MISCELLANEA APAV

JUL 2024 — N.º20
REVISTA SEMESTRAL
GRÁTIS

FICHA TÉCNICA

REVISTA MISCELLANEA
Nº REGISTO ERC: 127611 – JULHO 2024

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

DIRETORA
ROSA SAAVEDRA

ILUSTRAÇÕES
CONSTANÇA BRITO

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

Esta é a primeira edição de 2024 e, à semelhança de anos anteriores, é mais uma oportunidade para dar destaque às candidaturas que foram premiadas no âmbito do Prémio APAV para a Investigação. Assim, na Edição #20 da Miscellanea APAV será apresentado um artigo da autoria da vencedora do prémio, Vânia Simões, intitulado "A violência obstétrica no ordenamento jurídico português – contributos para uma evolução do quadro legislativo", que partilha uma reflexão acerca do problema conceptual e das dificuldades em legislar a violência obstétrica, e o artigo de Marta Pereira de Sousa, a quem foi atribuída uma menção honrosa e que, em coautoria com Inês Sousa Guedes e Jorge Quintas, apresentou o artigo "O papel das redes sociais enquanto mecanismos de perpetuação do *victim blaming* e do *slut-shaming*". Neste artigo, reflete-se acerca do papel das redes sociais na promoção e na perpetuação de discursos *victim blaming* e *slut-shaming* contra mulheres vítimas de violação.

O Prémio APAV para a Investigação é uma iniciativa que se destina a premiar trabalhos de investigação científica sobre temas ou problemas relacionados com a missão da Associação: apoiar as vítimas de crime, suas/seus familiares e amigas/os. Reflete também a contribuição crescente da Associação para o aperfeiçoamento das políticas públicas, sociais e privadas centradas no estatuto de vítima.

Este prémio é concebido em parceria com a Fundação Montepio, entidade cuja missão e valores se adequam aos princípios de atuação da APAV e à finalidade do Prémio. Em 2023, foi celebrada a sua nona edição. Neste número, gostaríamos ainda de sublinhar a participação da Escola de Criminologia da Faculdade de Direito da Universidade do Porto, através das/os suas/seus estudantes e docentes na elaboração de dois artigos: "A fraude romântica *online* como um problema em crescimento" e "*Ransomware*: a emergência de uma nova forma de cometer crimes". Esperamos que esta participação possa inspirar outras/os estudantes a submeterem os seus trabalhos, contribuindo para a disseminação de conhecimento sobre formas de vitimação e criminalidade emergentes. No primeiro destes dois artigos, é realizada uma revisão da literatura sobre a fraude romântica, percorrendo a história do seu surgimento, as diferentes estratégias e *modus operandi* utilizados, as razões que levam à escassez de denúncias no âmbito desta fraude, a legislação e os números existentes sobre o fenómeno. No segundo, procuram-se explicitar as dinâmicas características do *Ransomware*. Convido a explorarem o artigo para conhecerem este conceito que, não sendo novo, tem assistido um crescimento exponencial nos últimos anos. Por fim, uma breve reflexão acerca da criminalidade associada ao terrorismo através do artigo "Combate ao Terrorismo: Repressão, Prevenção e Protecção". Farei, à semelhança do que fazem os autores, um destaque particular para a matéria de proteção das vítimas e ao facto de não existir, em Portugal, qualquer disposição legal especial dedicada especificamente à sua proteção, integrando-se os seus direitos na perspetiva mais genérica dos direitos das vítimas e das vítimas especialmente vulneráveis, o que, dadas as particularidades desta forma de violência e crime pode ser, manifestamente, insuficiente.

Para terminar, uma nota relativamente ao papel que todas as pessoas têm na prevenção da violência e crime, seja através da partilha de conhecimento, como aqui se faz, seja através da denúncia de situações que conheçam. Deixo como mote, a frase de uma das últimas campanhas de sensibilização da APAV e que assinalou o Dia Internacional de Sensibilização sobre a Prevenção da Violência Contra as Pessoas Idosas: "O papel principal é meu" (ver pág. 47).

ROSA SAAVEDRA

NOTAS BIOGRÁFICAS

BEATRIZ **PARENTE ARAÚJO**

Estudante do 3º ano da Faculdade de Direito da Universidade do Porto. Tem como áreas de interesse a Investigação Criminal, Ciências Forenses, Terrorismo e Formas de Vitimação.

CARLOS **PINTO DE ABREU**

É advogado especialista em direito criminal, membro do Conselho Consultivo do Forum Penal - Associação dos Advogados Penalistas e vogal da Direcção da Associação Portuguesa de Apoio à Vítima. Foi membro da Comissão de Legislação, presidente da Comissão de Direitos Humanos, vogal do Conselho Geral, presidente do Conselho Distrital de Lisboa e vice-presidente do Conselho Superior, todos órgãos da Ordem dos Advogados. Foi também Presidente da Assembleia Geral do Forum Penal e presidente da Direcção da Caixa de Previdência dos Advogados e Solicitadores. É autor ou coautor de um vasto número de artigos e de livros publicados, entre os quais os seguintes: Estratégia Processual – de uma visão bélica para uma perspectiva meramente processual; Direitos do Homem – Dignidade e Justiça; Direitos Humanos – Cidadania e Igualdade; Direitos Fundamentais – Multiculturalismo e Religiões, Direitos Básicos – Alimentação, Saúde e Habitação, Protecção, Delinquência e Justiça de Menores – um manual prático para juristas… e não só; Legislação de Execução de Penas e Regime Penitenciário e Casos e Causas – a história também se repete…

CONSTANÇA **DUARTE**

Constança Duarte nasceu em Coimbra numa madrugada primaveril do ano de 1994. O seu interesse pela arte nasce do contacto prematuro com a biblioteca da sua mãe. Como filha única não tem outra opção senão aprender a entreter-se sozinha e a criar os seus mundos. Eventualmente cresceu mas manteve-se constante nos seus interesses e passa a vida debruçada sobre o papel ou sobre o barro criando danos permanentes no seu trapézio. Valoriza na sua vida e no seu trabalho o saber fazer, explorar diferentes materiais, desenvolver técnicas e, como se aborrece facilmente, descobrir coisas novas. Interessa-se pelos seres humanos enquanto objectos de estudo bizarros e pelo modo como a vida se vai construindo no meio da correria e da incerteza. A crescente digitalização do mundo empurra-a cada vez mais para o papel. Interessa-lhe a plasticidade do erro, valoriza a intuição no seu processo.

GABRIEL **AFONSO**

Natural do Porto, frequenta, de momento, o 3.º ano da Licenciatura em Criminologia da Faculdade de Direito da Universidade do Porto, no âmbito da qual fez parte do grupo que desenvolveu o presente artigo. Estreia-se na publicação de pesquisa científica, o seu grande objetivo de carreira. As suas áreas de interesse são cibercrime, CPTED e insegurança urbana.

GIL **NEVES VILELA**

É um jovem jurista que cresceu e estudou em Odemira até aos 17 anos, idade em que se mudou para Lisboa, onde, muito recentemente, em 2022, concluiu a licenciatura em Direito na Faculdade de Direito da Universidade de Lisboa. Actualmente, é advogado-estagiário na Carlos Pinto de Abreu e Associados - Sociedade de Advogados, SP, RL, e docente do Curso Profissional de Técnico de Serviços Jurídicos no Instituto para o Desenvolvimento Social (IDS).

INÊS **SOUSA GUEDES**

Licenciada, Mestre e Doutorada pela Faculdade de Direito da Universidade do Porto. Professora Auxiliar da mesma instituição. Membro integrada do Centro de Investigação Interdisciplinar em Justiça (CIJ) e investigadora colaboradora no CEJEIA (Centro de Estudos Jurídicos, Económicos, Internacionais e Ambientais), Universidade Lusíada. Vice Presidente do Conselho Pedagógico, membro da Comissão de Ética da FDUP e membro da Comissão Cientifica da Licenciatura em Criminologia. Incorpora o Conselho Diretor da Associação Internacional de Criminologia de Língua Portuguesa (AICLP) e o *European Working Group on Cybercrime*. As suas áreas de interesse são cibercrime, medo do crime e insegurança urbana.

INÊS **VIANA DA COSTA**

Estudante do 3º ano da Faculdade de Direito da Universidade do Porto. Tem como áreas de interesse o Cibercrime, Terrorismo e Direito Penal.

JOÃO **CAMBÃO DA CRUZ**

Estudante do 3º ano da Faculdade de Direito da Universidade do Porto. Tem como áreas de interesse a Criminalidade Organizada e o Cibercrime.

JORGE
QUINTAS

Jorge Quintas é Professor Associado da Faculdade de Direito da Universidade do Porto (Escola de Criminologia). Membro integrado do Centro de Investigação Interdisciplinar em Justiça (CIJ) e Vice--Presidente da Associação Internacional de Criminologia de Língua Portuguesa (AICLP). joliveira@direito.up.pt

JOSÉ
DE ALMEIDA

Estudante do 3º ano da Faculdade de Direito da Universidade do Porto. Tem como áreas de interesse o Terrorismo e a Radicalização, a Criminalidade Económica e o Cibercrime.

JOSÉ
DUARTE GOMES

Natural de Braga, viveu praticamente a sua vida toda em Famalicão. Frequenta, de momento, o 3.º ano da Licenciatura em Criminologia da Faculdade de Direito da Universidade do Porto, no âmbito da qual fez parte do grupo que desenvolveu este artigo. Tem como áreas de interesse o cibercrime, o crime organizado, a investigação criminal e a cooperação internacional, sendo esta última o seu grande objetivo de carreira.

MANUEL
MARTINS

Agente Principal da PSP desde 1994, prestando serviço na Esquadra de Espinho. No decorrer da atividade profissional frequentou diversas formações, sendo de realçar a área da violência doméstica. Frequenta atualmente o 3.º ano da Licenciatura em Criminologia pela Faculdade de Direito do Porto, no decorrer do qual realizou o presente trabalho. Tem como áreas de interesse o cibercrime, prevenção do crime, segurança e policiamento.

MARIA JOÃO
PEREIRA

Natural de Vila Nova de Gaia, é atualmente estudante do 3.° ano da Licenciatura em Criminologia na Faculdade de Direito da Universidade do Porto. É ainda voluntária do Instituto Português do Desporto e da Juventude, no projeto "Navegas em Segurança?"; envolvendo--se também no mundo universitário, nomeadamente, na Associação de Estudantes. Tem como principais áreas de interesse a cibercriminalidade e a prevenção e intervenção com vítimas e/ou crianças e jovens em risco, tendo apostado em formações, sobretudo, sobre estas últimas temáticas.

MARTA
PEREIRA DE SOUSA

Marta Pereira de Sousa é natural do Porto. Licenciada em Sociologia pela Faculdade de Letras da Universidade do Porto e com Mestrado em Criminologia pela Faculdade de Direito da Universidade do Porto, atualmente executa funções enquanto assistente editorial da revista Sociologia – Revista da Faculdade de Letras da Universidade do Porto. Em 2023, recebeu uma menção honrosa do Prémio APAV para a Investigação 2023, com o trabalho "O papel das redes sociais enquanto mecanismos de perpetuação do *victim blaming* e *slut-shaming* – um estudo empírico", que consiste numa versão mais desenvolvida do tema deste artigo. martagpereiradesousa@gmail.com

SAMUEL
MOREIRA

Licenciado, mestre e doutor em Criminologia pela Faculdade de Direito da Universidade do Porto (FDUP). É Professor Auxiliar Convidado da FDUP e Professor Auxiliar da Faculdade de Direito da Universidade Lusíada (FDUL) do Porto, lecionando em todos os ciclos de estudo em Criminologia. Simultaneamente, é membro da Comissão Científica do Doutoramento em Criminologia da FDUP. É Investigador Colaborador no CIJ (Centro de Investigação Interdisciplinar em Justiça) da FDUP e Investigador Integrado no CEJEIA (Centro de Estudos Jurídicos, Económicos, Internacionais e Ambientais) da FDUL. As suas principais áreas de lecionação e investigação incluem a (in) segurança, o policiamento e o cibercrime.

VÂNIA
SIMÕES

Assistente convidada na Faculdade de Direito da Universidade Nova de Lisboa e Universidade Autónoma de Lisboa, Advogada e Doutoranda em Direito.

01.

O PAPEL DAS REDES SOCIAIS ENQUANTO MECANISMOS DE PERPETUAÇÃO DO *VICTIM BLAMING* E DO *SLUT-SHAMING*

MARTA PEREIRA DE SOUSA,
INÊS SOUSA GUEDES
E JORGE QUINTAS

Introdução

As vítimas, enquanto indivíduos lesados com a prática de um crime, têm vindo a ser alvo, muitas das vezes, de uma campanha de culpabilização por parte da sociedade, com a multiplicação de opiniões e preconceções que atribuem a culpa do crime e da vitimização às próprias vítimas, sob pretensa de estas terem contribuído para a sua agressão, desculpabilizando, desta forma, a conduta dos ofensores (Schoellkpof, 2012).
Este *victim blaming*, muitas vezes aliado a comentários *slut-shaming* que procuram julgar e humilhar as mulheres pelas suas práticas sexuais – presumidas ou efetivas – (Hackman *et al.*, 2017), incide maioritariamente sobre as mulheres vítimas de violação – crime previsto e punido no Art.164º do Código Penal português – que, quer pela presença de ideais sexistas no seio da sociedade, quer pela imagem social negativa existente acerca da sexualidade feminina, são frequentemente conduzidas ao estatuto de principais incitadoras deste tipo de ataques (Ventura, 2018).
Estas narrativas são, na maioria das vezes, proferidas *online* nas redes sociais, plataformas que têm vindo a promover não só a maior visibilidade dos fenómenos em estudo, mas também a disseminação de discursos misóginos contra o sexo feminino, sendo de ressaltar que o *victim blaming* e o *slut-shaming* permeiam atualmente os discursos sociais acerca da violação (Schoellkopf, 2012; Zaleski *et al.*, 2016).
A presente investigação procurou então auscultar o papel das redes sociais na promoção e na perpetuação de discursos *victim blaming* e *slut-shaming* contra vítimas de violação. Atribuindo especial atenção à vertente dos social media, refletiremos ainda sobre a agência feminina nestes espaços e a forma como a figura da vítima é retratada nas notícias publicadas *online*, de modo a apreender como esta representação pode contribuir não só para a promoção do *victim blaming* e do *slut-shaming*, mas também para a banalização da violência sexual.
Com vista a determinar a influência das redes sociais na manutenção e na reprodução destes fenómenos, a presente investigação procurou desenvolver uma análise empírica de cunho qualitativo que, alicerçada na análise de conteúdo, se comprometeu a perscrutar comentários redigidos *online* em resposta a notícias de violação, de forma a apreender se entre estes existiam discursos *victim blaming* e *slut-shaming* acerca das vítimas e, se assim se verificasse, determinar quais os padrões discursivos, as crenças e as preconceções envolvidas na construção deste tipo de discursos, bem como as características do cenário de violação (da vítima, do ofensor, etc.) e do comentador, que determinam a maior propensão para a expressão de comentários *victim blaming* e *slut-shaming*.
Desta feita, o presente artigo conta com duas secções. Na primeira secção, será realizada uma revisão da investigação científica acerca da representação dos crimes de violação nos social media, observando-se nomeadamente a representação mediática das mulheres vítimas de violação nas notícias inscritas *online* e a resposta dos internautas. Serão ainda definidos os conceitos de *victim blaming* e de *slut-shaming*.
A segunda secção fica assim reservada para a apresentação do estudo empírico, com a descrição do desenho metodológico e a auscultação dos resultados.

1. A representação dos crimes de violação nos social media.

De acordo com Montiel (2014, p. 68) "*(…) sexism and misogyny in media has increased dramatically the last decades (…) as the new media environment has exacerbated existing problems and brings new challenges (…)*". São exemplos de novos desafios a crescente hostilidade do espaço *online* para com as mulheres

e o seu julgamento mediático. Neste sentido, torna-se deveras pertinente auscultar as redes sociais, com vista a aprofundar não só a incidência e os mais diversos contornos do *victim blaming*, fenómeno caracterizado pela forma como a "(…) victim of a crime or abuse is held partly or entirely responsible for the actions committed against them" (Schoellkopf, 2012, p. 2), e do *slut-shaming*, isto é, de narrativas misóginas que procuram julgar as mulheres com base na sua percebida atividade sexual (Hackman *et al.*, 2017) no seu domínio, mas também a forma como proporciona a abordagem acerca da violência sexual, as suas vítimas e ofensores.

O surgimento da Internet possibilitou a criação massiva de redes sociais, isto é, de novos espaços – digitalmente abstratos – de interação social que, pelo seu carácter sensacionalista e ilimitado, rapidamente conquistaram o interesse e a adesão da maioria da população (Datareportal, 2022). Nestes espaços, os indivíduos são convidados a criar perfis pessoais, onde lhes é possível não só partilhar as suas vidas, mas também consultar os mais diversos tipos de conteúdos, falar livre e anonimamente entre si e expressar as suas opiniões. Desta feita, também o *victim blaming* tem vindo a proliferar no contexto das redes sociais, onde é, maioritariamente, perpetrado através/a par do *slut-shaming* (Sills *et al.*, 2016; Webb, 2015, Zaleski *et al.*, 2016). Com efeito, as redes sociais têm sido autênticos palcos para uma dicotomia do sexo feminino: se por um lado contribuem, segundo Tate (2016), para a sexualização das mulheres, já que, ao reproduzir os ideais de beleza de sociedades sexistas, promovem a auto-sexualização de jovens e mulheres adultas em busca de "*likes*"; por outro, também para a sua censura, uma vez que são frequentemente criticadas pela forma como se vestem ou se apresentam nestas plataformas, através de comentários difamatórios que as definem, por palavras e discursos obscenos, como "oferecidas", etc. (idem). Ora, esta forma de *slut-shaming* digital, impulsionado pelo anonimato e pelo alcance infindável da Internet, visa não só a preservação dos "bons costumes", mas também "*(…) perpetuate and maintain cultural suppression of female sexuality (…)*" (Webb, 2015, p. 10), podendo ser levado a cabo, quer por homens, através de insultos e ameaças de cariz violento e sexual, para a imposição de "*(…) how women should behave and present themselves online*" (Tate, 2016, p. 37); quer por mulheres que, segundo Webb, quando influenciadas por uma educação sexista, rebaixam as suas "rivais", para garantir o seu privilégio sexual e a sua demarcação de condutas censuradas pelo olhar masculino. Note-se ainda que, segundo Tate, este *slut-shaming* tem como principais alvos não só mulheres vítimas de violação, mas também mulheres abertamente feministas e críticas da ideologia misógina.

Tate reflete ainda sobre os *e-biles*, isto é, uma forma de *slut-shaming* que se traduz na crescente criação de contas de ódio, de *e-mails* e mensagens violentas enviadas a mulheres, muitas das vezes, de forma gratuita, onde lhes são endereçados insultos, ameaças verbais de morte e de agressão (física e sexual), conteúdos gráficos, entre outros tipos de intimidação. Aliás, segundo Montiel (2014), a Internet e os "*(…) social media have (…) become (…) powerful vehicles for misogynistic threats and harassment (…)*." (p. 70), que procuram silenciar as mulheres, as vítimas e a narrativa feminista na luta pela igualdade de género.

Focando a violação da mulher, esta também pode ser molestada, segundo Webb (2015) e Montiel (2014), através das redes sociais, nomeadamente, com a partilha de *revenge porn*, com a publicação, por parte de (ex-) parceiros, de imagens íntimas da mulher em que esta aparece parcial ou totalmente nua em situações comprometedoras, um ataque direto ao seu consentimento e a sua intimidade sexual que confere também uma violação da mulher, mesmo sem o encontro violento que a caracteriza geralmente.

Há ainda o registo de casos de revitimização nestes espaços, com milhares de mulheres violadas a verem não só imagens e vídeos dos seus ataques publicados em redes sociais (e outros domínios privados criados para este efeito) (Webb, 2015), mas também a resposta social perante notícias de violação, que se pauta, muitas vezes, não pelo choque e revolta face ao sucedido, mas sim pela ridicularização e a culpabilização da vítima, que se "ofereceu", que "deixou" ou que não se debateu suficientemente, opiniões inerentemente *victim blaming* que são expressas em comentários acessíveis à vítima (Boux & Daum, 2015; Webb, 2015; Zaleski *et al.*, 2016). Aliás, segundo Zaleski *et al.* (2016) cujo estudo empírico, de cunho qualitativo, procurou refletir acerca do fenómeno da cultura de violação *online* através da análise de comentários a notícias de violação, "*(…) technology creates new avenues for victim blaming in regard to rape cases and society, overall.*" (Zaleski *et al.*, 2016, p. 923). Também Stubbs-Richardson *et al.* (2018) refletem acerca desta revitimização *online*, tendo concluído, através da sua análise empírica a comentários inscritos *online* sobre casos de violação com grande visibilidade mediática, que grande parte destes discursos se apoiavam em três grandes temas, sendo estes (1) a dicotomia "virgem-promíscua" e a crença no mundo justo; (2) a partilha de informação acerca de casos de violência sexual; e (3) a desmistificação de *rape myths*. Enfocando a nossa lente de análise sobre o primeiro tema, que arrecadou, de forma geral, um maior número de comentários em ambos os estudos mencionados supra, segundo os dados apresentados pelos autores, podemos afirmar que esta tendência traduz a crença generalizada do público que "*(…) bad things happen to bad people, that there are virgins and whores, or that rape is merely a deviant event*

that happens to girls who behave or dress 'inappropriately'". (Stubbs-Richardson *et al.*, 2018, p. 98).

Esta tendência dos internautas para o *victim blaming* e julgamento da mulher vítima pode dever-se igualmente à forma como as vítimas e os cenários da violação em si são enquadrados pelas narrativas mediáticas das notícias publicadas *online*.

A violência de género perpetrada contra as mulheres (violência doméstica, violência física, psicológica e sexual) é bastante sub-representada nos meios de comunicação (Meyers, 1997) devido não só a todo o tabu que ainda a envolve, mas também pela grande trivialidade que lhe é atribuída quer pelos media em geral, quer pela opinião pública (Montiel, 2014; Ventura, 2014).

No entanto, como é de conhecimento geral, as notícias são tanto ou mais rentáveis quanto maior for a negatividade e/ou a excentricidade associada aos seus factos. Assim sendo, Ventura (2014) argumenta que as notícias de violação vivem numa constante dualidade: ao mesmo tempo que são tratadas pela imprensa como um "assunto menor", são igualmente detentoras de um grande valor noticioso e furor mediático – especialmente quanto mais chocantes forem –, uma vez que se demonstram, só pela sua nomenclatura, incitadoras de uma curiosidade sórdida entre os leitores.

Ora, todo este sensacionalismo mediático da violação acarreta consigo, na perspetiva da autora e de Thacker (2017), consequências nefastas para a sociedade, pois "*constantly seeing and hearing about women being raped or threatened with rape (…) desensitizes (…) viewers and facilitates rape*" (Thacker, 2017, p. 91), bem como a violência de género e a desconsideração das vítimas.

Ademais, as notícias de violação tendem a privilegiar a descrição detalhada não só dos acontecimentos da violação, mas também, e principalmente, da vítima, enfatizando as suas características pessoais, o seu comportamento e o estado em que esta se encontrava no momento da violação (Montiel, 2014), apelidando-as ora "(…) como indefesas, fracas ou culpadas pela sua vitimação (…)" (Cerqueira & Gomes, 2017, p. 5), endossando assim o escrutínio da vítima e a tendência para o *victim blaming* entre os leitores internautas.

Um outro exemplo da maneira como as redes sociais proporcionam esta revitimização passa pela forma como os perfis da vítima são vasculhados, durante processos judiciais, em busca de fotos e/ou comentários mais ousados que façam prova da sua percebida imoralidade e conduta sexualmente promíscua, determinando a culpabilização da mulher pela violação (Boux & Daum, 2015; Tate, 2016; Zaleski *et al.*, 2016).

2. Estudo empírico

Os principais objetivos da presente investigação passavam pela intenção de (1) descrever os discursos produzidos *online* acerca de notícias de violação; com vista a (2) perceber se os comentários às notícias de violação divulgadas nas redes sociais possuem discursos *victim blaming* e *slut-shaming*; bem como (3) captar quais as características sociodemográficas da amostra associadas a uma maior propensão para a produção de discursos *victim blaming* e *slut-shaming*; e (4) determinar quais as características do evento da violação e seus intervenientes que fazem com que os internautas expressem mais discursos *victim blaming* e *slut-shaming*.

Desta panóplia de objetivos foi possível extrair as três questões de investigação que nortearam toda a investigação e posterior análise, sendo estas:

(1) Quais as principais crenças e perceções na base de discursos *victim blaming* e *slut-shaming* presentes *online*?;

(2) Qual o perfil de indivíduo mais propício à manifestação *online* de narrativas *victim blaming* e *slut-shaming* acerca de vítimas de violação?; e (3) Quais os cenários de violação noticiados que suscitam um maior número de comentários *victim blaming* e *slut-shaming*?

2.1. Metodologia

A metodologia da presente investigação foi cunhada, primordialmente, pelo método qualitativo que facilitou a auscultação das respostas dos internautas a um conjunto de notícias de violação de mulheres por meio da técnica de análise de conteúdo.

Os procedimentos passaram essencialmente pela pesquisa intensiva junto das páginas de *Facebook* dos periódicos Jornal de Notícias e Correio da Manhã, seguida da seleção das notícias de acordo com critérios de inclusão previamente definidos (sobre os quais dissertaremos abaixo), com auxílio de palavras-chave como "violação", "mulher violada", entre outros termos mais específicos que se vieram a demonstrar pertinentes consoante a crescente familiarização com os discursos captados.

Após esta seleção, foi encetada uma primeira auscultação/delimitação dos comentários a incluir na fase da análise – com a exclusão de todos os comentários que não fizessem alusão direta à notícia ou que surgissem em resposta a outros comentários –, sendo igualmente este o momento em que se realizou a caracterização sociodemográfica dos internautas e anonimização dos comentários.

A amostra da presente investigação foi então composta por meio de uma amostragem intencional, com a recolha de um conjunto de notícias cujos contornos respeitassem dois critérios centrais que se pretendia testar, sendo estes a perceção dos internautas acerca do estado da vítima (vítima "ideal" e vítima em estado vulnerável) e a relação entre a vítima e o seu alegado ofensor (estranho e conhecido).

Desta feita, foram selecionadas quatro notícias que retratassem, respetivamente, a violação de uma vítima "ideal" – vítima que, no momento do ataque, aparentava uma conduta normativa, encontrando-se na totalidade das suas capacidades

cognitivas – por parte de (1) um ofensor conhecido versus de (2) um ofensor seu desconhecido; e a violação de uma vítima em estado vulnerável – vítima alcoolizada que, devido ao seu estado alterado estava numa posição de grande vulnerabilidade – por parte de (3) um ofensor seu conhecido versus de (4) um ofensor desconhecido. Nesta lógica, muito sumariamente, a Notícia 1 (cenário vítima ideal – ofensor conhecido) relata a violação de uma jovem por parte do namorado, a Notícia 2 (cenário vítima ideal – ofensor desconhecido) a violação de uma mulher por um estranho durante um passeio, a Notícia 3 (vítima em estado vulnerável – ofensor conhecido) a violação de uma jovem inconsciente devido ao consumo excessivo de álcool por um amigo, e a Notícia 4 (vítima em estado vulnerável – ofensor desconhecido) a violação de uma mulher alcoolizada por parte de um desconhecido durante uma festa noturna. Ademais, é-nos ainda importante ressaltar que foram definidos igualmente um critério territorial, para que as notícias amostradas descrevessem apenas casos ocorridos em Portugal e um critério de maioridade da vítima.

Relativamente à caracterização sociodemográfica da amostra, composta por um total de 313 comentários, esta era maioritariamente constituída por indivíduos do sexo feminino com idades compreendidas entre os 40 e os 80 anos de idade (68,1%). No que diz respeito ao estado civil dos internautas amostrados, a maioria apresentava-se como casado, sendo ainda de ressaltar os 33,3% que se definia como solteiro. A clara maioria, 71,9%, afirmava estar empregada por conta própria ou de outrem.

Findada a amostragem, foi iniciada a análise dos comentários com base na análise de conteúdo, que foi ainda aliada a uma vertente de análise quantitativa de dados. Esta análise foi facilitada pela construção de uma grelha de análise composta por um conjunto de três medidas de análise: (1) a dimensão do perfil sociodemográfico percebido do comentador, sendo que se procurou registar – sempre que exequível e zelando pelo anonimato da amostra – o sexo, a faixa etária, o estado civil e a situação profissional dos internautas; (2) a dimensão do conteúdo do comentário em si, focada na captação dos seus temas (a quê ou a quem é que estes comentários se pretendiam referir) e subtemas (as ideias-chaves e idealizações que dão forma ao tema). A investigação expectava inicialmente encontrar Discursos sobre a vítima e Discursos sobre o ofensor, tendo sido definidos igualmente a priori alguns subtemas expectados para cada tema (ex. conduta, caracterização, punição, etc.). No entanto, no decurso da análise dos comentários, tornou-se necessária a criação de outros temas como a Preocupação securitária, que englobou os comentários que formularam preocupações ou críticas acerca da ordem social e do fenómeno da violação; os Discursos sobre a justiça e os Discursos sobre a prevenção e a punição do crime que discutiam, respetivamente, sobre cada uma destas vertentes no contexto nacional, entre outros temas de reduzida incidência na amostra; e, por último, (3) a dimensão da natureza do comentário, que consistia na classificação/agrupamento final dos comentários consoante o tema e o subtema ao qual faziam menção, sendo de salientar que para além dos expectados subtemas de *victim blaming* e *slut-shaming* para os Discursos sobre a vítima, pudemos acrescentar o subtema da compaixão.

2.2. Resultados

A presente investigação apurou que os comentários amostrados se referiam a uma larga panóplia de temas.

No entanto, ressaltamos que a grande maioria se concentrou, em primeiro lugar, nos Discursos sobre o ofensor, que arrecadaram 142 dos 313 comentários considerados (45,4%), especialmente nos três primeiros cenários; em segundo lugar, nos Discursos sobre a vítima, que motivou 35,8%, com especial expressão na Notícia 4 (cenário vítima em estado vulnerável – ofensor desconhecido) onde arrecadou 41 dos 112 comentários identificados para esta natureza; e por último, na Preocupação securitária, com 85 comentários (27,2%).

Começamos por destacar especialmente os Discursos sobre a vítima. Quantitativamente os comentários *victim blaming* foram preponderantes (N=79; 70,5% dos que se centraram na vítima), registando-se ainda frequentemente alguns comentários de *slut-shaming* (N=25; 22.3% dos que se centraram na vítima) e muito raramente discursos de compaixão para com a vítima, independentemente do seu estado/relação com o ofensor (N=8; 7,2% dos que se centraram na vítima).

Relativamente ao *victim blaming*, os comentários desta natureza foram maioritariamente proferidos por indivíduos do sexo masculino com idades compreendidas entre os 40 e os 80 anos de idade e incidiam maioritariamente sobre a crítica da conduta da vítima, que os internautas acusavam como tendo sido irresponsável, irrefletida ou, até mesmo, provocatória da violação, uma tendência que se verificou um pouco por toda a amostra, mas que se adensou especialmente na resposta aos cenários vítima em estado vulnerável (Notícia 3 e 4, onde obtiveram a sua maior expressão), tendo sido tecidos comentários como "Não querendo atirar as culpas para cima da senhora, mas também porque é que foi correr para uma zona de mato sozinha???" (Not. 2, F, 20-40); "Ela que pensasse em não fazer festa nenhuma, que nada lhe acontecia!" (Not. 3, M, 20-40) ou "Devia ter ficado sossegadinha em casa (…) já não tinha nada para se queixar" (Not. 4, M, 20-40).

Em segundo lugar, salientamos o subtema da descredibilização da vítima. Este subtema, apesar de estar diluído por toda a amostra, destacou-se especialmente na Notícia 1 (cenário vítima ideal – ofensor conhecido), onde os internautas procuraram desacreditar a vítima pelo

MAL ME QUER

“O MEU PENSAMENTO ERA SÓ FUGIR.”

VIOLAR ME QUER

CHAMADA GRATUITA
116 006
LINHA DE APOIO À VÍTIMA
DIAS ÚTEIS DAS 08H-23H

APAV®
associação portuguesa de
Apoio à Vítima

Se és vítima de violência no namoro, ou conheces alguém que seja, fala com a APAV.

facto de esta acusar o seu namorado, fazendo-o por meio de comentários irónicos e inusitados como "Onde é que já se viu, vir dizer que foi violada pelo namorado??? (…) se alguém se acredita nesta, queria era uma razão para lhe pôr os patins" (Not. 1, F, 40-80). Este subtema contou ainda com a presença de discursos que aludiam à fabricação da denúncia por parte da vítima, quer por vingança contra o suposto ofensor, quer em busca de interesses económicos/sociais, quer pelo facto de "estar na moda" dizer que se foi violada, referindo o aumento significativo das denúncias de violação após a eclosão do movimento *#MeToo* ("(…) aguardemos para ver se é verdade ou só mais uma frustrada kkkk" (Not. 2, M,40-80); "Agora é moda, quando não gostam vão fazer queixa à polícia!!!" (Not. 4, M, 40-80)).

Por último, para o *victim blaming*, registou-se ainda um conjunto considerável de comentários que criticavam o estado da vítima no momento da violação. Direcionados especificamente às vítimas em estado vulnerável das Notícias 3 e 4, estes comentários procuraram, quer de forma acusatória, quer por meio de uma ironia grosseira, imputar à vítima a culpa da sua violação ("Ela embebedou-se porque quis, fosse um bocadinho mais consciente não lhe tinha acontecido nada" (Not. 3, M, 40-80); "Ninguém a mandou ir enfrascar-se e roçar-se em gajos que não conhece de lado nenhum… correu-lhe mal" (Not. 4, M, 40-80)).

No que concerne ao *slut-shaming*, este foi também maioritariamente expresso por internautas do sexo masculino entre os 40 e os 80 anos de idade. O principal subtema mobilizado por este tipo de comentários foi a atribuição de promiscuidade à vítima, com os internautas a argumentar que esta, pela sua conduta/carácter, teria provocado a violação ao 'dar esperanças' ao ofensor, ou que a vítima teria mesmo desejado a agressão sexual ("(…) deve-lhe ter dado poucas esperanças deve, só imagino a libertinagem ele não voltava se não soubesse que tinha abertura…" (Not. 3, F, 40-80); "Se calhar não lhe tinha levado prenda… se calhar era o que ela preferia mesmo" (Not. 3, M, 20-40); "(…) temos certeza que a garagem da senhora não estava aberta a clientela?" (Not. 4, M, 40-80)).

Este tema contou ainda com o subtema das piadas misóginas, sendo relevante destacar um comentário inserido neste subtema que, referente ao cenário da Notícia 1 da jovem violada pelo namorado, declara que "O Código Civil Português decreta que a mulher tem de satisfazer as necessidades conjugais do homem" "(Not. 1, M, 40-80), traduzindo-se numa clara desvalorização da violação pela existência de uma relação amorosa entre a vítima e o seu ofensor.

Refletindo agora sobre os comentários realizados acerca do ofensor, estes foram na sua maioria proferidos por mulheres inseridas na faixa etária 40-80, sendo o seu principal subtema o apelo à punição do ofensor, um subtema que esteve presente de uma forma bastante significativa em todas as notícias, destacando-se, no entanto, a sua presença na Notícia 3 (cenário vítima em estado vulnerável – ofensor conhecido) com 42 dos 100 comentários registados para este subtema. É-nos importante ressaltar que estes discursos punitivos contavam não só com pedidos de prisão dos ofensores ("(…) Espero bem que não fique sem castigo, para a cadeia!" (Not.1, F, 40-80)), mas também, senão principalmente, com apelos à agressão ("Era enchê-los de porrada até que lhes saltassem os dentes todos fora (…)" (Not. 2, M, 40-80)), à castração ("VERGONHA, CASTRAÇÃO" (Not. 4, F, 20-40)), à violação ("que os violadores sejam sodomizados (…) Que sintam na pele (…) o que é ser violado (…)" (Not. 3, F, 40-80)) e, até mesmo, à morte destes últimos ("Pena Capital, não há outro remédio para estes animais" (Not. 2, M, 40-80)).

O segundo subtema predominante dos discursos contra o ofensor, igualmente destacado na Notícia 3, foi a caracterização deste último por parte dos internautas, que procuraram a clara desumanização do ofensor ao apelidá-lo de 'monstro' ("(…) um monstro que não vale sequer o ar que respira (…)" (Not. 1, M, 40-80)) – sendo esta a nomenclatura mais frequentemente utilizada –, de 'maluco' ("(…) Estes malucos não podem continuar por aí à solta" (Not. 2, F, 40-80)), de 'psicopata' ("(…) E só doentes, PSICOPATAS (…)" (Not. 2, F, 20-40)), de nomes injuriosos relacionados com animais ("Prisão para este porco (…)" (Not. 4, F, 20-40)), entre outros termos mais pejorativos da gíria popular.

Relativamente à Preocupação securitária, tema fortemente marcado pela preocupação dos internautas para com o fenómeno da violação, a grande maioria dos comentários desta natureza foram proferidos por mulheres, cerca de 75,3%, com idades entre os 40 e os 80 anos. Os principais subtemas identificados, dentro de um largo leque de subtemas, foi, primeiramente, a crítica à sociedade, com a multiplicação de discursos, especialmente na Notícia 3 (cenário vítima em estado vulnerável – ofensor conhecido), que procuravam criticar o estado atual da sociedade, demonstrando grande preocupação para com as proporções tomadas atualmente pelo fenómeno da violação, através de comentários como "As pessoas são muito más, vê-se bem (…) que atualmente ninguém sente empatia pelo próximo… para onde vai este mundo meu deus?" (Not. 2, F, 20-40), "todos os dias notícias de mais uma mulher violada!! (…) para onde vai esta sociedade??" (Not. 3, F, 20-40).

Em segundo lugar, ressaltamos o subtema de repúdio de discursos *victim blaming* e *slut-shaming* que representou todos os comentários que se opuseram veemente a discursos e comentários deste género, defendendo que "não interessa se é marido, namorado (…) se não há consentimento é CRIME." (Not.1, M, 40-80) e, principalmente, que "Nada justifica uma violação (…) nenhum comportamento é merecedor desta barbaridade" (Not. 3, F, 20-40).

Conclusão

Os resultados permitem concluir que: nos Discursos sobre a vítima, há um claro predomínio do *victim blaming* e em menor grau de *slut-shaming*, sendo raros os discursos de compaixão independentemente do cenário auscultado; nos Discursos sobre o ofensor, predominam os discursos punitivos; e a Preocupação securitária é também relevante.
Desta forma, os dados sugerem que os crimes de violação são campos férteis para a construção não só de narrativas misóginas e de estereótipos erróneos acerca das vítimas e do fenómeno da violação, mas também, se não principalmente, para a proliferação de discursos securitários, extremistas e violentos no que diz respeito à punição do crime e do seu perpetrador. Este contexto digital pouco *victim-friendly*, e consequentemente, pouco *women-friendly*, suscitou já o interesse pela criação de redes sociais exclusivamente para mulheres, espaços que poderiam albergar uma maior sororidade, empatia e liberdade feminina. No entanto, segundo Tate (2016), uma "*(…) feminist digital diaspora from public internet space would further marginalize women and create a vacuum for further sexist biases to circulate.*" (p. 40), sendo, na sua opinião, imperativo que as mulheres mantenham a sua presença nestes espaços e que lutem não só pelo seu empoderamento, pela igualdade de género e pela defesa das vítimas de violação, mas também pela educação de todos para as consequências nefastas da misoginia e dos estereótipos de género, que condicionam, igualmente, a vida de mulheres e homens com as suas representações restritivas.
Em jeito de conclusão, podemos ainda delinear algumas das limitações sentidas pela investigação que se manifestaram, principalmente, no momento da seleção das notícias a amostrar, maioritariamente quer pela complexidade do processo de pesquisa entre inúmeras notícias de violação nas páginas dos periódicos, quer pela criteriosidade envolvida na seleção destas mesmas notícias, que deveriam ser as mais compatíveis e expressivas possível dos cenários delimitados *a priori*.
Algumas direções futuras para a elaboração de novas investigações poderiam passar pela utilização de uma amostra mais numerosa, bem como pelo teste da reação dos internautas a condições de vulnerabilidade da vítima, por exemplo, a presença de deficiências cognitivas/motoras ou de relações de poder entre vítima e ofensor.

Referências bibliográficas

ALMEDINA (2022). Código Penal, 13º Ediçao. ISBN: 978-9-8940-0431-8

BOUX, Holly J. & DAUM, Courtenay W. (2015). "At the intersection of social media and rape culture: how facebook postings, texting and other personal communications challenge the "real" rape myth in the criminal justice system", Journal of Law, Technology and Policy, 90(1), pp.149 -186. https://illinoisjltp.com/journal/wpcontent/uploads/2015/07/Daum&Boux.pdf

CERQUEIRA, Carla, & GOMES, Sílvia (2017). "Violência de género nos media: Percurso, dilemas e desafios." In Neves, S. & Costa, D. (Org.) Violências de Género. (pp. 217-23). CIEG - Edições ISCSP. ISBN: 978-989-646-122-5

DATAREPORTAL (2022). Digital 2022 July Global Statshot Report. https://www.slideshare.net/DataReportal/digital-2022-july-global-statshot-report-jul2022-v02

HACKMAN, Christine L., PEMBER, Sarah E., WILKERSON, Amanda H., BURTON, Wanda & USDAN, Stuart L. (2017). "Slut-shaming and victim-blaming: a qualitative investigation of undergraduate students' perceptions of sexual violence", Sex Education, 17(6), 697-711. https://doi.org/10.1080/14681811.2017.1362332

MONTIEL, A. Vega (2014). "Violence against women and media: advancements and challenges of a research and political agenda". In A. Vega Montiel (ed). Gender and Media: A Scholarly Agenda for the Global Alliance on Media and Gender. Paris, UNESCO/IAMCR, pp. 17- 21

MEYERS, Marian (1997). News Coverage of Violence against Women: engendering blame. Sage Publications, Inc. ISBN: 978-08-0395-636-0. https://doi.org/10.4135/9781452243832

SCHOELLKOPF, Julia Churchill (2012). "Victim-Blaming: A New Term for an Old Trend", Lesbian Gay Bisexual Transgender Queer Center, 33. https://digitalcommons.uri.edu/glbtc/33/

SILLS, Sophie, PICKENS, Chelsea, BEACH, Karishma, JONES, Loyd, CALDER-DAWE, Octavia, BENTON GREIG, Paulette, & GAVEY, Nicola (2016). "Rape Culture and Social Media: Young Critics and a Feminist Counterpublic". Feminist Media Studies, 16(6), 935-951. https://researchspace.auckland.ac.nz/handle/2292/30994

STUBBS-RICHARDSON, Megan, RADER, Nicole E. & COSBY, Arthur G. (2018). "Tweeting rape culture: Examining portrayals of victim blaming in discussions of sexual assault cases on Twitter." Feminism & Psychology, 28(1), pp. 90-108. https://doi.org/10.1177/0959353517715874

TATE, Elisa (2016). "Challenging Women's Digital Agency: The Frequency of Slut Shaming in Social Media." The IJournal: Graduate Student Journal of the Faculty of Information, 1(1), 37-41.https://theijournal.ca/index.php/ijournal/article/view/26477

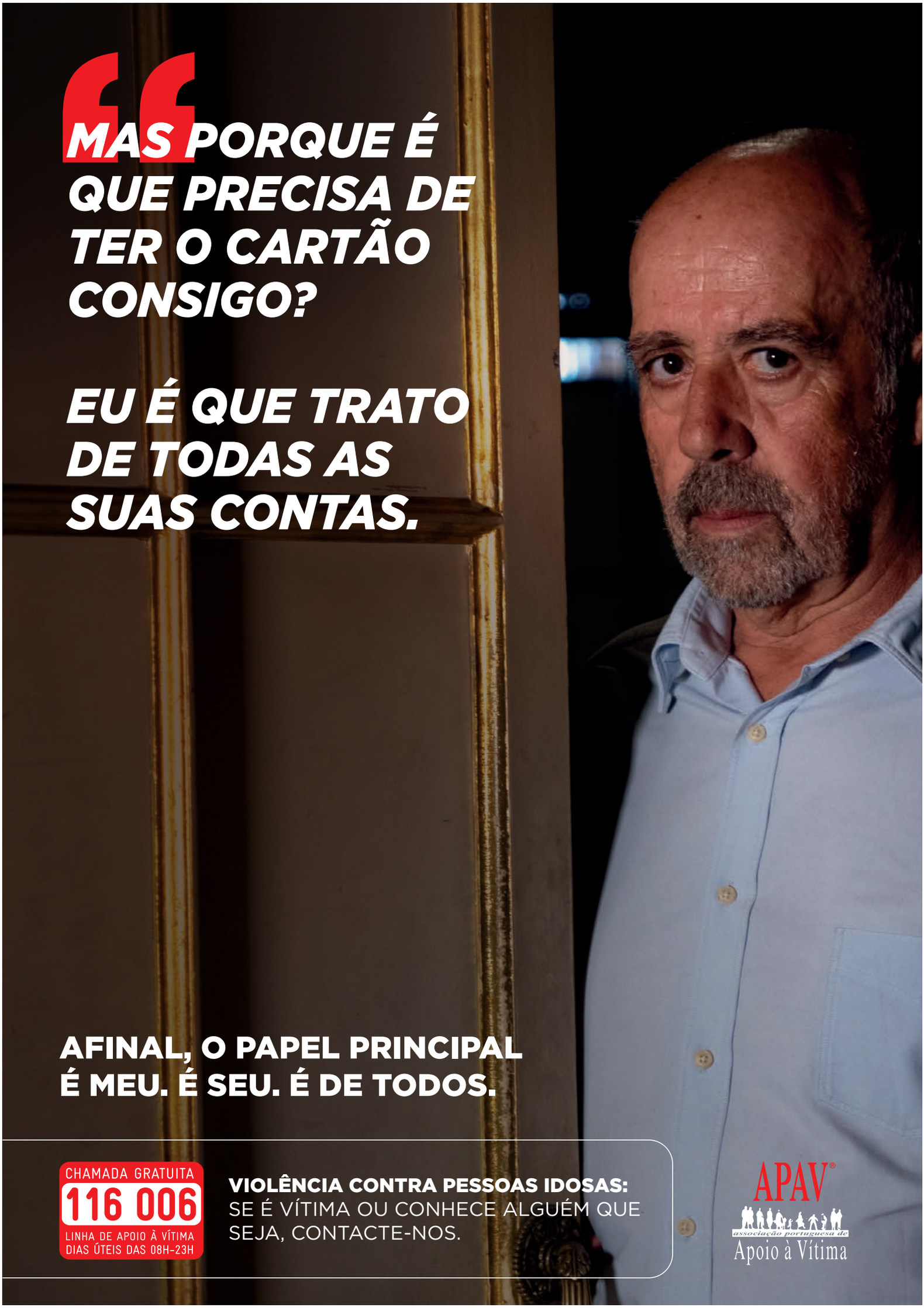
THACKER, Lily K. (2017). "Rape Culture, Victim Blaming, and the Role of Media in the Criminal Justice System." Kentucky Journal of Undergraduate Scholarship, 1(8), 89-99. https://encompass.eku.edu/cgi/viewcontent.cgi?article=1008&context=kjus

VENTURA, Isabel (2014). "Entre anjos e demónios – a narrativa mediática sobre a violência sexual." In AAVV(ed.), Manual de Boas Práticas para a Comissão de Proteção de Crianças e Jovens e todas as entidades que trabalham em prol dos direitos das crianças (pp.158-186). Associação Projeto Criar

VENTURA, Isabel (2018). Medusa no Palácio da Justiça ou Uma história da Violação Sexual. Tinta da China. ISBN: 978-98-9671-427-7

WEBB, Lewis (2015). "Shame transfigured: Slut-shaming from Rome to cyberspace." First Monday, 20(4), 1-23. http://dx.doi.org/10.5210/fm.v20i4.5464

ZALESKI, Kristen L., GUNDERSEN, Kristin K., BAES, Jessica, ESTUPIDIAN, Ely, & VERGARA, Alyssa (2016). "Exploring rape culture in social media forums." Computers in Human Behavior, 63, 922-927. https://doi.org/10.1016/j.chb.2016.06.036


“MAS PORQUE É QUE PRECISA DE TER O CARTÃO CONSIGO?
EU É QUE TRATO DE TODAS AS SUAS CONTAS.
AFINAL, O PAPEL PRINCIPAL É MEU. É SEU. É DE TODOS.
CHAMADA GRATUITA
116 006
LINHA DE APOIO À VÍTIMA
DIAS ÚTEIS DAS 08H-23H
VIOLÊNCIA CONTRA PESSOAS IDOSAS:
SE É VÍTIMA OU CONHECE ALGUÉM QUE SEJA, CONTACTE-NOS.
APAV®
associação portuguesa de
Apoio à Vítima

02.

A FRAUDE ROMÂNTICA *ONLINE* COMO UM PROBLEMA EM CRESCIMENTO

INÊS COSTA, BEATRIZ ARAÚJO, JOSÉ ALMEIDA,
JOÃO CRUZ, SAMUEL MOREIRA E INÊS GUEDES

Introdução

A cibercriminalidade constitui, atualmente, um problema significativo e com repercussões em larga escala, afetando de diversas formas a maior parte das regiões do mundo desenvolvido.
À medida que os sistemas informáticos em rede foram crescendo e se aperfeiçoando, o mesmo sucedeu com a natureza da criminalidade e dos abusos neste contexto cibernético. Com efeito, se nos primórdios da informática, os abusos se restringiam em grande medida a atividades relacionadas com a fraude e o roubo, que representavam a extensão dos crimes tradicionais ao ambiente eletrónico, ao longo do tempo foram surgindo novas e mais avançadas formas de crimes (por exemplo, vírus informáticos) que acabam por ter como alvo a própria infraestrutura informática.
A fraude romântica, que constitui o foco central do presente artigo, é um dos exemplos paradigmáticos de como a Internet tem engendrado novas modalidades de criminalidade, particularmente através de plataformas de relacionamento *online*.
Casos conhecidos e amplamente discutidos como os do Impostor do Tinder, Simon Leviev, que, através de um esquema Ponzi, enganou diversas vítimas, demonstram a extensão dos impactos deste tipo de fraude, não só económicos, como também psicológicos para os alvos.
É precisamente o impacto devastador em milhões de pessoas atualmente (Cross *et al.*, 2018), associada a uma escassez de estudos sobre o fenómeno, que elevam a pertinência de abordar a fraude romântica no contexto cibernético. Ademais, a utilização dos *sites* de namoro que são, de acordo com Cross (2021), utilizados para a perpetração desta fraude, têm vindo a aumentar.
Desta forma, este artigo efetua uma revisão da literatura existente sobre a fraude romântica, iniciando-se por uma abordagem ao cibercrime, apresentando diferentes classificações para o mesmo, as suas características e a legislação existente em Portugal sobre o fenómeno. De seguida, será realizada uma breve abordagem à fraude *online*, dissertando-se sobre a definição da mesma e uma proposta de taxonomia. Por fim, dar-se-á protagonismo ao elemento central do artigo, a fraude romântica, expondo a história do seu surgimento, as diferentes estratégias e *modus operandi* utilizados, as razões que levam à escassez de denúncias no âmbito desta fraude, a legislação e os números existentes sobre o fenómeno. Por fim, analisar-se-ão as características encontradas na literatura respeitante às características das vítimas e dos ofensores.

Cibercrime

De acordo com Yar (2016), o cibercrime pode ser entendido como o conjunto de ofensas que são cometidas através de um computador e de tecnologia eletrónica digital. No âmbito da cibercriminalidade, é comum distinguir-se entre ofensas assistidas pelo computador, isto é, crimes que já existiam antes do surgimento da Internet, mas que adotam uma nova vida no ciberespaço, e ofensas focadas no computador que correspondem a crimes que surgiram em paralelo com a Internet e que não conseguiriam existir sem a mesma, relevando aqui o papel que a tecnologia vai desempenhar (Furnell, 2003).
Outra classificação muito utilizada corresponde à de Wall (2003), que tem em conta o alvo ou objeto da ofensa, sendo propostas, então, quatro categorias do cibercrime: transgressão cibernética, furtos ou enganos *online*, ciber-pornografia e violência cibernética. A transgressão cibernética consiste na entrada não autorizada no computador ou no sistema pessoal de alguém ou de algo que tenha os direitos de posse desse sistema. Os furtos ou enganos *online* envolvem diferentes comportamentos, sendo os mais relevantes, pelo seu crescimento nos últimos tempos, a utilização fraudulenta de cartões de crédito e a *cyberpiracy*. A ciber-pornografia consiste na publicação, troca ou partilha

de materiais sexualmente explícitos no ciberespaço. A violência cibernética consiste no impacto violento que as ciberatividades de outro têm ou podem ter sobre um indivíduo ou sobre um grupo social ou político, atividades estas que podem ir desde *cyberstalking* a discursos de ódio. De acordo com Dias (2012), a cibercriminalidade apresenta diversas características, nomeadamente a transnacionalidade, a a-temporalidade, a deslocalização, a elevada tecnicidade e os elevados danos. A transnacionalidade remete para a dimensão global que a Internet tem vindo a tomar progressivamente, sendo mesmo definida como uma terra de ninguém e numa terra de todos, num tempo de todos e num tempo de ninguém (Rodrigues, 2009, p.161). Esta característica faz com que os ofensores possam ser muito mais rápidos, num espaço dificilmente controlado pela lei e, desde sua casa, chegar a qualquer parte do mundo, agravando o potencial dano das condutas criminosas (Sieber, 1998). Por sua vez, a cibercriminalidade é também a-temporal pelo desfasamento temporal entre a prática ilícita inicial e o seu resultado, como é comum nos casos de *emails* com *malware*, que podem ser abertos pelos seus recetores a qualquer momento. A deslocalização refere-se à passagem, cada vez mais progressiva, das práticas criminosas para o ambiente cibernético, o que, aliado ao anonimato e à perceção ou efetiva elevada probabilidade de impunidade, potencia a prática de crimes que de outra forma não executariam. Esta deslocalização também se observa nos conteúdos relacionados com o crime, que são transportados na própria Internet entre vários servidores para fugir à lei (Dias, 2012). De igual forma, e como já anteriormente citado, o anonimato é um elemento-chave na mais fácil perpetração das ciberofensas, incrementando a ocultação da identidade e/ou suas condutas. Já a elevada tecnicidade favorece o anonimato, uma vez que permite proteger muitos dos dados por programas de encriptação e palavras-passe, barrando o acesso a terceiros. Por último, tem sido enfatizado pela comunidade científica o conjunto de danos causados pelos cibercrimes, tal como será mencionado frequentemente neste artigo, que podem ultrapassar os danos dos crimes tradicionais, exatamente por todas estas características supramencionadas.

Legislação relativa ao cibercrime

No que diz respeito à legislação portuguesa sobre o cibercrime, inicialmente existia a Lei da Criminalidade Informática (Lei nº109/91, de 17 de agosto) que foi ratificada no seguimento da Convenção de Budapeste. Atualmente, a legislação relativa ao cibercrime é a Lei do Cibercrime (Lei nº109/2009, de 15 de setembro), entretanto atualizada pela Lei nº79/2021. Ademais, existem outras ciberofensas em diversos diplomas, nomeadamente no Código Penal, que já tipifica como crime a "Devassa através de meio de comunicação social, da Internet ou de outros meios de difusão pública generalizada" no Artigo 193º, a "Violação de correspondência ou de telecomunicações" no Artigo 194º e a "Burla informática e nas comunicações" no Artigo 221º. A legislação portuguesa sobre cibercrime é complementada por várias leis específicas que abordam diferentes aspetos da segurança digital e da propriedade intelectual. Estas incluem a Lei de Proteção de Dados Pessoais (Lei nº67/98, de 26 de outubro), a Lei da Proteção Jurídica de Programas de Computador (Decreto-Lei nº252/94, de 20 de outubro), o Código de Direitos de Autor e dos Direitos Conexos (Decreto-Lei nº63/85, de 14 de março) e o Regime Geral das Infrações Tributárias (Lei 15/2001, de 5 de junho). Estas leis formam um quadro regulatório abrangente para o cibercrime e a segurança digital em Portugal.

Fraude *online*

De acordo com Button e Cross (2017), a fraude abrange um vasto leque de atividades que têm em comum uma falsa representação que é usada para garantir uma vantagem ou causar uma desvantagem aos outros. Apesar das conceções atuais de fraude estarem fortemente ligadas às novas tecnologias (como a Internet), é importante notar que as tecnologias mais antigas forneceram os meios para a fraude nos séculos anteriores. Com efeito, as fraudes ocorrem desde que as pessoas podem falar e possuir bens. No entanto, à medida que os meios de comunicação e de comércio avançaram, o mesmo aconteceu com a oportunidade e a natureza deste fenómeno.
Uma das definições mais consensuais de fraude é a de Cross, Smith e Richards (2014, p.1) que a concetualizam como a "experiência de um indivíduo que respondeu, através do uso da Internet, a um convite, solicitação, notificação ou oferta desonesta, fornecendo informações pessoais ou dinheiro que levaram a uma perda financeira ou não financeira ou impacto de algum tipo".
Beals e os seus colaboradores (2015) desenvolveram uma taxonomia de fraude, dividindo a mesma em diversos níveis. No primeiro nível, é realizada uma distinção entre fraude contra um indivíduo e fraude contra uma organização. No segundo nível, existem sete subcategorias de fraudes financeiras individuais que se baseiam na expectativa de um benefício ou de uma consequência da transação efetuada, designadamente, fraude no investimento dos consumidores, fraude ao consumidor, fraude de emprego, fraude de prémios e subsídios, fraude de cobrança de dívidas fantasma, fraude de caridade e fraude de relações e de confiança.
No que diz respeito à fraude no investimento dos consumidores, espera-se um benefício no retorno de um investimento. No que concerne à fraude ao consumidor, o benefício esperado é um produto ou um serviço. Relativamente à fraude de emprego,

o benefício expectável é o emprego. Já no que respeita à fraude de prémios e subsídios, o benefício corresponde a um prémio, subsídio, ou a lotaria. Relativamente à fraude de cobranças de dívidas fantasma, o benefício esperado é evitar as consequências do não pagamento de dívidas que a vítima não sabia que eram devidas (e que eram falsas). Na fraude de caridade, o benefício esperado é contribuir para uma instituição de caridade ou organização sem fins lucrativos. Por fim, na fraude de relações e de confiança, o que se espera é promover ou continuar um relacionamento pessoal e por vezes íntimo. Esta última categoria inclui o objeto de estudo do presente artigo – a fraude romântica *online*.

No terceiro nível, os autores vão subdividir estas subcategorias com base no atributo do tipo de transação ou de relação fraudulenta. Nos dois últimos níveis, é feito o mesmo trabalho que no nível três, com as categorias obtidas nesse nível. Beals e colaboradores (2015) vão excluir o furto de identidade *online* desta tipologia, uma vez que consideram que para que exista uma fraude, a vítima deve ser enganada ou persuadida a participar no esquema fraudulento.

Fraude romântica

Feitas as considerações anteriores, importa agora destrinçar os contornos da temática em análise. Assim, a fraude romântica *online* como crime começou a ser alvo de preocupação em 2007 (Buchanan & Whitty, 2014). Apesar da prevalência desta fraude ter vindo a aumentar, este problema ainda é pouco estudado na Criminologia (Cross *et al.*, 2018), existindo poucas investigações cujo foco seja, especificamente, a fraude romântica (Cross, 2020). Nos casos em que a fraude romântica é alvo de estudo, esta tem sido examinada no âmbito do seu caráter distinto dos restantes tipos de fraude, dado que esta vai além dos elevados danos financeiros e pode provocar danos emocionais e psicológicos possivelmente mais prejudiciais. As vítimas mencionam muitas vezes, que os sentimentos de violação e traição decorrentes do término da relação romântica com o ofensor são ainda mais difíceis de lidar do que a perda de bens financeiros (Cross & Holt, 2021).

A fraude romântica é frequentemente considerada uma *advance fee fraud* (AFF), na qual o ofensor pede às vítimas para lhe enviarem dinheiro com a promessa de, mais tarde, receberem uma quantia monetária que é, na generalidade dos casos, significativamente maior que aquela que lhes foi pedida, quantia esta que nunca chega a ser recebida (Chang, 2008).

De acordo com Whitty (2013), os ofensores recorrem a diversas estratégias de engenharia social para enganarem as suas vítimas, tal como fazer-se passar por uma pessoa de autoridade (como um general do exército ou um empresário de sucesso). Além disso, os infratores tendem a estabelecer uma relação descrita como vulnerável, o que os levava a obter ajuda por parte das vítimas. Outra estratégia utilizada é a urgência, isto é, os ofensores apresentam uma falsa urgência, sugerindo que consequências negativas graves ocorrerão se a vítima não transferir dinheiro imediatamente. Eles podem até ameaçar terminar o relacionamento se as vítimas resistirem ao envio de fundos.

Demais características inerentes à fraude romântica e outras *advanced fee frauds* dizem respeito à promessa de ganho financeiro para quem é alvo do esquema (Onyebadi & Park, 2012); a utilização de um tom autoritário (Chang, 2008); a mistura de verdades e factos com mentiras de modo a confundir a vítima e tornar a sua história mais credível (Cross & Holt, 2021) e a presença de erros gramaticais, que pode ser justificado, de acordo com Onyebadi & Park (2012), pela ausência de conhecimento da língua falada (inglesa, normalmente) ou como uma estratégia que faz parte do seu esquema de deceção.

Tipicamente, o indivíduo que vai cometer a fraude encontra as suas vítimas em *sites* ou aplicações de encontros *online*, iniciando uma relação e mostrando desde uma fase precoce que estão apaixonados, mantendo a comunicação intensa e frequente (Cross, 2021). O facto de o ofensor utilizar *sites* legítimos para perpetrar as suas fraudes aumenta a probabilidade das vítimas caírem nestas fraudes (Button & Cross, 2017). Neste processo, o ofensor vai fazer com que a vítima se apaixone e confie no mesmo desde muito cedo. Este é capaz de começar por pedir pequenos "presentes" ou ajudas monetárias para testar se o seu esquema vai funcionar. Se a vítima concordar com os pedidos, o ofensor tem "luz verde" para avançar com a sua fraude, fazendo pedidos mais extravagantes. Este tipo de esquema tem vindo a ser entendido como uma evolução dos métodos fraudulentos, usados por ofensores, para obter lucro financeiro das suas vítimas (Cross, 2021).

Outra característica da fraude romântica *online* é o facto de esta corresponder a uma fraude que é considerada embaraçosa, o que reduz a probabilidade das vítimas reportarem o crime às autoridades, uma vez que têm medo de serem consideradas ingénuas. Além disso, as vítimas podem ter revelado informações pessoais ao ofensor no contexto do relacionamento *online* e podem ainda ter participado em atividades sexuais *online*, o que também as inibe de denunciarem o ofensor (Button & Cross, 2017).

Legislação e prevalência da fraude romântica

No Reino Unido, o crime de fraude está previsto no Fraud Act (2006). De acordo com este, o crime de fraude pode ser cometido de três formas, sendo uma delas e a mais usual a fraude por falsa representação, que se aplica quando uma pessoa, de forma desonesta, representa algo ou alguém de forma falsa, tendo como intenção com essa falsa representação obter ganho pessoal, causar perdas a outro(s) ou expor outro(s) a um risco de perda. Uma representação é considerada

falsa se for enganosa ou diferente da verdade e se a pessoa que a fizer estiver consciente de que o é. Gillespie (2021) sublinha que a caracterização da fraude romântica como um delito previsto no Fraud Act de 2006 é, em geral, inequívoca. A maioria dos casos apresenta claramente uma representação falsa, deliberadamente distorcida da verdade ou concebida para enganar, enquadrando-se assim facilmente na definição legal de fraude. Na nossa legislação, não existe uma menção específica ao crime de fraude romântica *online*. Todavia, podemos considerar que este crime corresponde a um concurso de crimes entre o crime de burla informática e nas comunicações (221º CP) e o de burla qualificada (218º CP).

Quanto à extensão da fraude romântica em Portugal, é possível constatar que os números existentes são escassos. No entanto, estas fraudes românticas são o tipo de criminalidade mais registada pela Linha Internet Segura, tendo existido 100 contactos por parte de vítimas, ao longo do ano de 2022 (APAV, 2023). Adicionalmente, verificam-se algumas ferramentas de apoio a estas fraudes românticas *online*, tais como a iniciativa da Internet Segura que lançou uma brochura com informações sobre a fraude romântica, apresentando sete dicas a seguir para evitar ser vítima deste tipo de fraude. Outra iniciativa corresponde à campanha de sensibilização da APAV no âmbito do Dia Europeu da Vítima de Crime, em conjunto com as celebrações do Mês da Internet Mais Segura, que nos apresenta alguns elementos transversais neste tipo de esquemas (APAV, 2023).

Em suma, enquanto o Reino Unido possui uma abordagem legislativa específica para a fraude através do Fraud Act de 2006, Portugal não tem uma menção explícita à fraude romântica *online* na sua legislação. No entanto, esses atos podem ser subsumidos sob os crimes de burla informática e qualificada. Os dados existentes apontam para a escassez de números, embora as fraudes românticas representem uma grande parte dos casos reportados à Linha Internet Segura em Portugal em 2022.

Características das vítimas

Conhecer as características típicas das vítimas da burla romântica *online* pode ajudar na prevenção do crime. Alguns *sites* de *online dating* já utilizam perfis de personalidade para caraterizar e combinar os seus utilizadores. Isto levanta a possibilidade de utilizar esses perfis de personalidade para detetar indivíduos que possam estar em risco de serem vítimas (Buchanan & Whitty, 2014).

Ao longo dos anos, tem existido alguma especulação sobre a tipologia das vítimas de fraude, tendo, no entanto, a maioria deste trabalho sido focada na fraude na sua generalidade, e não apenas na fraude romântica (Whitty, 2018).

De acordo com Buchanan e Whitty (2014), uma forte tendência para ter crenças românticas e idealizar relações predizem um maior risco de ser vítima de fraudes românticas *online*. Pelo contrário, outros fatores psicológicos tais como a tendência para a solidão, a extroversão, a agradabilidade, o neuroticismo e o *sensation seeking* não têm um efeito significativo. Segundo Buchanan e Whitty (2014), das variáveis que não foram associadas à vitimação, o *sensation seeking* é talvez a que requer mais comentários.

Na generalidade dos casos, quando as pessoas se envolvem em fraudes financeiras, estas fazem-no devido à excitação do processo e da antecipação de um prémio ou de uma recompensa (Lea *et al.*, 2009). No entanto, os processos da fraude romântica parecem ser bastante diferentes. Embora alguns indivíduos possam, de facto, ser atraídos para o esquema devido a uma busca de excitação, em muitos outros casos os processos podem ser muito mais complexos e muito semelhantes ao desenvolvimento tradicional de relações *online* (Buchanan & Whitty, 2014).

Pelo contrário, Whitty, num estudo realizado quatro anos mais tarde, encontrou uma ligação entre traços elevados de impulsividade e *sensation seeking*, traços mais baixos de agradabilidade e um maior risco de ser vítima de fraudes românticas *online*. Uma possível explicação para esta alteração é que, enquanto no estudo de Buchanan e Whitty (2014), o *sensation seeking* foi medido numa escala própria (Brief Sensation Seeking Scale), no estudo de Whitty (2018), o *sensation seeking* foi medido com uma subescala, tendo sido englobado na impulsividade no geral, onde se encontrou uma associação com a vitimação.

Adicionalmente, os traços que mediam a impulsividade, tal como previsto, previam a vitimação. As pessoas enganadas por esquemas românticos são solicitadas a cumprir rapidamente os pedidos dos criminosos (Whitty, 2013), o que talvez explique o facto de as vítimas terem maior probabilidade de obter uma pontuação elevada na subescala de "impulsividade de urgência". Além disso, são contadas às vítimas histórias elaboradas e fantasiosas (Whitty, 2013), o que pode explicar o facto de terem uma pontuação mais elevada de *sensation seeking* em comparação com as não vítimas (Whitty, 2018).

A constatação de que os indivíduos com traços mais baixos de agradabilidade tinham uma maior probabilidade de serem vítimas de uma fraude romântica foi menos fácil de explicar. Talvez os indivíduos menos bondosos tenham menos redes para os ajudar a verificar perfis ou talvez procurem relações mais prejudiciais.

A agradabilidade também pode ser uma posição mais transitória. Segundo Whitty (2013), os criminosos isolam a vítima dos seus entes queridos e obrigam-na a concentrar o seu tempo e recursos na relação fictícia e é difícil para as vítimas reconstruírem as suas redes sociais depois de a fraude ter ocorrido, o que pode explicar a razão para apresentarem traços mais baixos de agradabilidade (Whitty, 2018).

Além disso, Whitty (2018) concluiu que existe uma maior taxa de vitimização nas mulheres de meia-idade e com um elevado

nível de educação, encontrando também uma relação entre a confiança e um maior risco de vitimação por fraudes românticas *online*. O referido estudo fornece possíveis explicações para os indivíduos de meia-idade serem mais frequentemente vítimas deste tipo de fraude. Por um lado, podem ter mais rendimentos disponíveis e, por outro, este grupo pode ter mais probabilidades de procurar parceiros em sítios de encontros, em comparação com outros grupos etários. Relativamente à educação, o resultado obtido contradiz a crença popular de que apenas as pessoas "estúpidas" caem em esquemas fraudulentos. Segundo a investigadora, é possível que as pessoas com um nível de educação mais elevado tenham mais probabilidades de utilizar *sites* de encontro. No entanto, este resultado também sugere que ter um bom nível de educação não protege necessariamente as pessoas de serem burladas (idem). Por fim, as vítimas também têm maior probabilidade de obter uma pontuação elevada nas características de dependência em comparação com as não vítimas, o que sugere que têm dificuldade em afastar-se da fraude depois de introduzidas na narrativa (idem). Em suma, estudos indicam que características como crenças românticas idealizadas e impulsividade podem aumentar o risco de alguém se tornar vítima de fraudes românticas *online*, enquanto outros fatores, como o *sensation seeking*, podem ter uma relação complexa com a vitimação, variando conforme o contexto e a metodologia do estudo.

Características dos ofensores

Ao contrário do que acontece no estudo sobre a vitimação de crimes, onde os fatores que influenciam a vitimação têm sido bastante estudados, a investigação sobre os agressores ainda é escassa (Bilz *et al.*, 2023). De acordo com Anesa (2020), o ofensor de fraude romântica do sexo masculino apresenta-se muitas vezes como um viúvo, com formação superior e um emprego de prestígio, \e sublinha frequentemente que vive no estrangeiro. Já as ofensoras do sexo feminino usam fotografias atraentes e declaram regularmente que escolheram profissões que exigem cuidados e contacto humano. Assim, é possível elaborar um perfil de ofensor, tanto do sexo masculino como do sexo feminino. No perfil do sexo masculino, podemos observar características como ser uma figura de autoridade, ser empresário, gestor ou arquiteto, ser rico, ser viúvo e ser pai. Já as mulheres, nos seus perfis, apresentam-se como sendo semiprofissionais, estudantes, enfermeiras ou assistentes de ensino, utilizando uma fotografia de uma mulher convencionalmente bonita e pode ainda apresentar-se como órfã, como não sendo rica, sem filhos e sem nunca ter tido anteriormente uma relação romântica significativa (Anesa, 2020). Além disso, quando estes ofensores de fraude agem individualmente, tendem a apresentar características como a paciência, *social skills* (usar "falas mansas", e criação de confiança com a vítima), competências básicas de utilização de computadores e de edição de fotografias. Por último, os ofensores tendem a usar a negação da vítima como técnica de neutralização e a recorrer ao anonimato (Rege, 2009).

Conclusão

O estudo da fraude romântica *online* tem ganhado atenção apenas recentemente, com menos de vinte anos de investigação (Cross *et al.*, 2018). Apesar do uso crescente de aplicações de namoro, a investigação sobre fraude romântica, especialmente em relação ao perfil dos ofensores, não tem evoluído no mesmo ritmo.
Comparativamente aos restantes tipos de fraude, a fraude romântica *online* apresenta uma particularidade que se prende com os danos causados, uma vez que estes se estendem para além dos danos económicos, provocando também consequências graves emocionais e psicológicas.

Apesar dos estudos no âmbito da fraude romântica serem escassos, aqueles que existem apresentam resultados muito importantes, nomeadamente no que diz respeito às estratégias utilizadas pelos ofensores, tais como a utilização de um tom ou posição autoritária, a mistura de verdades e factos com mentiras de modo a confundir a vítima e tornar a sua história mais credível e a presença de erros gramaticais. Estes estudos, no âmbito das estratégias do ofensor revelam uma grande importância, uma vez que podem ajudar as vítimas a perceber quando estão a ser vítimas deste tipo de fraude.

É também comum que estes ofensores empreguem um *modus operandi* que passa pelo estabelecimento de uma relação de confiança com a vítima, fazendo-a sentir especial e amada. De seguida, os ofensores começam a realizar os seus pedidos, aumentando a quantia dos mesmos ao longo do tempo.

Os estudos têm abordado também o perfil das vítimas e dos ofensores de fraude *online*, tendo-se averiguado algumas características diferenciadoras. Todavia, mais investigações são necessárias para compreender a fundo as dinâmicas e motivações subjacentes, que impulsionam tanto as vítimas quanto os ofensores neste tipo de crime cibernético.

A falta de preocupação relativamente à fraude romântica nota-se também pela falta de legislação que regule a mesma e pela falta de dados relativos à vitimação por esta fraude. Uma vez que a fraude romântica não se encontra consagrada num tipo legal, não existem estatísticas oficiais sobre a vitimação por fraude romântica. Contudo, é de notar o trabalho da APAV que, através da Linha Internet Segura permite verificar um elevado número de contactos por parte das vítimas, em anos transatos.

Importa ainda realçar que este crime é de difícil investigação criminológica, uma vez que a fraude *online* (incluindo a fraude romântica *online*) comporta alguma das características da cibercriminalidade, nomeadamente o anonimato e a transnacionalidade. Estas características, além de dificultarem a investigação criminológica, complexificam também a deteção e punição dos ofensores.

Conclui-se que este tema é de elevada relevância e pertinência, sendo que, a ausência de literatura sobre o mesmo, deve ser combatida pela comunidade científica.

Referências bibliográficas

Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. Discourse, Context & Media, 35, 100398. https://doi.org/10.1016/j.dcm.2020.100398

Associação Portuguesa de Apoio à Vítima (2023). Nova campanha de sensibilização: burlas românticas online. https://apav.pt/apav_v3/index.php/pt/3185-dia-europeu-da-vitima-de-crime-nova-campanha-de-sensibilizacao-2

Beals, M., DeLiema, M., & Deevy, M. (2015). Framework for a taxonomy of fraud. Financial Fraud Research Center.

Bilz, A., Johnson, G. I. & Shepherd, L. A. (2023). Tainted Love: A Systematic Review of Online Romance Fraud. https://doi.org/10.48550/arXiv.2303.00070

Buchanan, T., & Whitty, M. (2014). The online dating romance scam: Causes and consequences of victimhood. Psychology, Crime and Law, 20(3), 261–283. https://doi.org/10.1080/1068316X.2013.772180

Button, M., & Cross, C. (2017). Cyber Frauds, Scams and Their Victims. Taylor & Francis Group.

Chang, J. (2008). An analysis of advance fee fraud on the internet. Journal of Financial Crime, 15(1), 71–81. https://doi.org/10.1108/13590790810841716

Citizens Advice Bureau (2002-2011). Fraud on the internet. Citizens Advice. https://www.citizensadvice.org.uk/Global/Migrated_Documents/adviceguide/i-fraud-on-the-internet.pdf

Cross, C., & Blackshaw, D. (2014). Improving the Police Response to Online Fraud. Policing, 9(2), 119–128. https://doi.org/10.1093/police/pau044

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. Trends and issues in crime and criminal justice, 474, 1-6.

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding Romance fraud: Insights from domestic violence research. British Journal of Criminology, 58(6), 1303–1322. https://doi.org/10.1093/bjc/azy005

Cross, C. (2020). Romance Fraud. In T. J. Holt, A. M. Bossler (eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 917–937). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_41

Cross, C. & Holt, T. J. (2021). The Use of Military Profiles in Romance Fraud Schemes, Victims & Offenders, 16(3), 385-406. https://doi.org/10.1080/15564886.2020.1850582

Dias, V. (2012). Investigação do Cibercrime. Data Venia, 1, 63-88.

Fraud Act (2006). UK Public General Acts. nº35. https://www.legislation.gov.uk/ukpga/2006/35/contents

Furnell, S. M. (2001). Categorising cybercrime and cybercriminals: The problem and potential approaches. Journal of Information Warfare, 1(2), 35–44. https://www.jstor.org/stable/26486092

Furnell, S. (2003). Cybercrime: Vandalizing the Information Society. In J.M.C. Lovelle, B.M.G. Rodríguez, L. J. Aguilar, J.E.L. Gayo, M.P.P. Ruiz (Eds.). Lecture Notes in Computer Science. Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45068-8_2

Gillespie, A. A. (2021). Just the money? Does the criminal law appropriately tackle romance frauds? Journal of International and Comparative Law, 8, 143-174.

Jammalamadaka, S. C., Mehrotra, S., Venkatasubramanian, N. (2005, November 21). StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability [Conference session]. CCS05: 12th ACM Conference on Computer and Communications Security 2005. Fairfax VA USA. https://doi.org/10.1145/1103780.1103799

Lea, S., Fischer, P., & Evans, K. (2009). The psychology of scams: Provoking and committing errors of judgement. The Office of Fair Trading. https://webarchive.nationalarchives.gov.uk/ukgwa/20140402132426/http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

Morris, F. (Director). (2022). The Tinder Swindler [O Impostor do Tinder]. [Film]. Raw TV.

Onyebadi, U., & Park, J. (2012). 'I'm Sister Maria. Please help me': A lexical study of 4-1-9 international advance fee fraud email communications. The International Communication Gazette, 74(2), 181–199. https://doi.org/10.1177/1748048511432602

Rege, A (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. International Journal of Cyber Criminology. 3. 974-2891.

Rodrigues, Silva – Direito Penal Especial, Direito Penal Informático-Digital, Coimbra, 2009.

Sieber, U. (1998). Legal aspects of computer-related crime in the information society–Comcrime-study. European Commission.

Wall, D. (Ed.). (2003). Crime and the Internet. Routledge.

Whitty, M. T. (2013). The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam. British Journal of Criminology, 53(4), 665–684. https://doi.org/10.1093/bjc/azt009

Whitty, M. T. (2018). Do You Love Me? Psychological Characteristics of Romance Scam Victims. Cyberpsychology, Behavior, and Social Networking, 21(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Yar, M. (2016). Online Crime. In Pontell, H. (Ed.). Oxford research encyclopedia of criminology and criminal justice. Oxford: Oxford University Press.

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society. SAGE Publications Ltd.


Dizem que o amor é cego. Ainda bem que já abri os olhos.
Não entregue
Esta mensagem não chegou ao perfil falso que roubou o dinheiro e amor da Maria.
Mas ela ainda pode ter a última palavra.
Se foi vítima de burla romântica online fale com a APAV
Linha Internet Segura
800 219 090
APAV
associação portuguesa de Apoio à Vítima
Centro Internet Segura
Co-financiado pela União Europeia
CNCS Centro Nacional de Cibersegurança PORTUGAL
REPÚBLICA PORTUGUESA EDUCAÇÃO
ipdj
FCT Fundação para a Ciência e a Tecnologia
Computação Científica Nacional FCCN
APAV Apoio à Vítima
altice fundação
Microsoft

03.

RANSOMWARE: A EMERGÊNCIA DE UMA NOVA FORMA DE COMETER CRIMES

GABRIEL AFONSO, MANUEL MARTINS, DUARTE GOMES,
MARIA JOÃO PEREIRA, SAMUEL MOREIRA E INÊS GUEDES

Introdução

É amplamente reconhecido que a Internet tem sido um agente crucial de mudança na sociedade. Se usada corretamente, numa aceção normativa, pode, por exemplo, aumentar a produtividade e melhorar a qualidade de vida dos cidadãos (Oreku & Mtenzi, 2017). Esta surgiu num meio militar, originalmente denominada por Ethernet, tendo evoluído para uma "rede de redes" que conecta praticamente todo o mundo.

Efetivamente, a utilização da Internet foi uma das dimensões da vida quotidiana que mais cresceu em tão curto espaço de tempo. Por conseguinte, a vida em sociedade e as estruturas que suportam o normal funcionamento dos Estados foram, em grande medida, transferidas para o ciberespaço (Guedes *et al.*, 2021, p. 3). Neste âmbito, é fundamental mencionar o papel importantíssimo que a Internet desempenha no auxílio à resolução dos mais diversos problemas, contudo, aportou, também, diversos riscos que comprometem a segurança dos indivíduos, bens e serviços, a economia dos países, e a segurança nacional e internacional. Tal trouxe diversos desafios, designadamente ao nível da regulação do fenómeno (Guedes *et al.*, 2021).

Neste sentido, o incremento da utilização da Internet e a transferência de muitas atividades rotineiras para o ciberespaço, sobretudo a partir dos anos 90 do século XX, desencadearam o desenvolvimento do que muitos autores assinalam como o "cibercrime" (Guedes *et al.*, 2021, p. 5). Um dos cibercrimes que mais se tem destacado é o *Ransomware*. Verifica-se uma tendência crescente desta ciberofensa, tendo sido, em 2022, uma das ciberameaças mais relevantes em Portugal. Prevê-se ainda que, no próximo Relatório de Cibersegurança, relativo ao ano de 2023, se registe um aumento da relevância do *Ransomware* (Centro Nacional de Cibersegurança, 2023). Este fenómeno tende a afetar, maioritariamente, organizações, e os ganhos financeiros revelam-se como o principal objetivo destes ataques, impulsionando continuamente a criação e disseminação do mesmo. Assim, dada a sua tendência de proeminência na atualidade, urge reforçar os esforços para a consciencialização e prevenção do *Ransomware*.

O presente artigo tem como objetivo explicitar as dinâmicas características do *Ransomware*, bem como refletir acerca da legislação vigente relativa a este fenómeno. Inicialmente, iremos enquadrar brevemente no âmbito do cibercrime, incidindo, posteriormente, na temática do *Ransomware*, aludindo ao seu *modus operandi* e à relevância das vítimas e dos ofensores neste processo. Finalmente, será apresentada uma breve reflexão relativamente ao enquadramento legal deste fenómeno e, de seguida, será efetuada uma breve conclusão.

Cibercrime

Diversas têm sido as definições de cibercrime avançadas pelos estudiosos. Pese embora isso, entre as mesmas é comum a ideia de que os cibercrimes são atos ilegais em que o ofensor utiliza um conhecimento especial do ciberespaço para a sua prática (*e.g.* Furnell, 2002, p. 21, *cit in* Guedes *et al.*, 2021). Para Wall (2003), o termo cibercrime não significa mais do que um comportamento danoso que se encontra, de alguma forma, relacionado com um computador. De acordo com Oreku e Mtenzi (2017), o cibercrime pode ser definido como uma atividade criminosa em que computadores ou redes informáticas são uma ferramenta, um alvo ou um local de atividade criminosa, ou, ainda, pode ser definido como a utilização de sistemas e tecnologias de informação para cometer furtos, extorsões, roubos de identidade, fraudes e, em alguns casos, espionagem corporativa.

O cibercrime acaba, assim, por refletir as desvantagens dos avanços tecnológicos, ou seja, as oportunidades criminais decorrentes da evolução da Internet. Comporta não tanto a um único tipo

de atividade criminal, mas a um conjunto diverso de atividades ilegais que têm em comum o ambiente eletrónico único ("ciberespaço") em que ocorrem. É um fenómeno com um crescimento exponencial, sem precedentes, e onde importa perceber até que ponto é possível os indivíduos se protegerem deste tipo de crime (Guedes *et al.*, 2021, p. 4). Além das dificuldades de definição, igualmente difícil se torna descrever as tipologias dos diferentes atos ilegais cometidos com recurso ao uso de tecnologias. Não obstante, têm sido desenvolvidos esforços nesse sentido. Uma das distinções mais comuns é a realizada por Furnell (2002), que distingue as ofensas focadas no computador, aquelas que têm como alvo a própria infaestrutura eletrónica (*hardware* e *software*) que compreende o tecido da própria Internet, ou seja, crimes que surgem do desenvolvimento tecnológico, e as ofensas assistidas por computador, aquelas que pré-datam a tecnologia ou a existência da Internet, ou seja, já existiam, mas que encontram uma nova vida *online*. É amplamente reconhecido que as características da cibercriminalidade incrementam os desafios à sua medição, assim como à atuação dos diferentes atores do sistema de controlo social formal (Dias, 2012). Desde logo, o cibercrime é um fenómeno altamente transnacional, ou seja, não se cinge às fronteiras de um determinado país. A cibercriminalidade é "terra de ninguém, terra de todos, num tempo de todos, e num tempo de ninguém" (Rodrigues, 2009, *cit in* Dias, 2012). O lugar onde o infrator cometeu o crime, na maioria das situações, é diferente do local onde este terá consumação, isto é, onde os resultados serão produzidos. Além do mais, o cibercrime é um fenómeno atemporal, na medida em que a prática ou ação inicial raramente corresponde, no tempo, à materialização final do crime (Dias, 2012). Além disso, a cibercriminalidade encontra-se associada a uma deslocalização, isto porque a ação criminal deslocou-se do terreno (físico) para o ciberespaço, e a um anonimato do ofensor, dificultando o acesso ao mesmo, sendo este, na maioria das situações, dificilmente identificado pelas autoridades competentes (Dias, 2012). Importa ainda referir que, continuamente, se encontram novas formas de executar crimes cibernéticos, sendo o cibercrime um fenómeno em constante atualização, que exige, para a prática de determinados crimes, uma elevada tecnicidade e competências específicas por parte do ofensor (Dias, 2012). Efetuado este enquadramento no âmbito do cibercrime, o presente artigo irá de seguida versar, mais concretamente, sobre o *Ransomware*.

Ransomware

O *Ransomware* deriva da aglutinação das palavras "*ransom*", "resgate" na tradução para o português, e "*software*", "código/programa" em português. Desde logo, o nome sugere, assim, a peculiaridade de a sua atuação ocorrer em dispositivos informáticos (Saisse, 2016). O *Ransomware* consiste, portanto, num tipo de *software* malicioso, ou *malware*, que ameaça uma vítima ao bloquear o acesso a dados ou elementos essenciais ao funcionamento de um determinado computador ou outro dispositivo eletrónico pessoal (Zetter, 2017). Para as vítimas recuperarem os seus dados, é-lhes exigido que paguem uma quantia monetária (Aurangzeb *et al*, 2017). Normalmente, os ofensores informam as vítimas de que um conjunto de dados foram encriptados, através de um *e-mail*, anúncios ("*pop-up´s*") ou de uma mensagem, solicitando o pagamento de uma determinada quantia para que o acesso seja restabelecido (Luo & Liao, 2007). As mensagens contêm informações relativas à quantia monetária a pagar, ao método de pagamento e ao método de recuperação (comummente, a *password* necessária para o acesso), após o pagamento ser realizado (Luo & Liao, 2007). Muitas vítimas acabam por ceder ao pedido dos ofensores, pagando a quantia exigida, pois pretendem salvaguardar dados importantes, para os quais não possuem qualquer cópia de segurança (Aurangzeb *et al.*, 2017). Desde a década de 80 que a extorsão de dinheiro através de ciberataques é registada, sendo o primeiro ataque por *Ransomware* reportado em 1989, utilizando um programa denominado AIDS Trojan (Aleem & Islam, 2017). Cada vez mais, com a evolução dos meios digitais, o ciberespaço tem-se tornado um potencial meio para a realização de crimes desta natureza, em que a obtenção de lucro constitui o objetivo máximo.
Os ataques por *Ransomware* podem não ser algo totalmente novo, no entanto, os últimos anos observaram um crescimento exponencial dos mesmos. Um relatório da Symantec aponta um aumento de 113%, em 2014, tendo a modalidade do *Ransomware* criptográfico sido a de maior crescimento. De um idêntico, a Europol alerta para o crescimento deste tipo de ataques em 2015 (Zahra & Shah, 2017). Já em 2016, a vitimação por *Ransomware* aumentou 3500% comparativamente a 2015, tendo existido um pagamento de 209 milhões de dólares por parte das vítimas nos primeiros meses de 2016 (Aurangzeb *et al.*, 2017). Efetivamente, a obtenção de lucro afirma-se como a maior motivação para a ampla disseminação do *Ransomware* (Indu & Sharma, 2018). De acordo com estatísticas da Homeland Security, desde 2016, ocorreram cerca de 1,5 milhões de ataques de *Ransomware* por ano (Ozer *et al.*, 2019), sendo que, relativamente aos ganhos, estima-se que os cibercriminosos tenham auferido um valor de mil milhões de dólares, em 2019, provenientes desses ataques. Estimava-se que esse valor, até 2021, pudesse atingir os 6 triliões de dólares em todo o mundo (Ozer *et al.*, 2019).
Consensualmente, os estudos têm dividido o *Ransomware* em dois tipos: o *Crypto Ransomware* (ou "*data locker*"), que consiste no bloqueio de ficheiros ou

dados, socorrendo-se, geralmente, do uso de criptografia, podendo ser disseminado através de *e-mails* ou *links*; e o *Locker Ransomware* (ou "*computer locker*") que se traduz no bloqueio do computador ou dispositivo através do controlo de dispositivos essenciais para a funcionalidade do mesmo, tais como teclado, monitor, entre outros (Savage, Coogan & Lau, 2015). É também identificada, ainda que de forma menos consensual, a existência de um terceiro tipo de *Ransomware*, o chamado "*scareware*". Este, ao contrário dos já enunciados, não apresenta em si próprio um perigo para as potenciais vítimas, mas procura assustá-las, ao ponto de estas pagarem, seja ao fazer-se passar por outra entidade credível, ou ameaçando divulgar ficheiros (Kok *et al.*, 2019). Tal pode ser concretizado através de *e-mails* ou de anúncios, os "*pop-ups*" (Beaman *et al.*, 2021).

Modus Operandi

Um ataque por *Ransomware* não se concretiza num momento único, obedece a um protocolo, isto é, trata-se de um processo faseado, em que cada uma das fases surge no seguimento da anterior, até ao culminar do processo, com o pedido de resgate. Segundo Liska e Gallo (2016), existe uma sequência cronológica para que o crime ocorra, sendo as fases definidas como implantação, instalação, comando e controlo, destruição e extorsão.
A implantação corresponde ao início do ataque, onde os componentes utilizados para infetar o sistema informático são acolhidos por este. Esta receção pode ocorrer por diversas formas: o ofensor pode, recorrendo a estratégias de engenharia social, solicitar esse mesmo acesso; através do acesso, pela vítima, a *sites* comprometidos, sem esta perceber; por *phishing* ou mesmo através da exploração de vulnerabilidades em sistemas informáticos acessíveis pela Internet (Aurangzeb *et al.*, 2017). Concluído o carregamento do arquivo malicioso, inicia-se a instalação, onde o código lançado no sistema vai comunicar com o sistema em uso pelos ofensores iniciando a instalação do *Ransomware*, podendo estas técnicas serem aprimoradas conforme o alvo que se pretende atingir. Instalado o *Ransomware*, este opera em silêncio, identificando e encaminhando para os ofensores uma quantidade volumosa de informação, perante a qual os ofensores decidem sobre o quão valioso é o alvo, fazendo depender dessa avaliação o valor do resgate a pedir, sendo esta a fase de comando e controlo. Já na fase da destruição dá-se início ao processo de criptografar arquivos, documentos, dados valiosos para os utilizadores, bloqueando-lhes o acesso. Executados estes passos, é iniciado o contacto com as vítimas, estamos na fase da extorsão. Normalmente, as vítimas, ao tentarem aceder ao sistema informático, deparam-se com uma mensagem a informar sobre o ocorrido, assim como com instruções sobre a forma de reverter o problema, o que, na esmagadora maioria dos casos, se concretiza no pagamento de uma quantia monetária.
De um modo idêntico, Tandon e Nayyar (2019) definem cinco fases no protocolo de um ataque por *Ransomware*.
A instalação do *software* malicioso, equivalente à fase de implantação.
O contacto com o servidor de comando e controlo, em tudo equivalente à terceira fase para Liska e Gallo (2016).
Na terceira fase, a troca de chaves (*handshake*), uma troca de informações sobre o sistema infetado, entre o código malicioso e o servidor dos ofensores, correspondente à fase de instalação projetada em Liska e Gallo (2016).
A codificação é o passo seguinte, semelhante à fase de destruição, onde os dados são encriptados ou é bloqueado o acesso ao sistema informático da vítima.
Por último, a extorsão, fase comum a ambos os estudos. Aqui, os arquivos codificados só podem ser recuperados através de uma chave privada, acessível apenas após o pagamento do resgate, normalmente em criptomoedas. Com efeito, os ciberofensores encontram-se em permanente evolução no que diz respeito ao pagamento (Aurangzeb *et al.*, 2017). Mais recentemente, este tem sido exigido em criptomoedas, moedas eletrónicas, ou *Bitcoins*, sendo atualmente o método de pagamento mais utilizado para tal (Aurangzeb *et al.*, 2017). Este método, em uso desde 2008, dificulta a localização do ofensor, permitindo a manutenção do seu anonimato e a perpetuação dos atos criminais, pela dificuldade na sua deteção (Richardson & North, 2017). Além deste, Paypal ou MoneyPak são exemplos de outras plataformas usadas (Richardson & North, 2017).

Vítimas e processo de tomada de decisão

No que concerne às vítimas de *Ransomware*, devemos atentar ao facto de que a maioria dos ataques costumava ser direcionada a utilizadores individuais. Contudo, mais recentemente, o *Ransomware* cujo alvo são organizações tornou-se a maior ameaça (Europol, 2021). Podemos, assim, classificar as vítimas em dois grupos: utilizadores domésticos individuais e entidades empresariais, estes últimos os alvos mais lucrativos (Atapour-Abarghouei *et al.*, 2019). Inicialmente, os ataques de *Ransomware* eram pouco direcionados, ocorriam sob a forma de disseminação pela Internet, tentando encontrar o alvo mais adequado, uma abordagem denominada de "*spray and pray*" (Wall, 2021). Mais recentemente, e sob a premissa da obtenção do maior lucro possível, os ataques são mais direcionados a organizações, designadamente nos setores da construção civil, tecnologias de informação, educação e saúde (Atapour-Abarghouei *et al.*, 2019). Por força das diferenças entre ambos os grupos, o comportamento do *Ransomware* que visa cada um deles é igualmente distinto. Os ataques que visam utilizadores individuais ou domésticos são oportunistas, perpetrados através de vetores de ataque indiscriminados (e.g., um *e-mail* de *spam*,

MAL ME QUER

“ERA UM CICLO VICIOSO: ORA PARECIA MUITO BOM, ORA ERA MUITO MAU.”

MANIPULAR ME QUER

CHAMADA GRATUITA
116 006
LINHA DE APOIO À VÍTIMA
DIAS ÚTEIS DAS 08H-23H

APAV®
associação portuguesa de
Apoio à Vítima

Se és vítima de violência no namoro, ou conheces alguém que seja, fala com a APAV.

no qual a potencial vítima é incentivada a clicar num *link* malicioso ou visitar um *site* comprometido), sendo os valores de resgate solicitados consideravelmente menores, mas com um número de vítimas muito superior. Ao nível individual, fatores como a idade, o nível de educação e os recursos financeiros são identificados como fatores que aumentam a probabilidade de um indivíduo ser vítima de um ataque de *Ransomware* e, subsequentemente, pagar o resgate. Não obstante, o nível de conhecimentos informáticos é apontado como um fator particularmente determinante. Soluções simples, como atualizações regulares de *software* e sistema operativo, segurança de *e-mails*, ferramentas *anti-malware* e *backup* dos dados, podem reduzir significativamente o número de ataques bem-sucedidos (Atapour-Abarghouei *et al.*, 2019).
Não obstante o acesso das grandes empresas a tecnologias de informação e a profissionais de cibersegurança, estas são regularmente vítimas de ataques por *Ransomware*, ataques estes mais direcionados, a chamada "caça grossa" (Atapour-Abarghouei *et al.*, 2019). Falamos de variantes de *Ransomware* graduais e secretas, que se concentram em evitar e escapar às contramedidas implementadas pelos especialistas em segurança, que lentamente assumem o controlo dos dados especificamente visados. Nestas situações, os valores de resgate são normalmente elevados. Os sistemas de segurança, o tipo de dados e os serviços com os quais estas empresas se relacionam, são os principais fatores de vitimação (Atapour-Abarghouei *et al.*, 2019). A prevenção afigura-se como a melhor solução. Um sistema robusto de *backup* e arquivamento de dados, boas ferramentas *anti-malware*, introduzir políticas de acesso e monitorização de terceiros, que possam constituir uma vulnerabilidade nos sistemas, acompanhada de um uso consciente das tecnologias, já que uma grande maioria dos ataques bem-sucedidos se devem a erros humanos, podem constituir elementos preventivos eficazes (Atapour-Abarghouei *et al.*, 2019).
Analise-se, agora, o processo de tomada de decisão típico das vítimas perante um ataque de *Ransomware*, no que concerne ao pagamento, ou não, do resgate. De acordo com Nichu (2021, *cit in* Connolly & Borrion, 2022), em 2020, 52% das vítimas de ataques de *Ransomware* pagaram o resgate solicitado. O poder dos infratores reside na pretensão da vítima em recuperar os seus dados, na probabilidade de destruição dos dados se o resgate não for pago e no compromisso da sua devolução após a vítima pagar o resgate (Connolly & Borrion, 2022).
Connolly e Borrion (2022) analisaram 41 ataques por *Ransomware*, entre 2014 e 2018, cujos alvos foram organizações, públicas e privadas, relativamente às consequências diversas que o ataque poderia ter para as organizações e a decisão destas pagarem, ou não, o resgate. Os participantes reconheceram que *backups* eficazes, uma estratégia clara de resposta a incidentes e uma visibilidade total da qualidade dos sistemas infetados e da rede são fatores importantes, contribuindo para a decisão de não pagar o resgate. Acresce o elevado valor do resgate, o perigo de vitimação secundária, a necessidade de recorrer a empréstimos, sobretudo por parte de pequenas empresas, para pagar o resgate, dificultando a sua situação financeira, e a etiquetagem da empresa como um alvo fácil, caso acedessem ao pagamento. Ademais, organizações que não possuam o devido conhecimento e real dimensão dos dados com que trabalham, estarão mais inclinadas a pagar o resgate exigido.
Nas organizações privadas, o risco de falência, como um resultado realista da perda de dados, conduz ao pagamento do resgate (Connolly & Borrion, 2022). O receio de uma possível incriminação por permitir o furto e/ou divulgação de dados confidenciais, o desejo em manter o ataque sofrido no anonimato e o sentimento de que, de alguma forma, são responsáveis pelo ataque, são igualmente apontados como fatores potenciadores do pagamento (Connolly & Borrion, 2022). O reduzido impacto que a destruição dos dados provocaria no funcionamento da empresa, por sua vez, foi a principal razão indicada para o não pagamento do resgate (Connolly & Borrion, 2022).

Perfil de Ofensores

As discussões sobre o cibercrime são frequentemente influenciadas por estereótipos. Por um lado, a imagem de um *hacker* solitário desmente a natureza coletiva de grande parte do crime cibernético e, por outro lado, as definições convencionais de crime organizado cibernético tendem a estar desatualizadas, tendo sido ultrapassadas pelo próprio fenómeno (Broadhurst *et al.*, 2014). Para além disso, embora não comummente associados a ciberofensores, os Estados também são capazes de cometer ou patrocinar atos criminosos neste âmbito.
O cibercrime possui um caráter transnacional que proporciona aos cibercriminosos, quer os que operam a nível individual, quer em grupo, até mesmo grupos de crime organizado, um potencial para escapar às contramedidas de combate, mesmo quando estas são concebidas pelos atores mais capazes (Broadhurst *et al.*, 2014).
Embora alguns tipos de crimes cibernéticos exijam um elevado grau de organização, logo concretizados por grupos organizados, a tecnologia digital capacitou os indivíduos como nunca. Assim, por exemplo, adolescentes, individualmente, são capazes de desativar sistemas de controlo de tráfego aéreo, fechar retalhistas e manipular transações na bolsa de valores (Broadhurst *et al.*, 2014). É consensual, mesmo entre investigadores académicos, que os grupos convencionais de crime organizado estão cada vez mais envolvidos no crime digital. McGuire (2012, *cit in* Broadhurst *et al.*, 2014) sugere que até 80% do crime cibernético pode ser resultado de alguma forma de atividade organizada, em que os grupos tradicionais de crime organizado

estão a alargar as suas atividades ao mundo digital. Os pontos críticos do crime cibernético com ligações potenciais a grupos de crime organizado são particularmente encontrados em países da antiga União Soviética. EUA, Roménia e China são outros países em destaque, tendo a Roménia, na pequena cidade de Râmnicu Vâlcea, um dos maiores centros de cibercrime, onde se localizam diferentes grupos de *hackers* (Broadhurst *et al.*, 2014).

McGuire (2012, *cit in* Broadhurst *et al.*, 2014) sugere uma tipologia de grupos orientados para crimes cibernéticos, com tendência a alterar-se à medida que o ambiente digital evolui. O grupo tipo I, opera essencialmente *online* e subdivide-se em "enxames", que compartilham características das redes, com propósito comum, mas sem liderança, e em *hubs*, também eles ativos *online*, com maior organização e estrutura de comando clara. O grupo tipo II, combina ofensores *online* e *offline*, os "híbridos", divididos em "híbrido agrupados", onde a ofensa é articulada em torno de um pequeno grupo de indivíduos, com atividade e método específico, e em "híbrido estendido", que opera de forma menos centralizada, muito associado, e diversidade de atividades criminosas. O grupo tipo III, opera essencialmente *offline*, usando, no entanto, tecnologia *online* para facilitar a sua atividade. Subdivide-se em "hierarquias", grupos criminosos tradicionais, mas que podem usar novas tecnologias para auxiliar a atividade, e em "agregados", pouco organizados, temporários e muitas vezes sem um propósito claro.

Segundo Wall (2021), os grupos mais prolíficos, entre janeiro de 2019 e maio de 2021, foram o Conti (RYUK), o MAZE e o REvil, com mais de 900 organizações atacadas pelos três. Os infratores individuais são normalmente jovens, com motivações diversas, desde ideológicas e financeiras, até de perseguição, retaliação e desejo de reconhecimento e fama.

Enquadramento Legal

Como visto anteriormente, um ataque por *Ransomware* não se concretiza num momento único, obedece a um protocolo de atuação, um *modus operandi*. Apenas com o preenchimento sequencial de cada uma das fases poderemos afirmar a presença de um ataque por *Ransomware* e, dessa forma, ver consumado o crime. Um ataque malicioso a um sistema informático com a finalidade última de obter informações confidenciais, mas que não bloqueia o acesso a dados e/ou ao próprio sistema, que não exige o pagamento de resgate para desbloquear os dados, não configura um ataque por *Ransomware*, não deixando, contudo, de constituir um ilícito criminal (Masseno & Wendt, 2017). Sendo uma prática disseminada mundialmente, há relativamente pouco tempo, o *Ransomware* não está tipificado "*qua tale*", sendo essa necessidade objeto de debate no âmbito da política legislativa (Masseno & Wendt, 2017). A exceção reside nos EUA, mais concretamente nos estados do Wyoming e da Califórnia, onde a previsão penal caracteriza o *Ransomware* autonomamente (Masseno & Wendt, 2017).

Em Portugal, a nível legislativo, a previsão legal das diferentes fases do *Ransomware* dispersa-se pela Lei do Cibercrime, pelo Regime Geral de Proteção de Dados (RGPD), assim como pelo artigo 158.º do Código Penal, onde se encontra plasmado o crime de extorsão. Assim, e no que respeita ao acesso ao sistema informático, vemos configurado um acesso ilegítimo, previsto no Art.º 6.º da Lei do Cibercrime, sendo o bem jurídico a proteger a segurança da disponibilidade exclusiva do sistema informático pelo seu titular. Porém, em grande parte dos casos, daríamos por preenchido um diferente tipo legal, o crime de acesso indevido, p.p. Art.º 47.º do RGPD, onde o bem jurídico a proteger, diferentemente, é a privacidade e autodeterminação informacional. Esta diferenciação reside no facto de a maioria dos sistemas informáticos conterem dados pessoais, logo de maior aplicação do RGPD. Pode ainda o acesso ser obtido através de *phishing*, caindo já para um distinto tipo legal, o previsto no Art.º 3.º da Lei do Cibercrime, a que corresponde o crime de falsidade informática, protegendo já diferente bem jurídico, a preservação da confiança no tráfego jurídico, entendendo a jurisprudência, embora com reservas da Doutrina, um crime cuja prática consubstancia um concurso real com um outro tipo legal, a burla informática e nas comunicações, dado preencher ambos os tipos, mas protegerem bens jurídicos diversos e autónomos (Ac. TRP). Ao tornar os dados inacessíveis, fica preenchido o tipo legal do crime de sabotagem informática, p.p. pelo Art.º 5.º da Lei do Cibercrime, protegendo desta feita bens privados, património, disponibilidade do sistema informático pelo titular, mas também bens públicos como a continuidade da vida em sociedade, seguindo ao encontro do disposto no Art.º 6.º da Convenção de Budapeste. Chegada a fase do pedido de resgate, encontram-se preenchidos os requisitos do crime de extorsão, p.p. pelo Art.º 223.º, do Código Penal, protegendo o bem jurídico património. Pode o crime assumir uma forma qualificada, atendendo ao valor do resgate solicitado ou às qualidades inerentes ao ofensor. Constata-se, assim, o diluir do crime de *Ransomware* por uma panóplia de previsões legais, atinentes a outros tipos de crime, não dispondo este de uma autonomia penal que, como é objeto de reflexão na conclusão, melhor atendesse ao dano que causa.

Relativamente ao quadro legal, constata-se uma ausência de tipificação do fenómeno, subjugando a sua verificação à prática de diversos outros crimes, culminando com a prática do crime de extorsão, sendo assim o autor, na maioria dos casos, punido pelo concurso real de crimes. Não podemos pensar num ataque de *Ransomware* como um momento fixo no tempo, mas sim como um processo que engloba um antes,

durante e depois, com o inerente espaço temporal decorrido.
Desta forma: atendendo à natureza semipública de alguns dos crimes que antecedem a extorsão digital e do consequente prazo de seis meses para formalizar queixa, converter a prática do *Ransomware* num tipo autónomo de crime, associado ao Art.º 223º, do C.P., mas diferenciando o recurso à tecnologia para a sua prática; agravando a moldura penal que o pune, dada a gravidade do dano causado; revestindo-o de natureza pública, deixando assim cair o prazo para queixa, não fosse descabido de validade, ganhando eficácia no combate e protegendo assim os direitos das vítimas, muitas vezes pessoas coletivas, mas que sofrem fortes impactos financeiros.

Conclusão

O *Ransomware* tem, nos últimos anos, evoluído em larga escala, evidenciando-se como uma atividade assente em componentes metodológicas específicas, direcionadas a vítimas, igualmente, específicas. Este fenómeno representa, por isso, uma ameaça significativa no atual cenário digital, comprometendo a segurança e a integridade de dados dos utilizadores, sejam estes individuais ou institucionais. São utilizadas técnicas avançadas de criptografia para bloquear o acesso a informações essenciais, exigindo, *a posteriori*, uma quantia monetária de resgate para reaver os dados bloqueados.
O impacto é significativo, não se circunscrevendo meramente aos danos financeiros, incluindo, igualmente, impactos na reputação e confiança do público na organização afetada. Considerando que, habitualmente, os pagamentos são realizados em criptomoeda, mais concretamente, *Bitcoin*, e que mais de 50 % dos ataques são direcionados a agências governamentais e empresas de pequena e média dimensão, com políticas de ocultação dos ataques (Ozer *et al.*, 2019), um esforço conjunto entre entidades, com rastreio das transações de *Bitcoin* e seguimento até ao endereço onde ocorre o levantamento da moeda, talvez, viesse produzir melhores efeitos na descoberta e consequente responsabilização dos infratores (Ozer *et al.*, 2019).
Ao nível da prevenção, o fator humano é preponderante. Assim, uma estratégia sólida de *backup* e restauração de sistemas, por si só, já não são suficientes para garantir segurança, pois os ofensores não se contentam simplesmente em criptografar sistemas, o "roubo" de dados é cada vez mais habitual, sendo estes utilizados para exercer uma extorsão secundária ou leiloados pelo mais alto valor na *dark web*.
Deste modo, importa o investimento em medidas preventivas, com atualizações regulares de *software*, soluções avançadas de segurança e uma cultura de segurança que abarque toda a organização.
Esta cultura deve começar no topo, com a compreensão, por parte dos responsáveis máximos, dos riscos cibernéticos, assumindo um compromisso de que tudo o que for possível realizar, será efetivamente realizado, com vista a proteger a organização e os seus clientes.

Referências bibliográficas

Acórdão Tribunal Relação do Porto, Proc. 2177/09.0 PAVNG. P1, de 14 SET 2016.

Atapour-Abarghouei, A., Bonner, S., & McGough, A. S. (2019). Volenti non fit injuria: Ransomware and its Victims. In 2019 IEEE International Conference on Big Data (pp. 4701-4707). IEEE.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. An analysis of the nature of groups engaged in cybercrime, International Journal of Cyber Criminology, 8(1), 1-20.

CNCS. (2023). Relatório Cibersegurança em Portugal - Riscos & Conflitos (4. ed.). Observatório de Cibersegurança. Centro Nacional de Cibersegurança.

Connolly, A. Y., & Borrion, H. (2022). Reducing ransomware crime: analysis of victim´s payment decisions. Computers & Security, 119, 102760.

Dias, V. (2012). Investigação do Cibercrime. Data Venia, 1, 63-88.

Europol (2021). European Union Serious and Organized Crime Threat Assessment. A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organized Crime. Publications Office of the European Union, Luxembourg.

Furnell, S. (2002). Cybercrime: vandalizing the information society. In International conference on web engineering (pp. 8-16). Berlin, Heidelberg: Springer Berlin Heidelberg.

Guedes, I. S., Moreira, S., & Cardoso, C. (2021) – "Cibercrime: Conceptualização, Desafios e Perceções Públicas", in Cibercriminalidade: novos desafios, ofensas e soluções. Lisboa: PACTOR – Edições de Ciências Sociais, Forenses e da Educação.

Indu, R., & Sharma, A. (2018). Ransomware: A New Era of Digital Terrorism. Computer, 1(02).

Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm. Computers, 8(4), 79. https://doi.org/10.3390/computers8040079

Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro.

Liska, A., & Gallo, T. (2016). Ransomware: Defending against digital extortion. "O'Reilly Media, Inc.".

Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. Information Systems Security, 16(4), 195–202. https://doi.org/10.1080/10658980701576412

Masseno, M. D., & Wendt, E. (2017). O ransomware na Lei: apontamentos breves de Direito Português e Brasileiro. Revista Eletrônica Direito & TI, 1(8), 13-13.

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. Iet Networks, 7(5), 321-327.

Oreku, G. S., & Mtenzi, F. J. (2017). Cybercrime: Concerns, challenges and opportunities. Information Fusion for Cyber-Security Analytics, 129-153.

Ozer, M., Varlioglu, S., Gonen, B., & Bastug, M. (2019). A prevention and a traction system for ransomware attacks. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 150-154). IEEE.

Regime Geral de Proteção de Dados (RGPD) - Lei n.º 58/2019, de 08 de agosto.

Richardson, R., & North, M., (2017). "Ransomware: Evolution, Mitigation and Prevention". Faculty Publications. 4276.

Saisse, R. C. (2016). Ransomware. Revista Eletrônica Direito & TI, 1(6), 14-14.

Savage, K., Coogan, P., & Lau, H. (2015). The Evolution of Ransomware.

Tandon, A., & Nayyar, A. (2019). A comprehensive survey on ransomware attack: A growing havoc cyberthreat. Data Management, Analytics and Innovation: Proceedings of ICDMAI 2018, Volume 2, 403-420.

Wall, D. (Ed.). (2003). Crime and the Internet. Routledge.

Wall, D. (2021). The Transnational Cybercrime Extortion Landscape and The Pandemic: Ransomware and changes in offender tactics, attack scalability and the organization of offending. European Law Enforcement Research Bulletin.

Zahra, A., & Shah, M. A. (2017, September). IoT based ransomware growth rate evaluation and detection using command and control blacklisting. In 2017 International Conference on Automation and Computing (ICAC) (pp. 1-6). IEEE.

Zetter, K. (2017). What is ransomware? A Guide to the Global Cyberattack's Scary Method. Wired.

04.

COMBATE AO TERRORISMO: REPRESSÃO, PREVENÇÃO E PROTECÇÃO

CARLOS PINTO DE ABREU
E GIL NEVES VILELA*

Introdução

Os últimos atentados terroristas ocorridos em Portugal remontam às décadas de 70 e 80 do século passado – uns levados a cabo por organizações portuguesas, nomeadamente o MDLP e as FP-25, e outros por grupos de cariz internacional, de que foi exemplo o Armenian Secret Army for the Liberation of Armenia, responsável pelo ataque à embaixada da Turquia em Lisboa, do qual resultaram várias mortes.
Já em finais do século XX e inícios do século XXI, o terrorismo adquiriu uma dimensão global e um mediatismo exacerbado até aí nunca atingido, em virtude do surgimento e actuação de grupos fundamentalistas e organizações terroristas como a Al-Qaeda e o Estado Islâmico (ISIS). Os atentados de 11 de Setembro de 2001 despertaram os povos, governos e instituições europeias para a urgência de fortalecer os mecanismos de cooperação internacional no combate ao terrorismo.
Ciente de que o objectivo de impedir a actividade terrorista depende de uma acção inteligente e coordenada entre os Estados-Membros, a União Europeia tem vindo a aprofundar, ao longo das últimas décadas, a tutela dos cidadãos e o combate destes crimes, adoptando inúmeras medidas relativas à prevenção e à repressão do terrorismo, bem como à protecção e salvaguarda das vítimas.
Refira-se que os Estados-Membros, incluindo Portugal, estão obrigados, por força dos Tratados, a aplicar e transpor para as respectivas ordens jurídicas as normas emanadas pelo Parlamento e Conselho Europeu. Nesta senda, aborda-se a resposta legislativa dada pela União Europeia e por Portugal aos perigos graves e danos irreparáveis do terrorismo.
Para este efeito, apresentamos de forma sucinta o enquadramento legal das medidas de repressão do terrorismo, das estratégias de prevenção desses crimes e da protecção dada às vítimas de actos terroristas.

Repressão

No âmbito do Direito da União Europeia, o principal instrumento de luta contra o terrorismo começou por ser a Decisão-Quadro 2002/475/JAI, do Conselho, de 13 de Junho de 2002, cuja primeira finalidade foi a criação de um regime jurídico comum a todos os Estados-Membros e estabelecer uma definição harmonizada das infracções terroristas, convocando a aproximação das legislações nacionais, sendo que esta Decisão-Quadro 2002/475/JAI foi já revogada. Entretanto foi aprovada e entrou em vigor a Directiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de Março de 2017, relativa à luta contra o terrorismo, que substituiu a Decisão-Quadro 2002/475/JAI do Conselho e alterou a Decisão 2005/671/JAI do Conselho.
Inicialmente, no ordenamento jurídico português, os crimes de terrorismo tinham a sua consagração em dois artigos: o artigo 300.º, relativo às organizações terroristas, e o artigo 301.º sob a epígrafe de "terrorismo", ambos do Código Penal.
Foi apenas em 2003 que, em resposta à aprovação da supra referida Decisão-Quadro de 2002, se procedeu a uma adaptação e alteração das normas jurídicas internas.
A transposição desse diploma concretizou-se, então, com a aprovação e entrada em vigor da Lei de Combate ao Terrorismo – Lei n.º 52/2003, de 22 de Agosto – que tem como objecto, nos termos do seu artigo 1.º, a previsão e a punição dos actos e organizações terroristas.
A Lei de Combate ao Terrorismo tem vindo a sofrer sucessivas alterações, mediante as quais se procedeu ao agravamento das penas, bem como ao alargamento do elenco de crimes de terrorismo. A Lei n.º 52/2003, de 22 de Agosto, foi alterada pela Lei n.º 16/2019, de 14 de Fevereiro, para passar a contemplar as exigências da Directiva 2017/541, e ainda pela mais recente Lei n.º 2/2023, de 16 de Janeiro.
Deste modo, a Lei de Combate ao Terrorismo, que criminaliza e pune a prática de actos terroristas com penas que podem chegar aos 25 anos de prisão, prevê, nos artigos 3.º e ss, a incriminação das organizações terroristas, dos actos terroristas em sentido próprio, do incitamento público à prática de actos terroristas, do acesso a mensagens de incitamento público à prática de actos terroristas, do treino para o terrorismo, do recrutamento para o terrorismo, da apologia

*Não adoptam o Acordo Ortográfico

pública da prática de actos terroristas, das deslocações para a prática de terrorismo e apoio a essas mesmas deslocações – seja deslocações para treino, para a prática de actos terroristas ou para adesão a organizações terroristas – e, ainda, do financiamento do terrorismo.

Prevenção

Actualmente, alguém que pretenda recrutar pessoas para uma organização terrorista, aliciando-as para a prática de actos terroristas, não está limitado aos seus contactos próximos e pessoais e ao meio social onde se insere. De facto, a disseminação da propaganda terrorista é hoje feita essencialmente pela *Internet* e pela *Darknet*– através da disseminação de vídeos, imagens, textos e gravações áudio com conteúdo violento e que incitam à violência. No caso do terrorismo jihadista, o alcance da sua máquina de propaganda vai muito para além das comunidades muçulmanas localizadas em determinados espaços geográficos. Assim, neste processo de radicalização e de recrutamento de pessoas para as organizações terroristas, podem, o recrutador e o recrutado – o fornecedor do conteúdo ou o difusor do conteúdo e o visualizador – estar em locais opostos do mundo, bastando que uns e outros tenham acesso à Internet. Aliás, são conhecidos vários casos de cidadãos portugueses que, mesmo sem terem qualquer ligação à comunidade muçulmana e ao radicalismo islâmico, decidiram abandonar o país para integrar as fileiras do autodenominado Estado Islâmico, situado numa zona da Síria. Citando Walter Laqueur, pode dizer-se que "*[the] success of a terrorist operation depends almost entirely on the amount of publicity it receives*".

Por isso, dada a inequívoca importância dos meios digitais no processo de expansão e de divulgação das acções violentas dos grupos terroristas, foi aprovado, em 29 de Abril de 2021, pelo Parlamento Europeu e pelo Conselho, um importante instrumento de prevenção do terrorismo – o Regulamento 2021/784, relativo ao combate à difusão de conteúdos em linha. Nos termos deste Regulamento, os Estados-Membros devem designar uma "autoridade competente" para procurar e identificar conteúdos e mensagens terroristas, bem como solicitar aos "prestadores de serviços de alojamento virtual" onde tais conteúdos e mensagens estão disponíveis – como o *Instagram*, o *TikTok*, ou o *Youtube* – a supressão dos mesmos ou o bloqueio do acesso a tais conteúdos. E, uma vez recebida a decisão de supressão, esses prestadores de serviços têm uma hora para acatar a decisão da autoridade nacional, sendo que, caso incumpram grave ou reiteradamente com esta obrigação, estão sujeitos ao pagamento de sanções pecuniárias. De modo a impedir uma eventual limitação injustificada do direito à liberdade de expressão e de informação, o Regulamento estabelece no seu artigo 1.º n.º 3 que "os materiais difundidos ao público para fins educativos, jornalísticos, artísticos, ou de investigação, ou para fins de prevenção ou combate ao terrorismo, incluindo os materiais que representem a expressão de opiniões polémicas ou controversas no quadro do debate público, não são considerados conteúdos terroristas". Em suma, com este Regulamento pretende-se que cada Estado-Membro designe uma autoridade nacional que identifique conteúdos terroristas, assegurando que, com a sua iniciativa, os mesmos sejam eliminados de forma rápida, reduzindo ao mínimo possível o número de pessoas com acesso a tais conteúdos.

Já no domínio da prevenção social, a 9 de Junho de 2020, a Comissão Europeia adoptou uma nova "Agenda de Luta contra o Terrorismo" com orientações relativas à prevenção, antecipação, protecção e resposta à ameaça terrorista, na qual propôs, entre outras medidas, a "promoção da inclusão e a criação de oportunidades através das políticas de educação, cultura, juventude e desporto", ou ainda o reforço da acção preventiva nas prisões, ao nível da reabilitação e reintegração de reclusos radicalizados, incluindo, e sobretudo, após a sua libertação.

Protecção das vítimas

Em matéria de protecção das vítimas de terrorismo, há a considerar a Directiva 2012/29/UE do Parlamento Europeu e do Conselho que define como vítima a "pessoa singular que tenha sofrido um dano, nomeadamente um dano físico, moral ou emocional, ou um prejuízo material diretamente causados por um crime" e também "os familiares de uma pessoa cuja morte tenha sido diretamente causada por um crime e que tenham sofrido um dano em consequência da morte dessa pessoa". Em Portugal, procedeu-se à transposição da referida Directiva através da aprovação do Estatuto da Vítima (Lei n.º 130/2015, de 4 de Setembro), que estabelece um conjunto de normas relativas aos direitos, ao apoio e à protecção das vítimas da criminalidade em geral.

O conceito de vítima, em Portugal, está corporizado no art.º 67.º-A do Código de Processo Penal. Com a Lei n.º 2/2023, de 16 de Janeiro, a redacção do n.º 3 do art.º 67.º-A passou a ser a seguinte: "as vítimas de criminalidade violenta, de criminalidade especialmente violenta e de terrorismo são sempre consideradas vítimas especialmente vulneráveis para efeitos do disposto na alínea b) do n.º 1". Nesse sentido, tornou-se inequívoco que as vítimas de terrorismo beneficiam do Estatuto de Vítima, incluindo dos direitos específicos previstos para vítimas especialmente vulneráveis, contemplados nos art.º 20.º e ss. da Lei n.º 130/2015, de 4 de Setembro.

De entre os vários apoios consagrados no Estatuto há a destacar:

i) o acesso da vítima, assegurado pelo Estado, a consulta jurídica – gratuita em determinados casos – e, se necessário, ao subsequente apoio e patrocínio judiciário;

ii) a possibilidade de a vítima ser reembolsada das despesas efectuadas em resultado de intervenção no processo penal e compensada pelos danos materiais e morais sofridos;

iii) o direito a que seja assegurado um nível adequado de protecção à vítima e, sendo caso disso, aos seus familiares, sempre que se considere que existe uma ameaça séria de represálias e de situações de revitimização ou fortes indícios de que a sua privacidade possa ser perturbada, designadamente com a convocação das medidas previstas na Lei da Protecção de Testemunhas;
iv) a possibilidade de a inquirição da vítima especialmente vulnerável ocorrer no regime de declarações para memória futura, conforme previsto no art.º 24.º do Estatuto – um dos direitos específicos previstos para as vítimas especialmente vulneráveis;
v) o recurso à participação no processo por videoconferência ou teleconferência, caso exista a presença do arguido na mesma sala – também para as vítimas especialmente vulneráveis; ou o afastamento daquele durante a prestação de depoimento, se tal se justificar;
vi) o direito a que as vítimas especialmente vulneráveis, na prestação de declarações ou depoimento, possam ser acompanhadas por um técnico especialmente habilitado;
vii) a aplicação obrigatória do mecanismo de reparação da vítima previsto no art.º 82-A do CPP na inexistência de pedido de indemnização civil, salvo se a vítima (especialmente vulnerável) a isso expressamente se opuser.

Assim sendo, apesar destes incisos, no que se refere especificamente às vítimas de actos terroristas, não há qualquer disposição legal especial dedicada à sua protecção, integrando-se os seus direitos na perspectiva mais genérica dos direitos das vítimas e das vítimas especialmente vulneráveis, o que pode ser insuficiente.
Ao contrário de Portugal, vários países da Europa – nomeadamente a Espanha, a Bélgica, a Itália e o Reino Unido – adoptaram legislação própria e medidas específicas de apoio e protecção às vítimas de terrorismo, o que parece encontrar explicação no facto de esses países terem sido confrontados, recentemente, com atentados terroristas provocados por radicalizados e fundamentalistas islâmicos, ou, então, por radicais com motivações de índole política, como foi o caso da Espanha e da Irlanda do Norte.
Em Portugal, a Associação Portuguesa de Apoio à Vítima (APAV) tem trilhado alguns passos na formação e na especialização de recursos para dar resposta a potenciais situações de vitimização por terrorismo.
Em concreto, a APAV dispõe desde 2013 da Rede de Apoio a Familiares e Amigos de Vítimas de Homicídio e de Terrorismo (RAFAVHT), que já conta com alguma casuística de apoio a Portugueses e familiares de Portugueses alvo de atentados fora de Portugal desde o ano de 2016.
Nessa senda, já em 2020, a APAV desenvolveu a Unidade de Apoio à Vitimação em Massa (UAVM), que se apresenta como uma resposta especializada de apoio a vítimas de violência massiva, como é o caso do terrorismo. Este apoio, igualmente disponibilizado aos familiares e amigos das vítimas, integra o modelo de intervenção próprio da APAV, combinando o apoio prático, psicológico, jurídico e social, de acordo com as necessidades identificadas, apoio esse prestado de forma gratuita e confidencial pelo período considerado necessário. O desenvolvimento destas respostas de apoio concreto está também vinculado à cooperação estreita com congéneres internacionais, bem como com as demais entidades de relevo nacionais na prevenção e resposta a eventuais situações de terrorismo.
No que tange à prevenção, a APAV colaborou no projecto Counter@act – Prevenção e Combate à Radicalização *online*, que teve como objectivo promover a mudança de comportamentos que dissuadam jovens de aderir a conteúdos, mensagens e propaganda radical ou de incitamento ao extremismo violento, através do desenvolvimento de uma campanha de narrativas alternativas *online* que veiculem histórias positivas de integração, em particular de jovens migrantes e de refugiados. Este projecto foi desenvolvido em parceria com a Polícia Judiciária (PJ), o Serviço de Informações de Segurança (SIS), a Associação Renovar a Mouraria, o Serviço Jesuíta aos Refugiados (JRS Portugal), e ainda a Logframe, a Digital Xperience, a Fundación Fernando Buesa (País Basco) e o Victim Support Europe.

Em conclusão

A criminalidade associada ao terrorismo, para além do seu simbolismo e potencial altamente lesivo de direitos fundamentais, invoca uma preocupação à escala global, na medida em que as organizações terroristas podem operar em diferentes países, aproveitando-se das facilidades de deslocação e de comunicação virtual, quase sem barreiras, existentes na era moderna.
Como tal, num verdadeiro espaço de Liberdade, de Segurança e de Justiça, compete à União Europeia promover a cooperação entre os Estados-Membros e a estes cabe assegurar que os respectivos sistemas jurídico-penais dão resposta adequada a este fenómeno, prevenindo a sua ocorrência e reprimindo eficazmente aqueles que praticam crimes de carácter terrorista, e, assim, transmitir à comunidade a necessária segurança e confiança.
Muitos dos incidentes terroristas verificados em território europeu, foram perpetrados, não por pessoas estrangeiras, mas por indivíduos nacionais e descendentes de comunidades migrantes, que já cresceram na Europa. São, muitas vezes, pessoas que se radicalizaram e se viraram contra o seu próprio país, onde nasceram, cresceram, foram formados, trabalham, mas que não sentem como seu e, muitas vezes, querem repudiar e destruir.
Por isso, a prevenção do terrorismo implica que se actue numa fase muito anterior à consumação dos actos, através da adopção de medidas que travem a radicalização de certos segmentos da sociedade. Neste âmbito, a estratégia de prevenção passa necessariamente por impedir a difusão, por meios digitais, de conteúdos que incentivem à violência e à prática de actos terroristas. Mas não só, urge também integrar

adequadamente as comunidades migrantes, promovendo a inclusão e a criação de oportunidades para todos os sujeitos, independentemente do seu estatuto social, da sua religião e da origem étnica.

No que tange à protecção das vítimas conclui-se que, em Portugal, ao contrário do que sucede em vários países da Europa, não há qualquer legislação especialmente dedicada à protecção das vítimas de terrorismo, aplicando-se a estas o Estatuto da Vítima – que contém um conjunto de medidas que visam assegurar a protecção e a promoção dos direitos das vítimas da criminalidade geral, o que pode ser *in casu* insuficiente e inadequado.

É, de resto, fundamental que Portugal aplique e transponha para a ordem jurídica interna as normas da União Europeia destinadas a prevenir e a combater o terrorismo, porquanto, ainda que não haja um histórico recente de ataques terroristas perpetrados em Portugal, também os cidadãos portugueses são susceptíveis de radicalização, podendo consumar um crime terrorista em território nacional, ou rumar a outro país para, aí, porem em prática os actos de barbárie que primeiramente viram na Internet e que são agora aliciados a cometer.

A APAV é essencial, na ausência de legislação específica, por dedicar-se proactivamente a formar e desenvolver recursos especializados de apoio às famílias, amigos e, mormente, às vítimas, para fazer face às graves consequências de potenciais situações de terrorismo em Portugal, ou mesmo para lá das nossas fronteiras.

É, por isso, essencial não apenas estudar melhor o fenómeno do terrorismo e apostar mais nas acções de prevenção como regular adequada e especificamente a temática e as suas consequências.

Referências bibliográficas

Al Rawi, Ahmed & Groshek Jacob (2018). Jihadist Propaganda on Social Media: An Examination of Isis Related Content on Twitter.

Coolsaet, Rick (2016). All radicalisation is Local - The Genesis and Drawbacks of an Elusive Concept.

Coolsaet, Rick (2016). Facing the fourth foreign fighters wave – What drives Europeans to Syria, and to Islamic State? Insights from the Belgian Case.

Dias, Figueiredo; Caeiro, Pedro (2005). A Lei de Combate ao Terrorismo.

Freitas, Pedro Miguel (2022). Ciberterrorismo e a Lei de Combate ao Terrorismo.

Huey, Laura. (2015). This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming.

Lopes, Araújo Joana (2019). Definição e Resposta ao Terrorismo na UE e em Portugal: o Que Fazer das Mulheres e Crianças Afiliadas ao Daesh?

Martins, Carneiro François Raúl (2010). Acerca de "Terrorismo" e de "Terrorismos"

Nesser, Petter, Stenersen, Anne & Oftedal, Emilie (2016). Jihadi Terrorism in Europe: The IS-Effect.

Sànchez-Cuenca, Ignacio (2007). The Dynamics of Nationalist Terrorism: ETA and the IRA.

Tribunal Constitucional:

Acórdão do Tribunal Constitucional, n.º 278/92, Processo n.º 442/91.

SUPREMO TRIBUNAL DE JUSTIÇA:

Acórdão do Supremo Tribunal de Justiça de 13 de Julho de 2022, Processo n.º 5/13.1JBLSB.L1.S1.

Acórdão do Supremo Tribunal de Justiça de 28 de Março de 2019, Processo n.º 257/18.0GCMTJ-BA.S1.

Acórdão do Supremo Tribunal de Justiça de 15 de Junho de 1998, Processo n.º 039546.

Acórdão do Supremo Tribunal de Justiça de 4 de Maio de 1994, Processo n.º 046225.

Acórdão do Supremo Tribunal de Justiça de 16 de Janeiro de 1992, Processo n.º 042166.

Acórdão do Supremo Tribunal de Justiça de 14 de Março de 1991, Processo n.º 042166.

Acórdão do Supremo Tribunal de Justiça de 19 de Dezembro de 1990, Processo n.º 040825.

Acórdão do Supremo Tribunal de Justiça de 22 de Junho de 1988, Processo n.º 039596.

Acórdão do Supremo Tribunal de Justiça de 7 de Outubro de 1987, Processo n.º 039006.

Tribunais da Relação:

Acórdão do Tribunal da Relação de Lisboa de 11 de Abril de 2023, Processo n.º 10/22.7JBLSB.L1-5.

Acórdão do Tribunal da Relação de Lisboa de 26 de Outubro de 2022, Processo n.º 38/20.1JBLSB-A.L1-3.

Acórdão do Tribunal da Relação de Lisboa de 9 de Maio de 2019, Processo n.º 257/18.0GCMTJ-AV.L1-9.

Acórdão do Tribunal da Relação de Lisboa de 16 de Junho de 2021, Processo n.º 5/13.1JBLSB.L1-3.

Acórdão do Tribunal da Relação de Lisboa de 27 de Novembro de 2018, Processo n.º 78/15.2JBLSB.L1-5.

Acórdão do Tribunal da Relação de Lisboa de 10 de Outubro de 2018, Processo n.º 257/18.0GCMTJ-R.L1-3.

Acórdão do Tribunal da Relação de Lisboa de 26 de Setembro de 2018, Processo n.º 257/18.0GCMTJ-F.L1-3.

Acórdão do Tribunal da Relação do Porto de 4 de Março de 2009, Processo n.º 0818115.

Acórdão do Tribunal da Relação de Lisboa de 4 de Fevereiro de 2004, Processo n.º3880/2003-3.

Acórdão do Tribunal da Relação de Lisboa de 16 de Janeiro de 1996, Processo n.º 0006685.

Acórdão do Tribunal da Relação do Porto de 23 de Fevereiro de 1994, Processo n.º 9321407.

Acórdão do Tribunal da Relação de Lisboa de 18 de Outubro de 1993, Processo n.º 0063965.

Acórdão do Tribunal da Relação de Lisboa de 27 de Julho de 1992, Processo n.º 0291083.

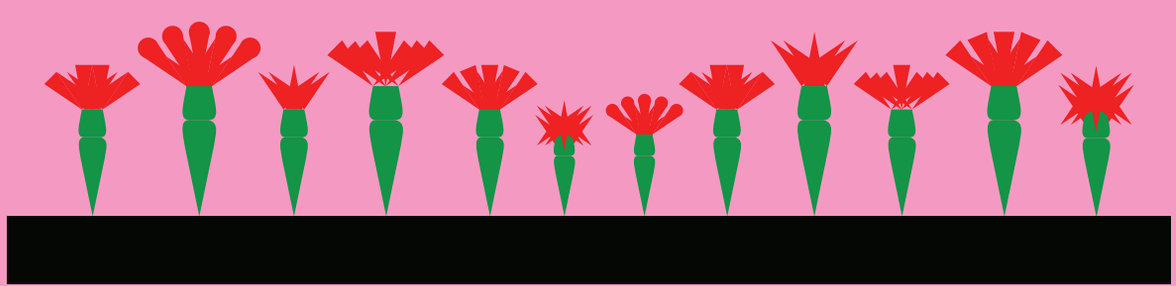
Acórdão do Tribunal da Relação de Lisboa de 24 de Outubro de 1990, Processo n.º 0262053.

Pareceres do Concelho Consultivo da Procuradoria Geral da República:

Parecer do Conselho Consultivo da PGR de 1 de Junho de 2011.

Parecer do Conselho Consultivo da PGR de 10 de Setembro de 1998.

APAV®



O 25 de Abril é liberdade para todas as pessoas.

APAV®
associação portuguesa de
Apoio à Vítima

50 anos do 25 de Abril

05.

A VIOLÊNCIA OBSTÉTRICA NO ORDENAMENTO JURÍDICO PORTUGUÊS – CONTRIBUTOS PARA UMA EVOLUÇÃO DO QUADRO LEGISLATIVO

VÂNIA SIMÕES

Resumo

Pese embora as primeiras críticas sobre a excessiva medicalização remontarem à década de 60/70 do século passado (Foucault – 1973, Arms -1975, Rich-1976, Martin 1987, Katz Rothman 1991, Mitford 1992, Davis-Floyd e Dumit – 1998), apenas em 2014, a Organização Mundial de Saúde reconheceu na Declaração sobre prevenção e eliminação de abusos, desrespeito e maus-tratos durante o parto nas instituições de saúde, a ocorrência de violência obstétrica um pouco por todo o mundo.

Suellen Miller *et al.* (2016), fazem notar que a violência obstétrica assume moldes diferentes nos "países desenvolvidos" e "subdesenvolvidos", referindo que nos países desenvolvidos existe um "excesso" de cuidados, prestados de modo precoce - "*too much, too soon*", e que nos países subdesenvolvidos, pelo contrário, a dificuldade de acesso a cuidados de saúde materno-infantis é um problema que pode inclusivamente comprometer a adequação dos cuidados de saúde prestados, remetendo-nos para uma realidade de "*too little, too late*". Estas realidades divergentes de violência obstétrica acabam por dificultar quer a conceptualização, quer a categorização da violência obstétrica (Simovic, 2019).

Na América Latina, a regulamentação sobre violência obstétrica ocorreu no início dos anos 2000, com a Argentina (2004) e a Venezuela (2007), seguindo-se outros países latino-americanos.

Atualmente, a Venezuela (2007) é o único país no mundo que penaliza a violência obstétrica, tendo sido um país pioneiro quanto à conceptualização da violência obstétrica que define como a "apropriação do corpo e processos reprodutivos das mulheres pelos profissionais de saúde, que se expressa num tratamento desumanizado, abuso de medicalização quanto a processos naturais, levando à perda de autonomia e capacidade decisória das mulheres sobre os seus corpos e sexualidade, com impacto negativo na qualidade de vida das mulheres (tradução livre)".

Na Europa (tal como em Portugal), é no ano de 2019 que surge o primeiro texto sobre o tema, com a Resolução do Conselho da Europa nº 2306/2019, de 3 de outubro, documento em que são exaradas recomendações aos Estados para a sua erradicação.

Espanha (2021), Itália (2016) e França (desde 2018) também têm demonstrado empenho no combate à violência obstétrica nestes últimos anos, com recurso a políticas públicas e alterações legislativas em curso nos seus ordenamentos jurídicos.

Para fazer face ao problema de saúde pública que a violência obstétrica representa em Portugal, em que 1 em cada 3 mulheres alega ter sido vítima de violência obstétrica (APDMGP, 2019), foi aprovada a Lei nº 110/2019, de 9 de setembro, que outorga direitos às mulheres em contexto de saúde sexual e reprodutiva na qualidade de utentes/pacientes, sendo o diploma aplicável a entidades públicas, privadas e ao sector social. Este diploma vem reafirmar os direitos das mulheres na qualidade de utentes/pacientes, agravando ainda a responsabilidade médica civil em situações de violência obstétrica, ao prever agora direitos específicos às mulheres, inerentes à qualidade de progenitora (ou potencial progenitora) que não estavam antes consagrados no nosso ordenamento jurídico, como o direito da parturiente à mínima interferência (Simões, 2023).

Seguiu-se a Resolução nº 181/2021, de 28/06, que recomenda ao Governo a erradicação das práticas de violência obstétrica, que é o primeiro instrumento legislativo em Portugal no qual surge expressamente o termo "violência obstétrica", termo esse que não consta no seio da Lei nº 110/2019, de 9 de setembro. Antes desta Resolução, o termo violência obstétrica tinha surgido numa petição pública submetida à Assembleia

da República em 2018, que solicitava a penalização da violência obstétrica em Portugal, a petição nº 507/XIII/2ª, que não foi aprovada pelo Parlamento por ter sido levada a plenário em outubro de 2019, altura em que a Lei nº 110/2019, de 9 de setembro, acabava de ser aprovada.
O debate português em torno da penalização da violência obstétrica iniciado em 2018, intensificou-se com a pandemia, devido às restrições que ocorreram de direitos das mulheres em contexto de assistência à gravidez, parto e puerpério.
Em julho de 2021, o Projeto-lei nº 912/XIV/2ª, da iniciativa da deputada não inscrita Cristina Rodrigues, traria o tema novamente para o Parlamento, tendo a discussão sido interrompida por ocasião da dissolução da Assembleia da República, em 2021.
Apesar da dissolução da Assembleia da República e da não recandidatura da ex-deputada, a mesma apresentou uma petição pública como forma de reaproveitar o Projeto-lei apresentado, para o conseguir levar ao Parlamento para aprovação.
Mais recentemente, o Bloco de Esquerda preparou três projetos-lei, não só para incorporar o termo "violência obstétrica" na Lei nº 110/2019, de 9 de setembro, mas também para criar a Comissão Nacional para os Direitos na Gravidez e Parto, fomentar formação a públicos diversos como forma de erradicar a violência obstétrica, prevendo ainda sanções para a prática de episiotomias para profissionais de saúde e hospitais – o Projeto-Lei nº 962/XV/2ª, o Projeto-lei nº 963/XV/2ª e o Projeto-resolução nº 947/XV/2ª, todos caducados em razão da dissolução do Parlamento.
Embora as mulheres já tivessem tutela no que respeita aos seus direitos em contexto de assistência obstétrica anteriormente a todos estes instrumentos supra mencionados, a ausência de reconhecimento jurídico/legal do fenómeno, da sua conceptualização e a normalização da violência contra as mulheres, tem contribuído para a invisibilidade da violência obstétrica nos tribunais, que tem estado ausente no debate jurisprudencial português.

A violência obstétrica desde o Direito Internacional dos Direitos Humanos

Em 2011, a White Ribbon Alliance elaborou a Declaração Universal dos Direitos da Mulher no Parto, relevante instrumento de *soft law* nesta matéria, onde os direitos das utentes/pacientes são apresentados como direitos humanos das mulheres e aos quais são contrapostas as respetivas categorias de desrespeito ou abuso. Estes direitos foram incorporados na Lei portuguesa nº 110/2019, de 9 de setembro, sob a forma de princípios no artigo 15º A do mencionado diploma.
Em 2014, a Organização Mundial da Saúde abordou na Declaração sobre prevenção e eliminação de abusos, desrespeito e maus-tratos durante o parto em instituições de saúde refere que em causa estão: "abusos, desrespeito, maus-tratos e negligência durante a assistência ao parto (…) violência física, humilhação profunda e abusos verbais, procedimentos médicos coercivos ou não consentidos, falta de confidencialidade, não obtenção de consentimento esclarecido antes da realização de procedimentos, (…) recusa de internação nas instituições de saúde, cuidado negligente durante o parto levando a complicações evitáveis e situações ameaçadoras da vida, e detenção de mulheres e seus recém-nascidos nas instituições, após o parto (…)." (OMS, 2014, p.1)
Também o Tribunal Europeu dos Direitos Humanos já se pronunciou em três decisões sobre a violação de direitos das mulheres na gravidez e parto, nos casos Ternovszky versus Hungria, Dubska e Krejova versus República Checa e Konovalova versus Rússia, não tendo, contudo, recorrido ao termo na análise dos casos.
Em 2019, a ONU, através da sua relatora especial, elaboraria o Relatório especial da ONU sobre direitos humanos e violência contra a mulher nos serviços de saúde reprodutiva, com enfoque no parto e violência obstétrica, onde adota a terminologia "violência obstétrica", abordando a sua ocorrência em diversos países.
Desde então que o comité CEDAW passou a utilizar o termo para "censurar" a Espanha em diversos casos em que foi suscitada a apreciação da violação de direitos humanos de mulheres na assistência obstétrica que receberam.
Na decisão CEDAW/C/75/D/138/2018 (p.13) é mencionado que: "*el Comité considera que la aplicación de estereotipos afecta el derecho de la mujer a ser protegida contra la violencia de género, en el caso presente la violencia obstétrica, y que las autoridades encargadas de analizar la responsabilidad por tales actos deben ejercer especial cautela para no reproducir estereotipos.*"
Na decisão CEDAW/C/82/D/149/2019 (p.17) é mencionado que: "*las consecuencias físicas y psicológicas que los eventos tuvieron para la autora, constituyen violencia obstétrica.*"
Na decisão CEDAW/C/84/D/154/2020 (p.16) é mencionando que: "*El Comité considera que el cúmulo de hechos del presente caso, en particular, la pérdida de dignidad, el abuso y el maltrato sufrido por la autora, la aplicación irregular de anestesia epidural y la falta de consideración de patologías previas sin el consentimiento informado y/o sin haber justificado la necesidad de dichas intervenciones y la omisión en recabar el consentimiento informado previo a realizar una cesárea, todo lo cual dejó secuelas físicas y psicológicas en la autora, constituyen violencia obstétrica.*"
O Comité CEDAW fez Recomendações ao Estado Português em 2015 e 2022, em matéria de saúde materna. Em ambas as Recomendações se frisou a necessidade de se cumprir o direito à informação e ao consentimento informado das mulheres, tendo-se ainda alertado, em 2015, o Estado Português para a alta taxa de medicalização dos partos ocorridos em Portugal, Recomendação novamente produzida em 2022.

Em 2019, o Conselho da Europa reconheceu a violência obstétrica enquanto forma de violência de género perpetrada no âmbito da prestação de cuidados de saúde, através da Resolução 2306 (2019), de 3 de outubro (CE, 2019). No ano seguinte, a União Europeia ("UE") adotou uma estratégia de Igualdade de Género para 2020-2025 (Com, 2020). A violência ginecológica e obstétrica só vem mencionada na Resolução do Parlamento Europeu, 2019/2169, de 21 de janeiro de 2021, nomeadamente no seu Considerando G, que afirma: "Considerando que a violência contra as mulheres em todas as suas formas (violência física, sexual, psicológica, económica ou cibernética) constitui uma violação dos direitos humanos e um dos maiores obstáculos à consecução da igualdade de género; considerando que uma vida sem violência é uma condição para a igualdade; considerando que a violência baseada no género na saúde, designadamente, a violência obstétrica e ginecológica são formas de violência que apenas se tornaram conhecidas nos últimos anos (...)" (PE, 2021).

Por instâncias do Comité CEDAW, já havia sido analisado o caso da cidadã brasileira Alyne Pimentel, em que o Estado Brasileiro foi alvo de uma declaração de violação de direitos humanos, na sequência de comunicação pelo Comité, em que a utente que esperou horas para que cuidados de saúde lhe fossem prestados, tendo acabado por falecer, óbito esse que poderia ter sido evitado se Alyne tivesse acesso a cuidados de saúde.

É efetivamente importante reconhecer que a violência obstétrica consubstancia uma relevante, quando não grave, violação dos direitos humanos das mulheres em contexto de assistência em saúde baseada num atendimento estereotipado, discriminatório e, consequentemente, violento.

O problema conceptual e as dificuldades em legislar sobre violência obstétrica

O conceito de violência obstétrica adotado pelos países latino-americanos não auxiliar a uma adequada aplicação das leis nacionais de violência obstétrica. Só na Venezuela, por exemplo, apenas duas condenações ocorreram por violência obstétrica desde 2007.

O recurso a conceitos indeterminados, vagos e "extrajurídicos" na definição legal de violência obstétrica dificultam uma apreciação objetiva, aos casos concretos, os termos empregues como "patologização" de eventos fisiológicos, "excesso de medicalização" ou "apropriação do corpo" da mulher. Também os grupos parlamentares têm tido dificuldades na conceptualização do fenómeno. Contudo, o reconhecimento jurídico da violência

obstétrica no ordenamento jurídico português faz-se necessária para que as vítimas acedam à justiça.
No Projeto-Lei nº 962/XV/2 (caducado), definiu-se como toda "a ação física e verbal exercida pelo pessoal de saúde sobre o corpo e os processos reprodutivos das mulheres ou de outras pessoas gestantes, que se expressa num tratamento desumanizado, num abuso da medicalização ou na patologização dos processos naturais, desrespeitando o regime de proteção na preconceção, na procriação medicamente assistida, na gravidez, no parto, no nascimento e no puerpério previsto na secção II da Lei n.º 15/2014, de 21 de Março, na sua redação atual."
No Projeto de Lei nº 912/XIV/2ª (caducado) foi definida como "qualquer conduta direcionada à mulher, durante o trabalho de parto, parto ou puerpério, praticada sem o seu consentimento, que consubstanciando um acto de violência física ou psicológica, lhe cause dor, dano ou sofrimento desnecessário ou limite o seu poder de escolha e de decisão".
Porém, só com uma adequada conceptualização do fenómeno teremos êxito em implementar uma justa reparação junto das vítimas.
No artigo n.º 15.º-A, n.º 1, alínea d), a Lei n.º 110/2019 refere-se que as mulheres têm direito a estar livres de qualquer forma de violência no âmbito dos cuidados de saúde reprodutiva que lhe são prestados, sem adotar especificamente o termo violência obstétrica. Esta lei estabelece ainda o direito à privacidade e confidencialidade (no 15.º-A, n.º 1, al. b)); direito à assistência contínua (15.º-G e 18.º, n.º 2); direito ao tratamento digno e respeitoso, livre de coação, violência e sem discriminação (no já referido artigo 15.º-A, n.º 1, alíneas c), d) e e)); direito a um intérprete se necessário (artigo 15.º-C, n.º 3); direito à informação, recusa e consentimento informado (14.º-A, n.º 1, al. a)); direito à liberdade e autonomia (15.º-A, n.º 1, al. g)); direito aos melhores cuidados de saúde, seguros e apropriados (15.º-A, n.º 1, al. f)) com recurso apenas às intervenções necessárias, de acordo com a melhor evidência científica (15.º-F, n.º 2) e as recomendações da OMS (15.º-F, n.º 6). Fora isso, fica também expressamente estabelecido o direito à amamentação (no número 15.º-H); o direito ao alívio da dor (15.º-F, n.º 4) e ao acompanhamento (12.º a 17.º).

Crimininalizar ou não criminalizar: eis a questão.

A necessidade de autonomizar a violência obstétrica como tipo legal de crime tem suscitado algumas questões.
A favor da criminalização, o argumento do acesso à justiça e da adequada reparação das vítimas, e, contra a criminalização, é dado o argumento da emergência de uma prática de medicina defensiva por parte dos profissionais de saúde (Simões, 2023).
A multiplicidade de bens jurídicos que podem estar em causa, tanto da mulher, como do nascituro/recém-nascido ou de ambos, não torna claro quais os bens jurídicos necessitados de tutela jurídico-penal (Simões, 2023).
Por um lado, a integridade física, moral e sexual da mulher, e em última *ratio*, a sua dignidade humana podem ser afetadas em situações de violência obstétrica.
Por outro lado, a vida e integridade física do nascituro podem ser alvo de interferências.
Sucede que ao aplicarmos preceitos existentes a situações de violência obstétrica, a dimensão de violência e as dinâmicas de poder exercidas neste contexto ficariam invisibilizadas, bem como a vulnerabilidade dos sujeitos afetados.
No passado defendeu-se a aplicação do art. 152º A do Código Penal às situações de violência obstétrica, pelo facto de prever no seio da sua tutela a condição de vulnerabilidade da mulher grávida (Simões, 2016). Porém, esta tutela não parece unânime, pois poderia levar-nos a uma aplicação analógica da lei penal, situação vedada pelo Código Penal (art. 1º do nº 3 do Código).
Assim, a vulnerabilidade dos sujeitos afetados, as dinâmicas de poder exercidas nestas relações jurídicas e a necessidade de tutela de bens jurídicos específicos, como o são a saúde sexual e reprodutiva, justificariam a autonomização de um tipo legal de crime de violência obstétrica (Simões, 2016 e 2023) (Faria, 2023).

Os atuais obstáculos no acesso à justiça por parte das vítimas

Para além da ausência de tipificação da violência obstétrica no ordenamento jurídico português, da ausência de reconhecimento do termo na lei e a sua consequente indefinição legal, outros empecilhos processuais obstaculizam o acesso das vítimas à justiça. De notar que o encargo probatório está do lado da vítima, que por vezes nem o processo clínico consegue para si ou quando se lhe tem acesso está insuficiente ou com incorreções. Soma-se a isto, perícias médico-legais que têm a violência obstétrica como normalidade clínica ou que dificilmente conseguem estabelecer um nexo causal entre as condutas e os danos, com tendencial menosprezo dos danos que não sejam físicos.
Como a violência obstétrica é equiparada à negligência médica as mulheres não são reconhecidas como vítimas e sujeitas ao pagamento de todos os encargos.
Oitenta e dois por cento (82%) dos partos ocorrem em instituições públicas, pelo que o Tribunal Administrativo e Fiscal é o competente para apreciar o mérito das causas, caracterizado pela demora nas decisões. Grande parte dos casos respeitam a asfixia perinatal, o que nos indicia que as mulheres tendem a desvalorizar a violação dos seus direitos, litigando, em grande medida, quando ocorrem danos sérios junto dos seus filhos.

Para onde caminhamos?

Os sucessivos projetos-lei apresentados em Portugal, junto do Parlamento, desde 2021, aliados às Resoluções europeias emitidas nesta matéria evidenciam uma tendência que vai no sentido de se reconhecer a violência obstétrica no ordenamento jurídico português, nem que seja por via da legislação europeia. Com mais de cento e setenta mil (170.000) assinaturas, foi apresentada recentemente uma petição pelo coletivo francês STOP VGO junto do Parlamento Europeu, a requerer a incorporação do termo na Convenção de Istambul, instrumento europeu em matéria de erradicação da violência contra as mulheres adotada em Istambul, a 11 de maio de 2011, aprovada pelo Governo português a 16 de novembro de 2012; ratificada pela Assembleia da República a 21 de janeiro de 2013 e que entrou em vigor em Portugal a 1 de agosto de 2014. O primeiro passo, o do reconhecimento desta forma de violência, é essencial para se oferecer uma tutela jurídica condigna às vítimas.

Referências bibliográficas

APDMGP — Associação Portuguesa pelos Direitos da Mulher na Gravidez e Parto (2019). Experiências de Parto em Portugal. 2.ª Edição: 2015-19. Lisboa: APDMGP. Disponível em https://associacaogravidezeparto.pt/wp-content/uploads/2020/12/Experie%CC%82ncias-de-Parto-em Portugal_2edicao_2015-19-1.pdf, último acesso: 2023-03-07, 15:24 UTC.

Dixon, L. (2015), Obstetric in a time of violence: Mexican Midwives Critique Routine Hospital Practices, Medical Anthropology Quarterly, Dec;29(4):437-54. doi: 10.1111/maq.12174. Epub 2015 Sep 14, disponível em https://anthrosource.onlinelibrary.wiley.com/journal/15481387, último acesso em 2023/03/09, 17h49 UTC.

Faria, Maria Paula Ramos D. (2023). A criminalização da violência obstétrica e os limites constitucionais de intervenção do direito penal. Em M. A. D. Almeida, P. Machete, F. U. Calvão, A. Cortês, R. Carvalho, L. Fábrica, M. Portocarrero, J. P. D. Silva, M. O. Martins, & A. Rocha (Eds.), Estudos em homenagem à Professora Doutora Maria da Glória F. P. D. Garcia (3 ed.). Universidade Católica Editora.

Miller, Suellen et al., Beyond too little, too late and too much, too soon: a pathway towards evidence-based, respectful maternity care worldwide, The Lancet, SERIES|MATERNAL HEALTH| V. 388, ISSUE 10056, P2176-2192, OCTOBER 29, 2016.

Ordem dos Médicos Portuguesa (2021). Parecer sobre o Projeto Lei 912/XIV/2ª (NIsc CR) "Reforço da proteção das mulheres na gravidez e parto através da criminalização da violência obstétrica. NU: 681879, Ref.: 1519/1.ª CACDLG, 20 de outubro de 2021. Lisboa: Assembleia da República. Disponível em https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d4644623231706333 4e686279396a595459314d6a686b4e693035595755794c54526c4f575174596a646c5953316d4e32517a4e6a67304d5441305a474d756347526d&fich=ca6528d6-9ae2-4e9d-b7ea-f7d3684104dc.pdf&Inline=true, último acesso: 2023/03/07 15:58 UTC.

Organização Mundial da Saúde (2014). Prevenção e eliminação de abusos, desrespeito e maus-tratos durante o parto em instituições de saúde, disponível em https://apps.who.int/iris/bitstream/handle/10665/134588/WHO_RHR_14.23_por.pdf, último acesso: 2023/03/07, 13:15 UTC.

Rodrigues, C. (2021). Projeto de Lei n.º 912/XIV/2.ª, Reforça a proteção das mulheres na gravidez e parto através da criminalização da violência obstétrica. Lisboa: Assembleia da República Portuguesa. Disponível em https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765247396a6457316c626e527663306c7561574e7059585270646d45764e4459334d545978596a45744e5467334d7930304d5451334c546b304e6a49745954526a595745784d7a59784e5467314c6d527659773d3d&fich=467161b1-5873-4147-9462-a4caa1361585.doc&Inline=true, último acesso: 2023/03/17, 15:39 UTC.

Simões, V. (2016). A Violência Obstétrica: a violência institucionalizada contra o género. Vencedor do Prémio Teresa Rosmaninho – Direitos Humanos, Direitos das Mulheres, atribuído pela Associação Portuguesa de Mulheres Juristas

(APMJ). Lisboa: APMJ. Disponível em https://apmj.pt/premio-teresa-rosmaninho, último acesso: 2023/03/07,15:56 UTC.

Simões, V. (2023, aguarda agendamento de provas). Violência obstétrica, Direitos das Mulheres e Tutela jurídica. Tese para obtenção do grau de Doutora na Universidade Nova de Lisboa. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa.

SIMONOVIC, Dubravka, Relatório especial sobre direitos humanos e violência contra a mulher nos serviços de saúde reprodutiva, com enfoque no parto e violência obstétrica, de 11 de julho de 2019, disponível em https://digitallibrary.un.org/record/3823698?ln=en, último acesso: 21/02/2024, 10h07 UTC.

STOP VGO, Petição "Ensemble, contre les violences obstétricales et gynécologiques!" disponível em https://www.change.org/p/l-europe-doit-reconna%C3%AEtre-les-violences-obst%C3%A9tricales-et-gyn%C3%A9cologiques, último acesso: 21/02/2024, 19h05 UTC.

White Ribbon Alliance (2011). Respectful Maternity Care: The Universal Rights of Childbearing Women, Washington D.C.: White Ribbon Alliance, Outubro 2011, disponível em https://whiteribbonalliance.org/wp-content/uploads/2022/05/WRA_RMC_Charter_FINAL.pdf, último acesso: 2023/03/7, 13:01 UTC.

Zaccagnini, A. (2016). Projeto-lei n.º 3.670/2016, de 11 de março. Roma: Camara dei Deputati, disponível em https://documenti.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0039650.pdf, último acesso: 2023/03/09, 17h24 UTC.

Legislação e Outros

Assembleia da República Francesa (2020), Proposition de résolution nº 3305 invitant le Gouvernement à faire de la lutte contre les violences obstétricales et gynécologiques une priorité et à mettre en œuvre les recommandations du Haut Conseil à l'Egalité en la matière (assemblee-nationale.fr). Paris: Assemblee Nationale. Disponível em https://www.assemblee-nationale.fr/dyn/15/textes/l15b3305_proposition-resolution, último acesso em 2023/03/09, 17h42 UTC.

Assembleia da República Portuguesa (2019). Lei n.º 14/2014, de 21 de março. Diário da República n.º 57/2014, Série I de 2014-03-21, pp. 2127-2131. Lisboa: Imprensa Nacional Casa da Moeda. Disponível em https://dre.pt/dre/detalhe/lei/15-2014-571943, último acesso: 2023/03/07, 14:40 UTC.

Assembleia da República Portuguesa (2019). Lei n.º 110/2019, de 9 de setembro. Diário da República n.º 172/2019, Série I de 2019-09-09, pp. 94-101. Lisboa: Imprensa Nacional Casa da Moeda. Disponível em https://dre.pt/dre/detalhe/lei/110-2019-124539905, último acesso: 2023/03/07, 14:33 UTC.

Assembleia da República Portuguesa (2021). Resolução da Assembleia da República n.º 181/2021, de 28 de junho. Diário da República n.º 123/2021, Série I de 2021-06-68, pp. 6-6. Lisboa: Imprensa Nacional Casa da Moeda. Disponível em https://dre.pt/dre/detalhe/resolucao-assembleia-republica/181-2021-165865615, último acesso: 2023/03/07, 16:53 UTC.

Assembleia Geral da Organização das Nações Unidas (1979). CEDAW – Convenção para a Eliminação de Todas as Formas de Discriminação contra Mulheres. Disponível em https://www.un.org/womenwatch/daw/cedaw/text/econvention.htm, último acesso: 2023/03/20, 22:22 UTC.

Bloco de Esquerda (2023):

- Projeto-lei nº 962, disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=263399 , último acesso em 22/02/2024, 14h16 UTC.

- Projeto-lei nº 963/XV/2ª, disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=263400, último acesso em 22/02/2024, 14h16 UTC.

- Projeto-resolução nº 947/XV/2ª, disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=263400, último acesso em 22/02/2024, 14h16 UTC.

Comité para a Eliminação de Discriminação contra Mulheres (2011). Alyne da Silva Pimentel Teixeira vs Brasil, Comunicação nº 17/2008, 29 de julho de 2011, Documento da Organização das Nações Unidas n.º CEDAW/C/49/D/17/2008, disponível em https://www2.ohchr.org/english/law/docs/cedaw-c-49-d-17-2008.pdf, último acesso: 2024/02/07, 15:33 UTC.

Comité para a Eliminação de Discriminação contra Mulheres (2019). N.A.E. v. Espanha, Comunicação n.º 138/2019, de 13 de julho de 2022, Documento da Organização das Nações Unidas n.º CEDAW/C/82/D/149/2019, disponível em https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW%2FC%2F82%2FD%2F149%2F2019&Lang=en, último acesso: 2024/02/07, 15:33 UTC.

Comité para a Eliminação de Discriminação contra Mulheres (2020). M. D. C. P. v. Espanha, Comunicação n.º 154/2020, de 9 de março de 2023, Documento da Organização das Nações Unidas n.º CEDAW/C/84/D/154/2020, disponível em https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/TBSearch.aspx?Lang=en&TreatyID=3&DocTypeID=17, último acesso: 2024/02/07, 15:35 UTC.

Comité para a Eliminação de Discriminação contra Mulheres (2022). Resolução do Comité para a Eliminação de Discriminação contra Mulheres n.º CEDAW/C/82/D/149/2019. Disponível em https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsgekS3XMuMTIW18D8vtwB38fJnPp13jDCkgmP1uEoaFJuB4nZLZNnPYqgEjogm9K1Cgn3YEbCRFqR5qxa8Z23HM9wCnl%2F2rMtQb8EbYObEUoTXLa0qRTeh6pYx15p9MiiA%3D%3D, último acesso: 2023/03/20, 22:23 UTC.

Comité para a Eliminação de Discriminação contra Mulheres (2022), Observações finais sobre o décimo periódico de Portugal, Documento da Organização das Nações Unidas n.º CEDAW/C/PRT/CO/10, de 12 de julho de 2022, disponível em https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW%2fC%2fPRT%2fCO%2f10&Lang=en, último acesso: 2024/02/07, 15:35 UTC.

Conselho da Europa (2019). Obstetrical and gynecological violence. Resolução n.º 2306, de 3 de outubro de 2019 (34.ª sessão). Disponível em https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=28236&lang=en&fbclid=IwAR1Fs_3dBoi-tKCM7djPEsTgGik2ZWjLbuBM4yDJfDPvo2FX5imvAE6xSow, último acesso: 2023/03/07, 13:23 UTC.

Referências bibliográficas

Conselho da Europa, Convenção para a Prevenção e o Combate à Violência contra as Mulheres e a Violência Doméstica, adotada em Istambul, a 11 de maio de 2011, disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1878&tabela=leis, último acesso: 22/02/2024, 14h00 UTC.

Comissão Europeia (2020). Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, Uma União de Igualdade: Estratégia de Igualdade de Género 2020-2025, COM(2020) 152. Bruxelas, 5 de março de 2020. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0152&from=EN, último acesso: 2023/03/07, 13:31 UTC.

Comité para a Eliminação de Discriminação contra Mulheres (2018). S.F.M. v. Espanha, Comunicação n.º 138/2019, 28 de fevereiro de 2020, Documento da Organização das Nações Unidas n.º CEDAW/C/75/D/138/2018, disponível em https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW/C/75/D/138/2018&Lang=en, último acesso: 2023/03/07, 15:33 UTC.

O Senado e a Câmara de deputados da Nação Argentina (2009). Lei de proteção integral para prevenir, sancionar e erradicar a violência contra as mulheres nos âmbitos em que desenvolvem as suas relações interpessoais Nº26.485. Argentina. Disponível em https://edisciplinas.usp.br/mod/resource/view.php?id=2698517, último acesso: 2023/03/09, 10:21 UTC.

A Assembleia Nacional da República Bolivariana da Venezuela (2007). Lei Orgânica sobre o Direito das Mulheres a uma Vida Livre de Violência. Assembleia Nacional da República Bolivariana da Venezuela. Venezuela. Disponível em https://www.acnur.org/fileadmin/Documentos/BDL/2008/6604.pdf último acesso: 2023/03/09, 10:25 UTC.

Ministério da Justiça e Direitos Humanos da Nação. Secretaria de Direitos Humanos e Pluralismo Cultural Argentina (2004). Lei Nacional do Parto Humanizado Nº 25.959. Secretaria de Direitos Humanos e Pluralismo Cultural, Argentina. Argentina (2004) Disponível em https://www.argentina.gob.ar/sites/default/files/ley_25929_parto_humanizado_decreto_web_0.pdf , último acesso: 2023/03/09, 10:16 UTC.

Ministério da Justiça português (1963). Código Penal, Decreto-Lei n.º 48/85. Diário da República n.º 63/1995. Série I-A de 1995-03-15. Lisboa: Imprensa Nacional Casa da Moeda. Versão atualizada e consolidada. Disponível em https://dre.pt/dre/legislacao-consolidada/decreto-lei/1995-34437675, último acesso: 2023/03/07, 15:16 UTC

Parlamento Europeu (PE) (2021). Estratégia da UE para a Igualdade de Género — Resolução do Parlamento Europeu, de 21 de janeiro de 2021, 2019/2169, disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2021-0025_PT.pd, último acesso em 2023/03/09, 17h44 UTC.

Jurisprudência

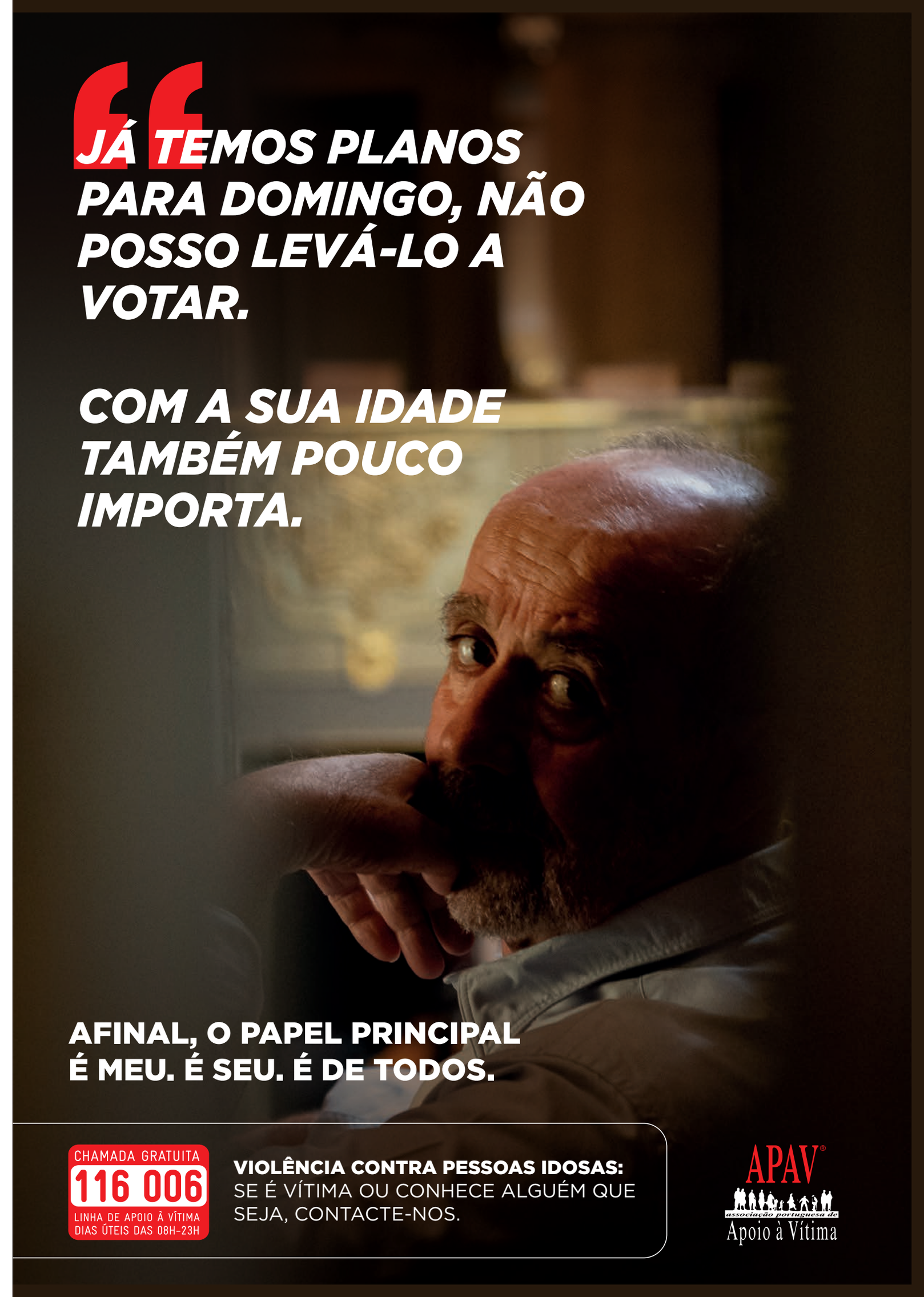
Tribunal Europeu dos Direitos Humanos:

VC c. Eslováquia, disponível em https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-107364%22]}

Ternovszky c. Hungria, disponível em https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-102254%22]}

Konovalova c. Rússia, disponível em https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-146773%22]}

Dubská c. República Checa, disponível em https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-148632%22]


“JÁ TEMOS PLANOS PARA DOMINGO, NÃO POSSO LEVÁ-LO A VOTAR.
COM A SUA IDADE TAMBÉM POUCO IMPORTA.
AFINAL, O PAPEL PRINCIPAL É MEU. É SEU. É DE TODOS.
CHAMADA GRATUITA
116 006
LINHA DE APOIO À VÍTIMA
DIAS ÚTEIS DAS 08H-23H
VIOLÊNCIA CONTRA PESSOAS IDOSAS:
SE É VÍTIMA OU CONHECE ALGUÉM QUE SEJA, CONTACTE-NOS.
APAV
associação portuguesa de
Apoio à Vítima

MISCELLANEA APAV N.º20

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-23H