interliga?

Se o estimado leitor se permitir a aceitar a premissa da existência de um corpo digital e se for possível considerar que esse corpo digital está cada vez mais fundido com o corpo físico, torna-se mais fácil apresentarmos algumas analogias e explanar tendências atuais.
Para muitos a utilização de *smartphones*, múltiplas aplicações, publicação de fotografias, criação de perfis e aceitação de políticas de partilha de dados, são atividades realizadas sem grande reflexão.
Porém, a maioria de nós aprendeu, desde criança, a refletir e criar estratégias de segurança ao navegar no mundo físico.
Se ensinamos as nossas crianças a não conversarem com estranhos na rua, ou a não aceitarem presentes e muito menos entrarem nos veículos de quem não conhecem, devemos com alguma urgência fazer o mesmo tipo de trabalho relativo à sua navegação *online*.
Se fechamos as cortinas dos nossos apartamentos porque ambicionamos por privacidade, então, temos de aplicar estratégias análogas na nossa vida digital. Se não distribuímos as chaves de nossa casa pela rua, então também não devemos partilhar as nossas *passwords* com terceiros e devemos ter cuidado com as palavras-passe que escolhemos. Se, por norma, nos parece avisado fechar a nossa mala ou mochila para que os nossos bens não caiam ou sejam furtados, então temos de aplicar as mesmas estratégias na nossa vida digital.
Se não queremos que as nossas imagens ou as imagens dos nossos filhos circulem nas várias caixas de correio, ou que todos no bairro tenham conhecimento da escola que frequentam, dos seus horários, das equipas desportivas que fazem parte, etc., temos também de refletir sobre o número de fotografias que publicamos *online* e as informações que cada uma dessas imagens revela.
Por outro lado, é também possível perceber como certas atitudes consideradas impensáveis no mundo físico, são facilitavas e muitas vezes encorajadas nas interações *online*.
E como um abuso sofrido *online*, no corpo digital, pode ter drásticas consequências no mundo físico.
Como referimos supra, estes comportamentos danosos já existiam previamente, porém, encontram na tecnologia um propulsor. A diferença está no alcance e potencialmente ao nível de dano.

O mundo digital está repleto de oportunidades.
Tem também, tal como o mundo físico, muitos perigos.
Cabe-nos garantir que todos os cidadãos estão munidos de ferramentas e conhecimento para uma navegação segura para que, empoderados com essas ferramentas, naveguem em liberdade.

Referências Bibliográficas

Delicado, A., Estevens, J., Rowland, J., Truninger, M., Salgado, S. (2021) Nós e a Internet: Diálogo global de cidadãos. Lisboa: Observa/Observatório da Qualidade da Democracia. Recuperado de https://observa.ics.ulisboa.pt/wp-content/uploads/2021/07/research_brief_final_05_07.pdf

Estatísticas Linha Internet Segura (2021). Recuperado de https://www.internetsegura.pt/noticias/estatisticas-apav-linha-internet-segura-2021

Eurostat, Digital economy and society statistics - households and individuals (2022). Recuperado de https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access

Grassi, P., Fenton, J., Newton, E., Perlner, R., Regenscheid, A., Burr, W., Richer, J. (2017) Digital Identity Guidelines: Authentications & Lifecycle Management, National Institute of Standards and Technology Special Publication 800-63B. Recuperado de https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2018). Technology-facilitated gender-based violence: What is it, and how do we measure it? Washington D.C., International Center for Research on Women. Recuperado de https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

Lewis, T., Gangadharan, S. P., Saba, M., Petty, T. (2018). Digital defense playbook: Community power tools for reclaiming data. Detroit: Our Data Bodies. Recuperado de https://detroitcommunitytech.org/system/tdf/librarypdfs/ODB-Digital-Defense.pdf?file=1&type=node&id=81&force=

Leyen, U. (2020). "Building the world we want to live in: A Union of vitality in a world of fragility", discurso sobre o estado da União. Recuperado de https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

Pordata, Indivíduos com 16 e mais anos que utilizam computador e internet em percentagem do total de indivíduos por grupo etário. Recuperado de https://www.pordata.pt/portugal/individuos+com+16+e+mais+anos+que+utilizam+computador+e+internet+em+percentagem+do+total+de+individuos+por+grupo+etario-1139-9242

[S.A], Relatório Cibersegurança em Portugal - Riscos e Conflitos, Junho de 2022. Recuperado de https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

VALENTE, M., NERIS, N; RUIZ, J; BULGARELLI, L. (2016). O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge porn no Brasil. InternetLab: São Paulo. Recuperado de https://www.internetlab.org.br/wp-content/uploads/2016/07/OCorpoOCodigo.pdf

Outros recursos eletrónicos

https://www.internetsegura.pt/lis/pedir-esclarecimento
https://www.inhope.org/EN
https://www.internetsegura.pt/lis/denunciar-conteudo-ilegal
https://datadetoxkit.org/pt/families/datadetox-x-youth/
https://myshadow.org/

07.

DA ADMISSIBILIDADE DA CAPTURA OU MONITORIZAÇÃO ENCOBERTA *ONLINE* DE DADOS INFORMÁTICOS COMO MEIO DE OBTENÇÃO DE PROVA NO PROCESSO PENAL PORTUGUÊS

GONÇALO GAGO DA CÂMARA

A captura ou monitorização encoberta *online* de dados informáticos: noção e enquadramento.

A figura da captura ou monitorização encoberta *online* de dados informáticos está longe de ser pacífica na doutrina. A causa desta celeuma doutrinal, prende-se com a forma como este meio de obtenção de prova é, incontornavelmente, severamente atentatório e limitador de direitos fundamentais dos cidadãos.
A captura ou monitorização encoberta *online* de dados informáticos consiste em as autoridades judiciárias usarem determinado tipo de *malware*, instalado *online* de forma remota e secreta, com vista a infiltrarem-se em sistema informático alheio, do suspeito ou do arguido, sem que este tenha conhecimento de tal diligência probatória e com vista a, de duas uma: retirar informação num único acesso ou intervenção (*Daten-Spiegelung*); ou monitorizar o sistema alvo por via de uma intervenção prolongada no tempo (*Daten-Monitoring*).
Este meio de obtenção de prova demonstra-se fulcral, por exemplo, para a intercepção de comunicações VoIP. Isto porque, a intercepção deste tipo de comunicações, porque encriptada, apenas será frutífera se for realizada na fonte, i.e., com a instalação prévia de malware no sistema informático fonte (ou receptor), por forma a capturar ou monitorizar, *online* e de forma sub-reptícia, os dados informáticos desencriptados.
Como já vinha adiantando PAULO PINTO DE ALBUQUERQUE em tom de crítica à então proposta legislativa que, mais tarde, se veio a tornar a Lei do Cibercrime: "A proposta de lei não trata o novo meio de obtenção de prova da captura ou monitorização encoberta de dados informáticos, isto é, a infiltração *online* pela polícia num sistema informático, por exemplo através dos chamados cavalos de Tróia, de modo a que a polícia possa em tempo real conhecer a informação à medida que ela é introduzida no sistema informático. Este tipo de infiltração visa, em regra, computadores pessoais, PDA e telemóveis, onde se proceda à criação, tratamento e armazenamento de dados e informações multifacetados da pessoa suspeita, neles se incluindo textos, sons e imagens da pessoa (...)".
A defesa do recurso à captura ou monitorização encoberta *online* de dados informáticos como meio de obtenção de prova tem vindo a angariar adeptos na doutrina, motivados pela convicção de que a incessante evolução tecnológica veio determinar que as autoridades de investigação criminal se encontram crescentemente despojadas dos meios adequados para repelir e investigar actividades ilícitas no ciberespaço.
Concomitantemente, DAVID SILVA RAMALHO acrescenta que este é "(...) o motivo pelo qual temos assistido recentemente a uma defesa (...) da admissibilidade das ditas buscas *online* com fundamento, por um lado, numa aplicação directa do regime da intercepção de comunicações, previsto no artigo 18.º da Lei do Cibercrime, por vezes mesclado com o regime das buscas por forma a retalhar por via interpretativa uma base legal apta a legitimar aquele meio de obtenção de prova, e, por outro, na aplicação do regime da pesquisa de dados informáticos, previsto no artigo 15.º da Lei do Cibercrime.".
Sucede que o princípio da legalidade, que rege todo o processo penal, é fortemente fragilizado por considerações deste cariz, uma vez que, tendo em consideração o contexto

constitucional em que estas normas se inserem, em momento algum o legislador português permite, no actual estado d'arte, que as autoridades judiciárias se façam valer do uso deste meio de obtenção de prova. Vejamos.

As doutrinalmente badaladas (falsas) vias de escape retiradas dos artigos 15.º, 16.º e 18.º da Lei do Cibercrime

Começando pela análise do disposto no artigo 18.º da Lei do Cibercrime, verificamos à partida que o que é permitido é a mera intercepção de comunicações, no momento do seu tráfico, e não a procura de dados imóveis, armazenados em determinado sistema informático até ser encontrado algo criminalmente relevante.
Neste sentido, também não será defensável afirmar que se encontram, no n.º 3 do artigo 18.º da LC, evidências da admissibilidade da captura ou monitorização encoberta *online* de dados informáticos de acesso único (Daten–Spiegelung) arguindo que nesta sede é permitida a recolha e registo de dados de tráfego, uma vez que é apenas disso que se tratam: dados de tráfego, i.e., que pressupõem a movimentação dos dados que são recolhidos apenas se estiverem em deslocação entre dois ou mais terminais de comunicação.
Caso contrário, nem faria sentido a utilização da expressão "intercepção", uma vez que a mesma, para que seja útil, pressupõe movimento.
Preconizando o entendimento de DAVID SILVA RAMALHO a este respeito, não se afirme que a remissão que o n.º 4 do artigo 18.º faz para o regime das escutas telefónicas englobaria o disposto no artigo 189.º do CPP quanto a escutas ambientais que determinam, em semelhança ao cavalo de Tróia que se instalaria no sistema informático visado aquando da captura ou monitorização encoberta de dados informáticos, a instalação de suportes técnicos capazes de captar som, pois tal regime foi manifestamente excluído da letra do n.º 4 do artigo 18.º da Lei do Cibercrime dado que o legislador remete directamente apenas para os "(...) artigos 187.º, 188.º e 190.º do CPP".
Outra perspectiva através da qual alguns autores pretendem defender que a captura ou monitorização encoberta *online* é admissível, é por via da análise comparativa entre este possível meio de obtenção de prova, as buscas tradicionais (arts. 174.º e ss. do CPP), a pesquisa de dados informáticos (artigo 15.º da Lei do Cibercrime) e a apreensão de dados informáticos (artigo 16.º da lei do Cibercrime).
Começando pelo primeiro tipo, vejamos que, nos termos do artigo 174.º n.º 3 do CPP, aplicável *ex vi* n.º 6 do artigo 15.º da Lei do Cibercrime, a autoridade judiciária teria de estar presente, sempre que possível, na diligência.
Esta expressão, decalcada no disposto no n.º 3 do artigo 174.º do CPP, tem levado a doutrina a discutir, afinal de contas, qual será a consequência da ausência da autoridade judiciária aquando da feitura da pesquisa informática.
BENJAMIM SILVA RODRIGUES considera, a nosso ver correctamente, dada a limitação intensa de direitos fundamentais em causa e, sobretudo, o constante do artigo 32.º n.º 4 da CRP, que o disposto no artigo 15.º n.º 1 da Lei do Cibercrime deverá ser restritivamente interpretado, preconizando-se o entendimento de que a realização da pesquisa de dados informáticos sem a presença da autoridade judiciária, deverá ser eliminada da norma em questão.
Já DUARTE RODRIGUES NUNES, uma vez que considera, que não estamos perante uma restrição intensa de diretos fundamentais, interpreta a expressão "sempre que possível" exegeticamente.
Consideramos que é evidente a verificação de uma restrição intensa de direitos fundamentais aquando do recurso à pesquisa informática – nem que seja, no mínimo, por ser um veículo da ingerência e devassa da reserva à intimidade da vida privada –, pelo que aproveitamos para citar, num tema conexo, um Acórdão do Tribunal de Justiça da União Europeia, em sede do qual resulta um claro exemplo da devida consideração da restrição intensa de direitos fundamentais: "Assim, os artigos 4.º e 8.º da Diretiva 2006/24, ao estabelecerem regras para o acesso das autoridades nacionais competentes aos dados, são igualmente constitutivos de uma ingerência nos direitos garantidos pelo artigo 7.º da Carta (Respeito pela vida privada e familiar). Do mesmo modo, a Diretiva 2006/24 é constitutiva de uma ingerência no direito fundamental à proteção dos dados pessoais, garantido pelo artigo 8.º (Proteção de dados pessoais) da Carta, visto que prevê um tratamento dos dados pessoais.
Há que constatar que a ingerência que a Diretiva 2006/24 comporta nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, como também salientou o advogado geral, entre outros, nos n.ºs 77 e 80 das suas conclusões, é de grande amplitude e deve ser considerada particularmente grave.
Além disso, o facto de a conservação dos dados e a sua utilização posterior serem efetuadas sem que o assinante ou o utilizador registado sejam informados disso é suscetível de gerar no espírito das pessoas em causa, como salientou o advogado geral nos n.ºs 52 e 72 das suas conclusões, a sensação de que a sua vida privada é constantemente vigiada".
Deste modo, salvo melhor entendimento, reiteramos a nossa discordância com o entendimento de que a pesquisa de dados informáticos não consubstancia uma restrição intensa de direitos

fundamentais, dado que não devemos fazer uso deste argumento, ou melhor, daquele excerto da letra da lei, na égide de uma interpretação exegética, com vista a trivializar o carácter intensamente lesivo que a busca/pesquisa informática tem na esfera do visado (e até na esfera de pessoas que se relacionam com o mesmo).
A partir do momento em que há uma intromissão, ainda que legitimada pelo *ius imperii* ou *ius puniendi,* porque devidamente autorizada ou ordenada por autoridade judiciária, na vida privada do arguido em virtude da feitura de uma busca/pesquisa informática, estamos, *ab initio*, perante uma restrição intensa dos direitos constitucionalmente garantidos do arguido, uma vez que há uma ingerência total (e, por vezes, desenfreada) na vida privada do mesmo.
Retomando a questão da presença da autoridade judiciária, bem sabemos que, como elucida GERMANO MARQUES DA SILVA, no respeitante à figura do juiz, "a intervenção de um juiz na limitação de direitos fundamentais, sendo já uma garantia, não é, porém, por si só garantia suficiente contra o arbítrio na limitação dos direitos", mas é, certamente, uma barreira apenas transponível em casos excepcionais e não, certamente, transponível a bel-prazer, em prol do fortalecimento de uma interpretação literal da medida normativa da limitação de direitos fundamentais.
Afinal de contas, a aplicação de normas processuais penais não se coaduna, evidentemente, com qualquer interpretação utilitarista ou instrumentalizadora dos direitos, liberdades e garantias do arguido, em prol da reprodução de elementos formais normativos, em preterição da devida consciencialização da inserção sistemática da norma em apreço.
A presença da autoridade judiciária tem um escopo notoriamente garantístico, pois visa assegurar a vigilância e direcção da diligência probatória, tendo por missão asseverar que a mesma é efectuada no estrito e cabal respeito pela legalidade, quer seja pela tutela das formalidades necessárias, quer pela salvaguarda dos direitos dos arguidos que, não bastante já serem alvos de um procedimento criminal são, por vezes, vítimas de abusos de poder.
Deste modo, quando o legislador opta por permitir que a diligência probatória seja efectuada sem ser na presença da autoridade judiciária, tal permissão deverá ser restritamente interpretada, uma vez que a *ratio legis* daquela previsão, em conformidade com as garantias processuais constitucionais, revela que não só a regra será a autoridade judiciária estar presente, como a sua não comparência deverá ser uma medida de ultima ratio e devida a razões ponderosas e devidamente fundamentadas, em consonância, nomeadamente, com o disposto no artigo 32.º n.º 8 da CRP que proíbe toda e qualquer produção de prova abusiva que, nomeadamente, resulte na intromissão na vida privada do visado.
Visto que já nos pronunciámos quanto ao conteúdo desta (infeliz) expressão utilizada pelo legislador, desde já concedemos que este factor não é, de facto, impedimento, porquanto a autoridade judiciária poderia estar presente no momento da busca, ainda que não no local alvo (pois frustraria o cariz encoberto da mesma), mas sim estando presente ao vigiar o técnico que efectue a busca remota.
Quanto ao argumento utilizado por DUARTE RODRIGUES NUNES para obviar ao embate com o princípio da legalidade pelo facto de não existir previsão legal que permita a utilização deste meio de obtenção de prova, afirmando que o legislador ao não distinguir "(...) entre pesquisas "presenciais" e *online* não está a excluir expressamente as pesquisas *online* (...)" não é um entendimento do qual possamos preconizar, uma vez que não se coaduna com o devido enquadramento infraconstitucional do sistema processual penal português.
Esta interpretação não se nos afigura adequada ao caso em concreto, uma vez que não tem em devida consideração, a razão pela qual o legislador distingue a pesquisa presencial da *online*.
A verdade é que o legislador não efectua tal distinção, pois passa por dois pressupostos: o primeiro é que o princípio da legalidade em sentido estrito determina que só são permitidas as acções encobertas (onde a captura ou monitorização encoberta de dados informáticos se inseriria) que estão legalmente consagradas – o que afasta logo à partida o meio encoberto de obtenção de prova em apreço – e o segundo, é que o legislador não distingue entre pesquisas presenciais e *online* porque parte do princípio que a pesquisa informática prevista na lei do cibercrime pressupõe, *ex vi* n.º 6 do artigo 15.º, que o arguido, nos termos do artigo 176.º n.º 1 do CPP, tem conhecimento (ainda que possa ser por terceiros – n.º 2 do mesmo preceito) da pesquisa de que está a ser alvo.
Quando muito, o que poderíamos admitir é que o requisito do conhecimento da diligência por parte do alvo poderia ser afastado em eventuais capturas encobertas *online* efectuadas no âmbito da leitura conjunta do disposto nos arts. 176.º n.º 1 parte inicial e 174.º n.º 5 al. a) do CPP. E, mesmo neste caso, embatemos necessariamente no problema de estarmos perante um meio de obtenção de prova encoberto que não se encontra expressamente tipificado pelo que, nos termos da reserva de lei resultante do artigo 18.º n.º 2 da CRP e do princípio da legalidade *stricto sensu*, terá sempre de ser considerada inviável.
Não se afirme, também, que o constante do n.º 5 do artigo 15.º da Lei do Cibercrime demonstra a possibilidade de uma captura ou monitorização encoberta de dados informáticos, na medida em que a extensão da diligência, prevista neste preceito legal, a outro sistema informático, também pressupõe sempre que o arguido tenha conhecimento da diligência efectuada no sistema informático por via do qual se acede ao segundo.
Reiteramos: Não é concebível que se argua pela admissibilidade de tal meio de obtenção de prova na medida em que, tal seria admitir, num pleno Estado de Direito Democrático, que fosse admissível a prática de diligências probatórias não previstas na lei.
Compreendemos que se torna crescentemente mais difícil para as autoridades de investigação criminal, acompanhar ou combater os meios pelos quais são praticados os crimes informáticos ou as vicissitudes por via das quais os mesmos se manifestam ou são auxiliados na sua preparação, execução e consumação, pelo que admitimos ser compreensível a criação ou utilização de meios de obtenção de prova de cariz encoberto, com vista a munir aquelas entidades dos recursos idóneos a equilibrar a investigação de redes criminosas altamente organizadas, ou de ilícitos altamente atentatórios de direitos fundamentais.
Mas a admissão de tal meio de obtenção de prova, não poderá resultar da interpretação forçada e optimista de normas em vigor que abrem espaço à obscuridade hermenêutica e à limitação ilegítima de direitos fundamentais num contexto jusconstitucional.
Em respeito pelos princípios da proporcionalidade, da segurança e certeza jurídicas e da confiança dos cidadãos na actuação estatal, a possibilidade de recurso a tais meios de obtenção de prova deverá estar devida, concreta e expressamente tipificada.
A consagração deste meio de obtenção de prova deverá obedecer a requisitos materiais concretos, olhando para o que se encontra desbravado pela doutrina e para as lições fornecidas pelo direito comparado.
É neste sentido que países como a Itália, a Alemanha e Espanha inovaram ao permitir a captura ou monitorização encoberta *online* de dados informáticos, mas apenas em certos casos de ocorrência e de natureza excepcional e em respeito por um conjunto cumulativo de requisitos materiais e formais.
Por conseguinte, conseguimos admitir a consagração deste meio de obtenção de prova desde que o mesmo se encontre expressa e indiscutivelmente tipificado, esteja dependente do preenchimento de critérios taxativos, que a sua utilização seja permitida apenas durante um período determinado de tempo que, uma vez esgotado, estará dependente de novo despacho fundamentado pela autoridade judiciária e que a autorização ou validação dependa de fundamentação exaustiva, i.e., procedimentalmente descritiva e delimitativa do seu escopo e abrangência, pelo Juiz de Instrução Criminal, na égide do que é, incontestavelmente, dada a natureza do meio de obtenção de prova *sub iudice,* matéria abrangida pelo princípio da reserva de Juiz.

Da eventual consagração da captura ou monitorização encoberta *online* de dados informáticos no ordenamento jurídico português

Ao contrário da porção da doutrina que considera, no actual estado d'arte, ser admissível o recurso à captura ou monitorização encoberta *online* de dados informáticos, não cremos que tal meio de obtenção de prova seja admissível, ou esteja sequer consagrado no actual estado do sistema processual penal português.
O processo penal não se coaduna com a existência de "meias verdades normativas", sem substância expressa e concretamente tipificada na lei, por forma a justificar o recurso a meios de obtenção de prova gravemente limitadores de direitos fundamentais.
Afinal de contas, é essa a fórmula que devidamente norteia todo o processo penal de cariz acusatório vigente no nosso ordenamento jurídico, em conformidade com o determinado pelos arts. 29.º e 32.º n.º 5 da CRP.
Caso contrário, estaríamos perante um verdadeiro Estado-polícia Orwelliano, cego de meios e complacente perante a vitimização de cidadãos em prol da "eficácia" da prossecução da acção penal e da Justiça.
O processo penal do nosso ordenamento jurídico de Estado de Direito Democrático,

obedece a um conjunto alargado de princípios gerais fundamentais, tais como o princípio da segurança jurídica e o da protecção da confiança dos cidadãos, o que determina que toda e qualquer produção e aplicação legislativas se deverá conformar àqueles princípios, na medida em que os mesmos revelam quais as devidas valorações fundamentadas do legislador constituinte, consagrante dos direitos fundamentais, limitados pelo processo penal.

Os princípios da segurança jurídica e da protecção da confiança, acarretam com eles a exigência da consolidação de um mínimo de certeza e segurança aquando da tutela de direitos fundamentais, bem como na salvaguarda das expectativas legitimamente criadas na égide da devida protecção da confiança da comunidade na ordem jurídica e na actuação do Estado, sobretudo quando estamos perante uma limitação grave de direitos, liberdades e garantias, como o recurso à captura ou monitorização encoberta *online* de dados informáticos.

Razão pela qual não se poderá deixar em aberto, como se de uma carta branca se tratasse, qualquer que seja o método ou procedimento limitante ou restringente de direitos fundamentais em processo penal.

Em concordância, MANUEL DA COSTA ANDRADE refere que a actividade hermenêutica da legislação existente não pode resultar na aceitação de "normas penais em branco", maleáveis e passíveis de subsunção aos novos meios técnicos de invasão e devassa.

Subsequentemente, preconizando o entendimento por nós também adoptado, BENJAMIM SILVA RODRIGUES salienta pertinentemente que por esta via se concretiza uma «(...) tremenda devassa dos direitos informáticos constantes do sistema informático. Mais do que lesar-se o direito à inviolabilidade do sigilo das comunicações electrónicas corre-se, agora, um efectivo risco de lesar o direito à autodeterminação informacional (...). Havendo, com uma actuação das instâncias formais de controlo, no contexto de uma investigação criminal, a confluência da lesão, com um único acto, simultaneamente de dois direitos fundamentais e apenas estando prevista a admissibilidade da lesão de um deles (...), que se afigura proibido o acesso a tais dados pessoais de terceiros. Com a infiltração de um vírus informático ou outro específico meio de "monitorização", verifica-se que se dá uma "grande devassa" de todo o sistema informático, em níveis desproporcionados».

Por conseguinte, o primeiro obstáculo intransponível no sentido da inadmissibilidade actual da captura ou monitorização encoberta *online* de dados informáticos, será inevitavelmente o facto de tal implicar a aceitação de meios encobertos altamente danosos de direitos fundamentais que não estão previstos – ou expressamente previstos – em qualquer diploma legal nacional.

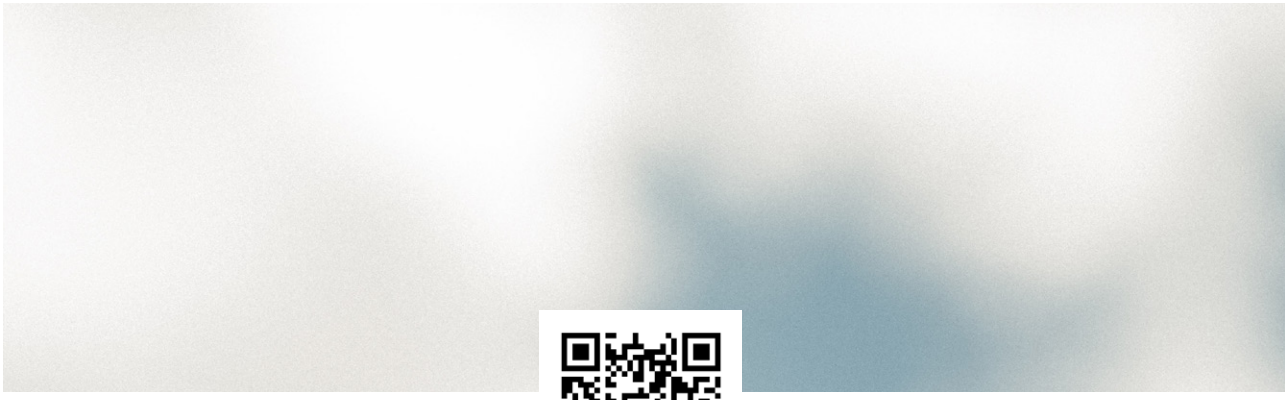
Se considerarmos que tal meio de obtenção de prova se encontra na actual letra da lei, será o mesmo que admitir a existência de uma limitação tremenda dos direitos fundamentais, sem substância positivada expressa, concreta, inequívoca e delimitada, puramente em prol da prossecução cega da acção penal – em detrimento directo dos princípios da proporcionalidade, da segurança jurídica, da lealdade processual dos órgãos de investigação criminal e da protecção da confiança dos cidadãos na actuação do Estado – indigna de um Estado de Direito, e digna de um Estado onde a prova abusiva de direitos fundamentais é admitida, aplaudida e encorajada.

Este meio de obtenção de prova consubstancia logo à partida uma violação clara e indiscutível do princípio da reserva de lei e da legalidade em sentido estrito, na medida em que não se encontra concreta e expressamente previsto em nenhum diploma legal em vigor e a limitação de direitos fundamentais que o mesmo acarreta não se coaduna com interpretações fantasiosas, derivativas ou integrativas da lei processual penal.

Concomitantemente, para além da inexistência de norma legal habilitante, o alargamento da actual letra da lei à admissão da captura ou monitorização encoberta *online* de dados informáticos, é contrária à devida interpretação histórica da mesma, uma vez que, aquando da entrada em vigência da mesma, nunca o legislador cogitou ou sequer enquadrou aqueles meios de obtenção de prova.

Por outro lado, mesmo que a título puramente hipotético se admita, como parte da doutrina supra-referida (DAVID SILVA RAMALHO e PAULO PINTO DE ALBUQUERQUE), que este meio de obtenção de prova se encontra consagrado no ordenamento jurídico português, por via da leitura conjunta do disposto nos artigos 15.º e 19.º da Lei do Cibercrime, tal consagração estará, como devidamente salientam aqueles autores, inevitavelmente ferida de inconstitucionalidade material, por violação do princípio da proporcionalidade dos artigos 26.º n.ºs 1 e 2 e 32.º n.º 4 da CRP, porque, tratando-se de matéria de reserva de Juiz, permitiria o recurso a este meio encoberto de obtenção de prova sem supervisão ou controlo por parte de um juiz.

Nestes termos, o recurso actual à captura ou monitorização encoberta *online* de dados informáticos como meio de obtenção de prova em processo penal, consubstancia prova ilícita, em conformidade com o disposto no artigo 126.º n.º 3 do CPP.



MISCELLANEA
Nº17 **APAV**

INSTITUIÇÃO DE SOLIDARIEDADE SOCIAL
PESSOA COLETIVA DE UTILIDADE PÚBLICA

RUA JOSÉ ESTÊVÃO, 135 A, PISO 1, 1150-201 LISBOA
TEL. 21 358 79 00 | APAV.SEDE@APAV.PT

APAV®
associação portuguesa de
Apoio à Vítima

CHAMADA GRATUITA
116 006
LINHA DE APOIO À VÍTIMA
DIAS ÚTEIS DAS 08H-22H