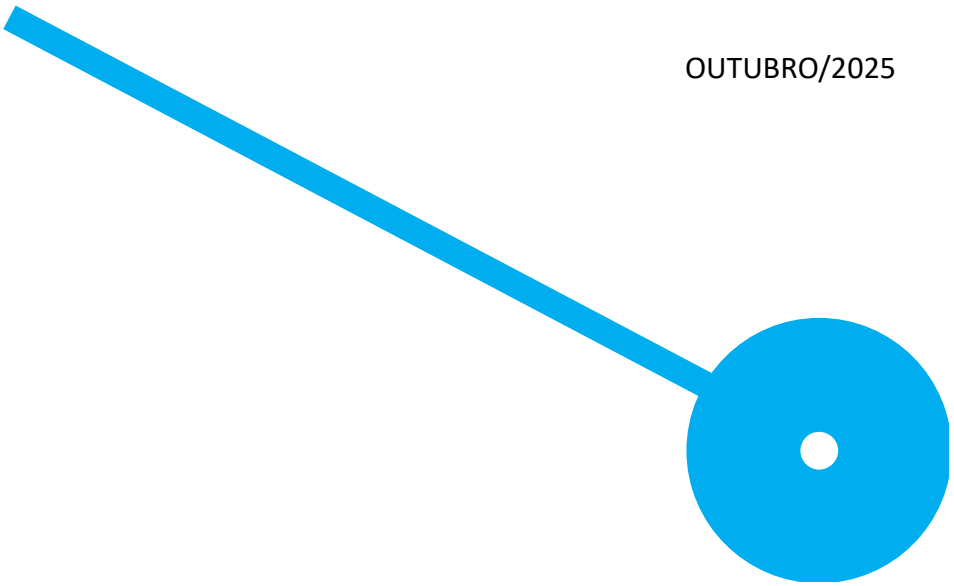
ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

MESTRADO
Práticas Jurídico-Digitais

O Fenómeno do *Sextortion*: Perspetivas Jurídica e Tecnológica

Paulo Lourenço



OUTUBRO/2025

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M MESTRADO
Práticas Jurídico-Digitais

O Fenómeno do *Sextortion*: Perspetivas Jurídica e Tecnológica

Paulo Lourenço
8230583

Orientadores

Professor DOUTOR Pedro Dias Venâncio

Professor DOUTOR Marco Vieira Gomes

Dissertação apresentado para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Práticas Jurídico-Digitais pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto.

OUTUBRO/2025

Declaração de Integridade

Eu, Paulo Jorge Enes Lourenço, estudante nº 8230583, do Mestrado de Práticas Jurídico-Digitais da Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto, declaro que não fiz plágio nem auto-plágio, pelo que o trabalho intitulado "O Fenómeno do *Sextortion*: Perspetivas Jurídica e Tecnológica" é original e da minha autoria, não tendo sido usado previamente para qualquer outro fim. Mais declaro que todas as fontes usadas estão citadas, no texto e na bibliografia final, segundo as regras de referenciação adotadas na instituição

Agradecimentos

Expresso um profundo agradecimento a todos os meus colegas e professores que, de alguma forma, contribuíram para esta caminhada.

Agradeço ainda de forma especial aos meus orientadores Professores, Dr. Pedro Venâncio e Dr. Marco Gomes, pela orientação científica e pela disponibilidade, tornando possível a conclusão deste trabalho.

Agradeço de igual forma à minha família, em especial à Anita Lourenço pela paciência e incentivo quando faltava motivação.

Resumo

A presente dissertação tem como objetivo compreender o fenómeno do *Cibersextortion*, entendido como a prática pela qual um agente, recorrendo às tecnologias de informação e comunicação (TIC), ameaça publicar conteúdos íntimos de uma vítima, com a intenção de obter vantagens patrimoniais, favores sexuais ou outras condutas que a vítima não aceitaria voluntariamente. Esta definição, ao adotar o prefixo "*Ciber*", distingue o fenómeno de figuras próximas, como a extorsão ou a coação sexual prevista no Código Penal e coloca-se no universo do ciberespaço. A questão central que orienta a investigação consiste em analisar de que forma o ordenamento jurídico português enquadra o *Cibersextortion* e em que medida a resposta legal e jurisprudencial se revela adequada face à evolução tecnológica e ao carácter transnacional do fenómeno. Para responder a esta questão, analisaram-se as condutas típicas mais comuns, que combinam engenharia social, manipulação psicológica, criação de perfis falsos e recurso a malware, incluindo práticas como *quishing* e *deepfakes*.

Por fim, conclui-se que o *Cibersextortion* afeta bens jurídicos diversos, abrangendo, não só a liberdade de autodeterminação sexual, a reserva da intimidade da vida privada e o património, mas igualmente a segurança e a confidencialidade de redes e sistemas informáticos ou, ainda, a privacidade e integridade dos dados pessoais. Constata-se ademais, uma significativa dispersão normativa, o que reforça a necessidade de investir na cibersegurança, na literacia digital e na cooperação internacional como meios essenciais para mitigar a proliferação do *Cibersextortion* e garantir a tutela efetiva dos direitos fundamentais.

Palavras-Chave: Cibercrime; *Cibersextortion*; Crime; Ofensores; Vítimas.

Abstract

This dissertation aims to understand the phenomenon of Cybersextortion, understood as the practice whereby an agent, using information and communication technologies (ICT), threatens to publish a victim's intimate content with the intent of obtaining financial advantages, sexual favors, or other conducts that the victim would not voluntarily accept. This definition, by adopting the prefix "Cyber," distinguishes the phenomenon from related concepts, such as extortion or sexual coercion as defined in the Penal Code, and situates it within the realm of cyberspace. The central research question is to analyze how the Portuguese legal framework addresses Cybersextortion and to what extent the legal and jurisprudential response proves adequate in the face of technological evolution and the transnational character of the phenomenon. To answer this question, this research analyzes the most common typical conducts, which combine social engineering, psychological manipulation, the creation of fake profiles, and the use of malware, including practices such as quishing and deepfakes.

Finally, the study concludes that Cybersextortion affects a diverse range of legally protected interests, encompassing not only the freedom of sexual self-determination, the right to privacy, and property, but also the security and confidentiality of computer networks and systems, as well as the privacy and integrity of personal data. Furthermore, a significant legislative fragmentation is noted, which reinforces the need to invest in cybersecurity, digital literacy, and international cooperation as essential means to mitigate the proliferation of Cybersextortion and to ensure the effective protection of fundamental rights.

Keywords: Crime; Cybercrime; Cybersextortion; Offenders; Victims.

Índice

Tabelas e Siglas

I.A.	Inteligência Artificial
CDADC	Código dos Direitos de Autor e Direitos Conexos
CP	Código Penal
CRP	Constituição da República Portuguesa
DoS.	Ataque de negação de serviço (*denial-of-service*)
DLG	Direitos Liberdades e Garantias
LC	Lei do Cibercrime
LPDP	Lei de Proteção dos Dados Pessoais
MP	Ministério Público
OPC	Órgão de Polícia Criminal
PJ	Polícia Judiciária
p.p.	Previsto e Punível
RASI	Relatório Anual de Segurança Interna
RAT	*Remote Access Trojan*
RGPD	Regulamento Geral de Proteção de Dados
ss.	Seguintes
USB	*Universal Serial Bus*
TC	Tribunal Constitucional
TIC	Tecnologia de Informação e Comunicação
VPN	*Virtual Private Networ*

I. Introdução

A utilização massiva por parte de crianças e jovens da *Internet* potenciou o surgimento de novas oportunidades e novas formas de praticar crimes. Oportunidades essas exploradas pelos ofensores tanto pela facilidade de contacto com as vítimas como pela facilidade de se manterem no anonimato (Guedes et al., 2022). A crescente centralidade das redes sociais, das plataformas de mensagens instantâneas e das aplicações de encontros nas dinâmicas sociais contemporâneas, aumentaram a exposição das pessoas aos riscos próprios do ciberespaço. A facilidade de partilha de informação pessoal combinada com a falsa perceção de segurança no uso das tecnologias, têm sido exploradas pelos ofensores. Estes recorrem a estratégias de engenharia social, manipulação psicológica e perfis falsos para ganharem a confiança das vítimas para, dessa forma, obterem conteúdos íntimos. Esta realidade tem originado um número crescente de queixas junto das autoridades policiais, como a Polícia Judiciária, e de referências em relatórios nacionais, como o Relatório Anual de Segurança Interna (RASI), que desde 2017 (RASI, 2017) passou a mencionar o *Cibersextortion* [1] como uma ameaça relevante à segurança digital.

A literatura académica internacional sobre o *Cibersextortion* tem vindo a crescer, refletindo a gravidade do fenómeno, mas no contexto português a investigação académica continua incipiente. Esta dissertação pretende contribuir para aprofundar este debate, analisando o fenómeno do *Cibersextortion* nas suas dimensões tecnológica e jurídica. Pretende igualmente demarcar o fenómeno do *Cibersextortion* de outras práticas próximas, como o *Revenge Porn*, o *Catfishing* e o *grooming online*.

O presente estudo está estruturado em duas partes complementares. Na primeira parte, de natureza teórica, é realizada a delimitação conceptual do *Cibersextortion*, a análise das suas tipologias e motivações, bem como do seu *modus operandi*, destacando a

[1] Apesar de o título da dissertação referir o termo *sextortion*, utiliza-se ao longo do texto a designação *Cibersextortion*, por se entender que o objeto de análise se circunscreve ao âmbito do ciberespaço e às condutas ali praticadas.

forma como os ofensores exploram as vulnerabilidades humanas e tecnológicas. Na segunda parte aborda-se o enquadramento jurídico nacional que permite tipificar e punir as condutas praticadas durante o *Cibersextortion*. Salienta-se o papel da Lei do Cibercrime (LC) [2], do Código Penal (CP) [3], da Lei de Proteção de Dados Pessoais (LPDP) [4] e da Convenção de Lanzarote [5], especialmente relevante na proteção de menores. Procede-se ainda à análise critica da jurisprudência nacional, com destaque para decisões recentes dos tribunais portugueses, que expõem a dispersão dos tipos penais aplicáveis à prática do *Cibersextortion*, por legislação extravagante. Por fim, nas conclusões, para além da referência ao impacto do fenómeno nas vítimas, quer no plano psicológico e social quer no plano patrimonial, sublinha-se a importância do desenvolvimento de políticas pública que articulem prevenção, literacia digital e apoio especializado.

II. Enquadramento teórico e conceitual do *Cibersextortion*

O *Cibersextortion* consolidou-se na última década como uma das formas mais preocupantes da criminalidade mediada pelas TIC. A sua análise exige uma compreensão clara da evolução do conceito, da sua distinção face a práticas afins e das motivações que orientam a atuação dos ofensores. Este capítulo apresenta o enquadramento teórico e conceptual do fenómeno, começando pela definição e evolução histórica do termo, incluindo a forma como passou a ser reconhecido em relatórios de segurança e nas práticas das autoridades. Aborda depois as nuances do *Cibersextortion* em relação a outras condutas criminais praticadas em linha (*online*), como o *Revenge porn*, o *Catfishing*, o *Cyberstalking*, o *Cyberbullying* e o *Grooming online*. Por fim, apresenta-se um catálogo de tipologias do *Cibersextortion*, organizado segundo as principais motivações identificadas na literatura (económicas, sexuais,

[2] Lei n.º 109/2009, de 15 de setembro – Diploma conhecido por lei do Cibercrime – disponível em https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-128879174

[3] https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1995-34437675 - Versão consolidada. Diário da República n.º 63/1995, Série I-A de 1995-03-15.

[4] Publicação: Diário da República n.º 151/2019, Série I de 2019-08-08, páginas 3 – 40 Emissor: Assembleia da República
Data de Publicação: 2019-08-08 - disponível em: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

[5] Convenção do Conselho da Europa para a Proteção das crianças contra a Exploração Sexual e os Abusos sexuais, que teve lugar em Lanzarote a 25 de outubro de 2007. Consultada em linha em: https://rm.coe.int/168046e1d8 - Acedido em 19/09/2025

pessoais e integradas) que serviu para identificar as estratégias usadas pelos ofensores e as vulnerabilidades que estes exploram nas vítimas. Esta abordagem inicial permitiu compreender a complexidade do fenómeno e serviu de base para a análise jurídica desenvolvida nos capítulos seguintes.

1. Definição e Evolução do Conceito

1.1 Etimologia do termo *Sextortion*

O Vocábulo *sextortion* resulta da combinação de duas palavras da língua inglesa, *sex* (sexo) e *extortion* (extorsão) (Nilsson et al., 2019 ; Ramalho & Ramalho, 2023 ; O'Malley & Smith, 2024; Da Silva, 2025). O termo *sextortion* não é novo. Embora tenha surgido na imprensa, em casos de extorsão sexual em linha, e no discurso público, com relativa frequência a partir de 2010, o jornal *Los Angeles Times* já em 1950 o tinha utilizado (Wittes et al., 2016; Los Angeles Times, 1950). Entre outros autores, Açar utiliza a expressão "*sexual extortion*", duas palavras, para se debruçar sobre o tema da extorsão sexual de crianças no ciberespaço (Açar, 2016). Os dois termos *"sextortion"* e *"sexual extortion"* surgem como sinónimos em situações de ameaça de divulgar imagens de natureza sexual da vítima caso esta não forneça mais imagens ou concorde com favores sexuais (Finkelhor et al., 2022). No mesmo contexto, o FBI (*Federal Bureau of Investigation*), tanto utiliza a expressão *"sexual extortion of children"* para se referir ao ato de coagir uma criança a produzir conteúdo sexual no qual retrate o seu corpo, como fotografias ou vídeos, sob ameaça de publicação de fotografias intimas previamente fornecidas ao ofensor (France, 2022), como os termos *"sexual extortion"* ou *"sextortion"* para, grosso modo, fazer referência a comportamentos semelhantes [6].

No contexto português o termo "*sextorsão*" é outra forma utilizada por autores e entidades públicas para se referirem a uma forma de chantagem sexual onde são usados filmes ou imagens para obter dinheiro das vítimas (Pereira et al., 2023). Por força do uso generalizado do termo *sextortion* por órgão de polícia criminal (OPC), académicos e

[6] https://www.justice.gov/usao-wdmi/pr/2023_0503_*Sextortion*_Indictment - Acedido em 17/09/2025

sociedade em geral durante a última década em Portugal - como, por exemplo, no alerta lançado pela Polícia Judiciária (PJ) em setembro 2015, onde o termo é utilizado para salientar o aumento de queixas relacionadas com o crime de devassa da vida privada e extorsão associados ao uso das redes sociais na *Internet* (Polícia Judiciária, 2015) -, a expressão ganhou relevância e é amplamente utilizada.

O termo *sextortion* surge pela primeira vez no RASI de 2017 onde é caracterizado como uma modalidade de extorsão baseada em *Malware* (RASI, 2017), ou seja, programa que é introduzido num sistema, geralmente de forma dissimulada, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicação ou do sistema operativo, ou perturbe a vítima (Paulsen & Byers, 2019).

No RASI de 2018, o termo *sextortion* surge no âmbito dos crimes ciberinstrumentais, ou seja, crimes cometidos através do uso de tecnologias informáticas, que servem como instrumento para praticas de crime, no caso organizado, (RASI, 2018) [7].

Nos RASI de 2019 e 2020, o termo *sextortion* não consta nos documentos. No entanto, ambos os relatórios fazem referência a situações que podem configurar a sua ocorrência. No caso do RASI de 2019, é referido que se registou um aumento da criminalidade investigada relativa à exploração sexual de menores *online* (RASI, 2019), *per se*, esta referência não indica a ocorrência de práticas de *sextortion*. No entanto, o relatório de 2020, assinala um aumento de casos onde, sob ameaça de divulgação de informações privadas, se exigia pagamentos em *criptomoedas* – Moeda Virtual- [8], atos que podem configurar alguma forma de *sextortion* (RASI, 2020).
No relatório de 2021 o termo *sextortion* surge novamente para dar conta do aumento significativo de incidentes da classe "recolha de Informação" onde é referido como dos

[7] Adiante abordaremos com maior profundidade as considerações doutrinais sobre os crimes instrumentais.
[8] A alínea d) do Artigo 2º, (Definições), da DIRETIVA (UE) 2019/713 DO PARLAMENTO EUROPEU E DO CONSELHO de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho, define como «Moeda virtual», uma representação digital de valor que não é emitida nem garantida por um banco central ou uma autoridade pública, não está necessariamente ligada a uma moeda legalmente estabelecida e não possui o estatuto jurídico de moeda ou dinheiro, mas que é aceite por pessoas singulares ou coletivas como meio de troca e pode ser transferida, armazenada e comercializada por via eletrónica.

casos mais comuns, ao lado de casos de *Vishing* [9] e *CEO Fraud* [10] (RASI, 2021). E, o Boletim do Observatório de Cibersegurança desse ano, refere que os casos categorizados como engenharia social pelo CERT.PT mais comuns no 1º semestre de 2021 foram o *sextortion* com (49%), seguido do *CEO Fraud* com (12%), da tentativa de burla mediante caso fictício de herança (11%) e da burla através de MBWay (7%) [11].

No RASI do ano seguinte o documento refere que, à semelhança de 2021, os ataques de engenharia social continuaram a ser predominantes, e o *sextortion* surge agora associado à receção de mensagens de correio eletrónico que implicam coação moral (RASI, 2022). Ou seja, enquanto no RASI de 2021 o termo *sextortion* aparece de forma abstrata enquadrado nos ataques de engenharia social, no RASI de 2022, "autonomiza-se" em relação ao *Vishing* e ao *CEO Fraud*, apresentando-se uma breve definição do conceito como "*essencialmente receção de mensagens de correio eletrónico que implicam coação moral*."(RASI, 2022).

No RASI de 2023 consta como definição "*A Sextortion refere-se a tentativas de extorsão através do envio de mensagens com a ameaça de exposição de imagens de teor íntimo da vítima*."(RASI, 2023). O RASI de 2024, mantendo a definição base de 2023, acrescenta que o *sextortion* é uma extorsão sexual cometida através de meio informático, e que continuava a ser uma ameaça relevante que representava 8% dos incidentes de Engenharia Social (RASI, 2024).

A utilização do termo "*sextortion*" neste trabalho, não implica que concordamos com o seu uso sem reservas, uma vez que entendemos que o termo mais adequado seria utilizar o prefixo (Ciber) ou (Cyber) para passar a se designar *Cibersextortion* ou *Cybersextortion* tal como acontece, por exemplo, com os termos *Cyberstalking*, *Cyberbullying* ou (Cibercrime) o que ajustaria o uso do termo ao espaço em que os atos

[9] No RASI 2021, considera-se *vishing* como a aprática de realizar chamadas telefónicas para validar dados ou transferência bancária ilicitamente efetuada. Disponível em https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNLI0NgcAIUgtZwUAAAA%3d – Acedido em 17/09/2025.

[10] No documento "Boas Práticas de Cibersegurança em Teletrabalho" consultado através do sítio *Internet* do CNCS em (https://www.cncs.gov.pt/docs/boas-prticas-de-cibersegurana-em-teletrabalho.pdf),
Refere o seguinte sobre *CEO Farud:* "Ocorre quando um colaborador autorizado a fazer pagamentos é ludibriado [por alguém que se faz passar pela chefia da organização] no sentido de pagar uma fatura falsa ou realizar uma transferência não autorizada da conta bancária da organização.", traduzida de NIST IR 7298 Revision 2, Glossary of Key Information Security Terms: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf) - Acedido em 17/09/2025.

[11] https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf - Acedido em 17/09/2025.

são praticados. Ou seja, se o *Cyberstalking*, o *Cyberbullying* e o Cibercrime são assim designados por serem praticados no ciberespaço, mas a sua prática pode ocorrer no mundo físico, de onde aliás são originários e identificados como *Stalking*, *Bullying* e crime respetivamente. Então, com o *sextortion* devia acontecer o mesmo. O *sextortion* é uma prática que pode ocorrer fora do ciberespaço e, a utilização desta designação, em nosso entender, poderá ser redutora da complexidade que se pretende abranger com o termo, uma vez que pode gerar confusão com, por exemplo, os crimes de Extorsão do artigo 223º ou o de Coação Sexual do artigo 163º, ambos do CP. Aliás, não existe no ordenamento jurídico português o crime de *sextortion*, sendo estes atos punidos por recurso a esses e a outros crimes previstos para o mundo físico.

Posto isto, e tendo em vista a delimitação dos comportamentos que pretendemos analisar com este trabalho, optamos por passar a utilizar o termo *Cibersextortion,* mais adequado ao idioma português. Ou seja, passaremos a usar o termo *Cibersextortion* para nos referirmos aos atos em que, de grosso modo, o agente, através das tecnologias de comunicação - entenda-se meios de comunicação digitais -, na posse real ou presumida de imagens, vídeos ou mensagens de texto da vítima, ameaçar divulgar os ficheiros para extorquir valores pecuniários, manter a vítima num estado de submissão que permita ceder a favores ou atos sexuais, ou qualquer exigência que de outra forma a vítima não aceitaria praticar. Por questões de coerência, sempre que possível adaptaremos igualmente as referências encontradas na literatura ao termo s*extortion* para *Cibersextortion*, como alias já temos vindo a fazer.

1.2 *Cibersextortion* e outros "crimes" praticados em linha

Durante a elaboração deste trabalho encontramos várias posições sobre aquilo que se entende por *Cibersextortion*. Em alguns casos o fenómeno é confundido com outras práticas de caraterísticas muito próximas, mas que na sua essência se afastam dele (Ramalho & Ramalho, 2023). Os académicos, a comunicação social e o público em geral confundem frequentemente o *Cibersextortion* com o *Revenge Porn*, expressão utilizada para se referir a pornografia de vingança que consiste na publicação de imagens ou

vídeos de cariz sexual da vítima nas redes públicas. Conteúdos esses, cedidos ao ofensor de forma voluntária por meio da prática de *sexting* [12].

Ou seja, troca, entre pessoas durante uma relação amorosa consensual, ou outra forma não consentida, de imagens ou vídeos de cariz sexual onde, depois da vontade manifestada por uma das partes pelo fim do relacionamento, o agente, na tentativa de o manter, ameaça a vítima de publicar na *Internet* os ficheiros íntimos que tem em sua posse. A prática de *revenge porn* pode acontecer igualmente após o fim da relação, aqui o ofensor publica os ficheiros comprometedores na *Internet* com o objetivo de humilhar a vítima (Ramalho & Ramalho, 2023).

Embora estes crimes, *Cibersextortion* e *Revenge Porn*, sejam frequentemente associados, devem ser diferenciados. O *Revenge Porn* caracteriza-se pela partilha não consensual de material de cariz sexual de uma vítima, usualmente com o objetivo de lhe causar "embaraço". O *Cibersextortion* também envolve a ameaça de publicar material de cariz sexual relativo à vítima, mas neste caso sob a exigência de determinadas contrapartidas ilegítimas, muitas vezes pecuniárias. Esta relação entre os dois crimes contribui para a confusão. Acresce que tanto o *Cibersextortion* como o *Revenge Porn* são crimes relacionados com o sexo, mas ao contrário do *Revenge Porn*, o *Cibersextortion* depende em grande medida do silêncio forçado da vítima para ter sucesso. O objetivo do *Cibersextortion* é tipicamente obter material sexual ou dinheiro e, o silêncio e o medo de exposição pública da vítima são vitais para atingir esses objetivos. Portanto, no *Cibersextortion*, mesmo que o ofensor tenha acesso a informações privadas da vítima, não significa que as divulgará. Enquanto o objetivo do *Revenge porn* é disseminar o conteúdo sexualmente explícito da vítima e o silêncio da vítima não impede que objetivos do sejam alcançados (Hedidi, 2023).

[12] O termo *sexting* resulta das palavras 'sex' (sexo) e 'texting' (envio de SMS) e significa a troca de mensagens eróticas com ou sem fotos via telemóvel, chats ou redes sociais. O maior perigo do *sexting* é que essas fotos ou mensagens acabem espalhadas pela Net ou nas mãos de pessoas erradas! O fenómeno do *sexting* é especialmente comum entre adolescentes e jovens adultos. Na grande maioria das vezes as imagens ou mensagens íntimas são enviadas no contexto de uma relação de namoro com motivações diversas: Fornecer uma "prova de amor "pelo envio de fotos eróticas; Desejo de afirmar audácia e autoconfiança exibindo o corpo de forma sedutora; Solicitar ao parceiro(a) para fazê-lo sob a forma de chantagem emocional; Ser aliciado por alguém a fazê-lo durante uma conversa *online;* Enviar fotos ou mensagens de terceiros por vingança; Enviar fotos ou mensagens por erro (em especial a partir de um telemóvel). https://www.internetsegura.pt/Sexting - Acedido em 17/09/2025.

A prática conhecida por *Catfishing* é outra forma, e verifica-se quando o agente, por meio da ocultação da sua verdadeira identidade, leva a vítima a acreditar que está numa relação romântica baseada na boa-fé, mas na qual o agente apenas está interessado na obtenção de benefícios financeiros e gratificações sexuais (Reis, 2024).

O *Cyberstalking*, perseguição através dos meios digitais, é fundamentalmente o ato de perseguir alguém, mas no ciberespaço. Por exemplo, o *stalker* enviar mensagens de forma insistente, mesmo que a vítima não responda, seguir a vítima em todas as redes sociais para dessa forma monitorar a sua vida, reagindo a todas as suas publicações e comentários[13]. Ou seja, o *Cyberstalking* pode ser definido como uma forma de perseguição que utiliza a *Internet* ou outra tecnologia eletrónica, com intenção de assediar ou perseguir a vítima, o que, pela persistência nas abordagens, lhe provoca constrangimento e medo (Goncalves, 2023; Pereira & Matos, 2015).

O *Cyberbullying*, à semelhança do *Cyberstalking*, é uma prática antiga, mas potenciada pelo advento da *Internet*. Ganhando assim os prefixos "Cyber". Dessa forma, se o *Cyberstalking* corresponde à ação de perseguir alguém através de meios digitais, no caso do Cyberbullying, corresponde a comportamentos intencionais e repetitivos de agressões entre indivíduos onde o mais forte agride o mais fraco (Pereira & Matos, 2015), mas igualmente através de meios digitais (Guedes et al., 2025), onde os seus efeitos podem ter impactos maiores nas vítimas. Aqui, o agressor pode tornar-se omnipresente na vida da vítima, a distância que os separa está ao alcance do envio de uma nova mensagem, reação a uma publicação ou publicações espontâneas constrangedoras para a vítima nas redes sociais desta[14].

O *grooming* é outro comportamento trazido para o universo digital, sendo designado na literatura especializada como "*grooming online*" e tida como a prática através da qual os ofensores escondem a sua verdadeira identidade para manipular a vítima, a maior parte das vezes mais jovens (Casa Branca et al., 2016) e que, em casos de *Cibersextortion*, solicitam a partilha de conteúdos sexuais ou encontros presenciais.

[13] https://quor.pt/criminal/stalking-redes/ - Acedido em 17/09/2025
[14] https://www.internetsegura.pt/sites/default/files/2020-12/FA_CyberBullying.pdf - Acedido em 17/09/2025

O *grooming online* e o *Catfishing* são formas de manipulação que utilizam os meios digitais, mas que embora se sobreponham em alguns aspetos táticos, apresentam características diferentes. O *grooming* é uma estratégia predadora, deliberada e prolongada no tempo que visa a construção de confiança através da introdução progressiva de conversas sexualizadas do *groomer* com vítimas, na maior parte das vezes menor de idade, e tendo como principal objetivo a exploração sexual (Wittes et al., 2016; Liggett, 2019).

Por seu turno, o *catfishing*, como vimos acima, consiste na criação de uma identidade falsa para enganar as vítimas, que podem ser menores ou adultas e com propósitos mais diversos (Edwards & Hollely, 2023; Wittes et al., 2016). Estes podem incluir obtenção de material sexualmente explícito para chantagem, lucro financeiro em fraudes românticas ou vingança, não se cingindo a exploração sexual de menores apresentando-se assim como uma estratégia mais abrangente de dissimulação (Ray & Henry, 2023).

1.3 Catálogo de tipologias de *Cibersextortion*

O fenómeno do *Cibersextortion* que aqui se pretende analisar carece, como vimos acima, de melhor delimitação tanto no uso desta designação, tanto quanto aos atos praticados pelos ofensores, de modo a permitir enquadrar os vários comportamentos nos tipos legais de crime existentes. Caso contrário, o catálogo de termos utilizados para enquadrar juridicamente comportamentos semelhantes, pode dispersar daquilo que é essencial, ou seja, da previsão legal existente para proteção de bens jurídicos tidos na doutrina e na sociedade em geral como merecedores de tutela penal (Dias, 2001). O *Cibersextortion* pode ser executado de várias formas e em várias situações dependendo das motivações dos ofensores. Neste ponto apresentamos formas pelas quais o *Cibersextortion* é praticado. Apesar da panóplia de motivações encontradas, e correndo o risco de não englobar todas elas, identificam-se quatro categorias principais que motivam os ofensores a praticarem *Cibersextortion*, são elas, económicas, sexuais, pessoais e integrada (Wolak & Finkelhor, 2016; Liggett, 2019; O'Malley & Holt, 2022; Henry & Umbach, 2024).

1.3.1 Motivações económicas

Nas motivações económicas encontram-se aquelas em que o ofensor, na posse dos ficheiros da vítima, age de forma a obter ganhos financeiros para si ou para terceiros (Edwards & Hollely, 2023), e são mais frequentemente relatados em situações de crime organizado (O'Malley & Holt, 2022). Este *modus operandi*, tem como alvo principal os homens, maioritariamente na faixa etária entre os 20 e os 39 anos de idade (Edwards & Hollely, 2023; O'Malley & Smith, 2024).

Nestas situações, os ofensores criam perfis falsos em plataformas *online*, muitas vezes fazendo-se passar por mulheres jovens e atraentes com intenção de estabelecer uma relação amorosa com a vítima (O'Malley & Holt, 2022; Wittes et al., 2016). Trata-se de casos enquadráveis na prática de *Catfishing*, em que as vítimas são persuadidas a participar em sessões de exposição sexual através de *webcam* ou a partilhar imagens e vídeos sexualmente explícitos. Esses ficheiros são posteriormente utilizados para ameaçar a vítima com a divulgação publica do material, caso não pague determinada quantia pecuniária (Liggett, 2019; Wolak & Finkelhor, 2016).

Em alguns casos os ofensores recorrem à ameaça de publicar materiais sexualmente explícitos das vítimas, mesmo que não os possuam, mas que, por meio de *e-mails* de *phishing* [15] onde alegam ter gravado a vítima em atos sexuais (Pethers & Bello, 2023) ou pela utilização de *deepfake* [16] (Tzani et al., 2024), levam a vítima a acreditar que são detentores desses materiais. Para garantirem sucesso, os ofensores imprimem urgência nas ações da vítima, para dessa forma causar medo e ansiedade com o intuito de aumentar as probabilidades de um pagamento (Liggett, 2019; O' Malley, 2023). O medo do cibercrime contra a propriedade está sobretudo associado à insegurança

[15] O *phishing* deve o seu nome à palavra inglesa "*fishing*" que significa "pescar", uma vez que estes grupos lançam o anzol e fazem-se passar por entidades geralmente conhecidas e credíveis, para obter acesso a contas privadas. A prática consiste em utilizar métodos tecnológicos que levam o utilizador a revelar dados pessoais e/ou confidenciais. Este tipo de ataques é geralmente acompanhado por mensagens de *SPAM*, enviadas para vários utilizadores. Embora possam haver tipos de *phishing* que pedem os dados directamente por resposta ao e-mail, na maioria dos casos, estão articulados com um website onde o utilizador preenche os seus dados. Geralmente os dados pessoais roubados dizem respeito a informações de contas bancárias, logins de contas online e outras informações confidenciais. Disponível em - https://www.internetsegura.pt/Phishing - Acedido em 17/09/2025

[16] Os *deepfakes* são imagens, vídeos ou gravações de áudio criados por inteligência artificial, que parecem reais, mas foram manipulados digitalmente ou falsificados. - https://cnnportugal.iol.pt/deepfakes/abuso-sexual/deepfakes-podem-causar-danos-duradouros-nas-criancas-saiba-como-as-proteger/20250329/67e29f2fd34ef72ee443e42f - Acedido em 17/09/2025

económica. Já o medo do cibercrime interpessoal é menos influenciado por fatores socioeconómicos. Nesse caso, pesa mais a perceção do crime interpessoal no mundo físico (Guedes et al., 2025).

O esquema predatório, não raras vezes, inicia-se nas redes sociais como ou Instagram, em aplicações de encontros como *Tinder* ou *OkCupid* e aplicações de mensagens com *Skype* ou *WhatsApp* (Edwards & Hollely, 2023; Tzani et al., 2024). Segundo alguns estudos esta modalidade de *Cibersextortion* financeiro e organizado, tem os seus *hotspots* em países como as Filipinas, Costa do Marfim e Marrocos e Estados Unidos, frequentemente ligados a áreas com altos indicadores de pobreza e corrupção (Liggett, 2019; Edwards & Hollely, 2023). As vítimas desta modalidade de *Cibersextortion* sofrem perdas financeiras significativas e danos psicológicos severos, causados por sentimento como vergonha e culpa que pode levar a ideação suicida (Nilsson et al., 2019; O'Malley & Smith, 2024).

1.3.2 Motivações sexuais

Por motivações sexuais entende-se aqueles casos em que o ofensor pretende obter da vítima favores sexuais, sejam presenciais ou através da *Internet*, ou materiais sexualmente explicito como fotografias ou vídeos. Ou seja, o que motiva o ofensor para agir é a gratificação sexual, seja em encontros presenciais ou mediados por meios digitais (Liggett, 2019; Ray & Henry, 2024). Nesta modalidade de *Cibersextortion*, os menores e as mulheres são mais visadas pelos ofensores (Wolak et al., 2018; Ray & Henry, 2024) e a obtenção inicial dos materiais sexualmente explicito ocorre, por exemplo, com recurso ao *grooming online* onde os ofensores podem passar a ideia de terem a mesma idade das vítimas para criar um vínculo *online* e dessa forma, progressivamente, solicitarem a produção e envio de conteúdos sexualmente explícitos, como fotografias de partes do corpo, atos sexuais gravados em vídeo ou recreação de fantasias sexuais específicas, que podem expor características psicológicas dos ofensores como, por exemplo, a identificação de parafilias como o sadismo, hebefilia ou a pedófila (Liggett, 2019). Outra forma dos ofensores chegarem às vítimas é através da manipulação em redes sociais, tal como acontece no *Cibersextortion* com motivações

financeiras, e, em menor grau, através de *hacking* [17] ou gravações sem autorização da vítima (Tzani et al., 2024).

Quanto às vítimas desta modalidade, fatores psicológicos como níveis de ansiedade elevados associados ao medo de rejeição e abandono e à descoberta da sexualidade podem aumentar a sua vulnerabilidade, tornando-as alvos mais suscetíveis à pressão psicológica e manipulação dos predadores que buscam gratificação sexual (Tzani et al., 2024). Este tipo de *Cibersextortion*, intrinsecamente associado à exploração sexual e à violência sexual facilitada pela tecnologia está muitas vezes ligado à exploração sexual infantil e em linha, visando com frequência a produção e divulgação de material de abuso sexual infantil (Edwards & Hollely, 2023; Wittes et al., 2016). A pressão exercida pelo ofensor sobre a vítima para que cumpra as exigências, sob ameaça de exposição pública dos seus ficheiros íntimos, é um elemento central para se identificar a natureza predadora desses indivíduos e as graves consequências emocionais, psicológicas e sociais para as vítimas (Nilsson et al., 2019).

1.3.3 Motivações pessoais

No caso da prática do *Cibersextortion* por motivações pessoais, o ofensor age para se vingar ou exercer poder e controlo sobre a vítima. Ou seja, utiliza a ameaça de publicar os conteúdos íntimos que tem em sua posse para controlar o comportamento da vítima, exercer domínio sobre ela e impor a sua vontade (Ray & Henry, 2024; Liggett, 2019). Esta forma de agir é particularmente comum em casos de *Cibersextortion* ocorridos durante ou após relações de namoro ou de mera intimidade sexual. Prática denominada de *Revenge Porn*. Através da qual, como acima exposto, o agressor obtém os ficheiros comprometedores da vítima de forma consensual, por exemplo, através da prática de *sexting*, para posteriormente ameaçar a vítima com a sua publicação caso não cumpra com exigências como permanecer num relacionamento indesejado, encontrar-se contra

[17] O *hacking* (também chamado de cyber *hacking*) é a utilização de meios não convencionais ou ilícitos para obter acesso não autorizado a um dispositivo digital, sistema informático ou rede de computadores. O exemplo clássico é um cibercriminoso que explora vulnerabilidades de segurança para invadir uma rede e roubar dados. Os *hackers* dividem-se em 3 categorias principais, com base nos seus motivos e táticas: *Hackers* maliciosos "*black hat hackers* ", que pirateiam para causar danos; Hackers éticos "*white hat hackers*" (que pirateiam para proteger empresas de danos; *Hackers* vigilantes ou "*gray hat hackers*" que confundem a linha entre *hacking* "bom" e "mau". https://www.ibm.com/think/topics/cyber-hacking - tradução nossa - Acedido em 18/09/2025.

sua vontade com o agressor ou a cumprir com listas de exigências e regras impostas pelo agressor (Wolak & Finkelhor, 2016).

Em boa verdade, o *Revenge Porn*, quando praticado com recurso às TIC e existe ameaça para obter vantagem, é uma forma de *Cibersextortion* na medida em que consagra todos os seus elementos característicos. Vejamos, o *Cibersextortion* é caracterizado pela posse de ficheiros sexualmente comprometedores da vítima, seguido da ameaça de divulgação condicionada a uma contrapartida e, caso essas contrapartidas não sejam realizadas, dá-se a publicação dos ficheiros. Consumando-se dessa forma a prática de *Cibersextortion*.

Neste contexto das motivações pessoais de *Cibersextortion*, as mulheres surgem como as principais vítimas e, como principais ofensores, surgem os parceiros íntimos ou ex-parceiros que procuram manter controlo e poder sobre a vítima (O'Malley & Holt, 2022; Liggett, 2019). Esta forma de *Cibersextortion* está muitas vezes associada a violência no namoro, casos de *Cyberstalking* e outras formas de abuso com recurso a imagens (Wolak et al., 2018), onde a ameaça surge como parte de um padrão mais amplo de abuso e coação (Ray & Henry, 2023). Os impactos nas vítimas desta forma de *Cibersextortion* é igualmente traumática causando ansiedade duradoura, perda de relacionamentos com familiares e amigos, problemas no trabalho ou escola e sofrimento emocional significativo (Wolak et al., 2018; O' Malley, 2023).

1.3.4 Motivações integradas

Cibersextortion motivado por razões integradas, ou seja, motivações que podem ocorrer pela combinação de duas ou mais categorias acima descritas, daquelas com outras ou ainda, com outros métodos complementares. A ver, o ofensor pode obter os ficheiros comprometedores de diversas formas, pelo *hacking*, por exemplo, através do uso de *keyloggers* [18], *malware* para *webcams* ou ataques de força bruta para obter palavras-

[18] Trata-se de um programa concebido para registar quais as teclas que são premidas num teclado de computador utilizado para obter palavras-passe ou chaves de encriptação e, assim, ignorar outras medidas de segurança. Ou ainda, de um programa remoto concebido para registar quais as teclas que são premidas num teclado de computador, utilizado para obter palavras-passe ou chaves

passe e aceder a dispositivos ou aplicações informáticas da vítima. Pode ainda dar-se o caso de o ofensor furtar ou roubar os equipamentos da vítima (Liggett, 2019; Wittes et al., 2016).

Nas motivações económicas identificamos o uso de *deepfake* como uma das práticas usadas como meio de obtenção de ficheiros comprometedores das vítimas, mas o uso dessa tecnologia não é exclusivo dessa forma de atuar, tal como nenhuma das outras formas de obter os materiais comprometedores o é. Neste contexto integrado de motivações para a ação dos ofensores, o recurso a *deepfake*, tal como acima referido, elimina a necessidade de adquirir material explicito real o que torna a sua utilização possível em qualquer uma das motivações identificadas (Tzani et al., 2024). Fica assim claro que as motivações subsequentes que levam ao *Cibersextortion* podem configurar qualquer uma das acima mencionadas.

III. Perspetiva tecnológica

Este capítulo versa sobre as principais técnicas e instrumentos utilizados. Apresenta-se a forma como são aplicados para recolher informações e ganhar a confiança da vítima e, posteriormente, transformar esses dados em instrumentos de ameaça. A análise inicia-se com a engenharia social, onde se percebe a manipulação da perceção e do comportamento humano como vulnerabilidade a ataques informáticos. Segue-se a abordagem de ataques por recurso a programas informáticos maliciosos, como *Keyloggers*, ferramentas de captura de captura de ecrã ou programas que potenciam acesso ilícito aos dispositivos e aumentam a capacidade coerciva do ofensor. São ainda abordadas estratégias que utilizam *e-mails* e o papel das plataformas digitais, como redes sociais *online*, serviços de mensagens e ambientes de videojogos, na seleção e abordagem às vítimas. Conclui-se o presente capítulo com algumas considerações sobre as práticas de manipulação psicológica, a utilização de perfis falsos e a criação de

de encriptação e, assim, ignorar outras medidas de segurança. https://csrc.nist.gov/glossary/term/key_logger - tradução nossa - Acedido em 18/09/2025

vínculos afetivos artificiais. Recursos que permitem aos ofensores prolongar o controlo e intensificar a vulnerabilidade das vítimas.

1 *Modus operandi*

Compreender o *modus operandi* dos ofensores é essencial para perceber como o fenómeno do *Cibersextortion* se concretiza na prática. A forma como os agressores obtêm acesso aos conteúdos íntimos e exercem pressão sobre as vítimas revela o recurso à vulnerabilidade humana, à exploração tecnológica e a estratégias psicológicas de forma combinada.

1.1 Engenharia Social

Em cibersegurança, o fator humano está diretamente ligado ao sucesso ou insucesso dos ataques levados a cabo através de esquemas de engenharia social e ao grau de ignorância dos utilizadores relativamente às boas práticas em cibersegurança. Por essa razão, a caraterística mais comum nos ataques modernos é concentrarem-se no elo mais fraco da cadeia de segurança, ou seja, no ser humano (Winnefeld Jr. et al., 2015). Se tais situações ocorrem em contexto de cibersegurança, onde existe formação e treino específico, então a vulnerabilidade das pessoas comuns é ainda maior. Estas não dispõem da mesma preparação nem estão suficientemente sensibilizadas para este tipo de ataque. Ou seja, em contexto de *Cibersextortion*, estas práticas revelam-se como uma das técnicas de ataque mais utilizadas pelos ofensores.

Os ataques de engenharia social podem, no que respeita à primeira recolha de informação da vítima, ter início tanto no ambiente físico, através, por exemplo, da recolha e análise do lixo no local de trabalho da vítima, como através de ações psicológicas, como persuasão, criação de confiança ou simplesmente sendo gentil (Coelho, 2013). Fica claro que esta prática assenta na manipulação das perceções, emoções e padrões de confiança das vítimas, conduzindo-as a adotar comportamentos que expõem os seus dados pessoais ou, no caso do *Cibersextortion*, conteúdo íntimos,

frequentemente sem que estas se apercebam de imediato da gravidade da situação (Tavares, 2017). Ao contrário de outros métodos de ataque, não exige, em muitos casos, grande sofisticação tecnológica numa fase inicial, bastando a construção de pretextos convincentes que induzam a vítima a partilhar informações ou executar ações suscetíveis de comprometer a sua privacidade (Europol, 2018).

Nos ambientes digitais, a engenharia social manifesta-se através de correio eletrónico, mensagens instantâneas, chamadas telefónicas (*vishing*) [19] ou mensagens de texto (*smishing*) [20]. Estes ataques são mais fáceis de concretizar do que a exploração de vulnerabilidades técnicas, uma vez que não exigem investimento significativo, requerem apenas os custos associados ao envio de mensagens ou chamadas telefónicas (Tavares, 2017). A escolha do meio de contato depende, assim, em larga medida, do perfil da vítima e da avaliação feita pelo agressor sobre a plataforma onde julga haver maior probabilidade de sucesso. Não raras vezes, a aproximação inicia-se com mensagens aparentemente legítimas, enviadas a partir de contas criadas para o efeito, com o objetivo de conferir credibilidade à abordagem.

O recurso à personalização é outra estratégia recorrente, os ofensores consultam dados públicos da vítima nas redes sociais como nomes de familiares, de colegas, localizações que frequentou ou interesses pessoais, para serem incorporados nas abordagens e dessa forma aumentar a confiança na comunicação e criar a ilusão de proximidade. O uso, igualmente corrente, de serviços e ferramentas de I.A. Generativa aumentam a "qualidade" da personalização bem como a quantidade de ataques. No caso particular do *Cibersextortion*, a manipulação psicológica é frequentemente combinada com elementos técnicos, de modo a ampliar a eficácia da ação criminosa. Dessa forma, as campanhas de *phishing* podem ser acompanhadas de anexos infetados com *malware* que depois de instalado nos dispositivos eletrónicos, exploram simultaneamente tanto

[19] ***Smishing*** – baseia-se no envio de uma mensagem de telemóvel (SMS ou MMS), confirmando o vínculo a uma empresa de serviços que irá cobrar uma quantia diária, caso o utilizador não anule o vínculo através do website da empresa. A tentativa de *phishing* ocorre no próprio *website*, sendo este o meio de obter os dados do utilizador. Disponível em - https://www.internetsegura.pt/Phishing - Acedido em 17/09/2025

[20] ***Vishing*** – trata-se de um *e-mail* que aparenta ser de uma instituição totalmente legítima, convidando o utilizador a contactar a entidade por telefone. No momento da chamada, o utilizador não é atendido por uma pessoa, mas sim por um atendedor automático, que solicita vários dados pessoais para "verificação de segurança". Disponível em - https://www.internetsegura.pt/Phishing - Acedido em 17/09/2025

a vulnerabilidade humana como vulnerabilidades técnicas. Algumas vezes os ofensores, recorrem mesmo à engenharia social como etapa preliminar de um ataque mais amplo. Por exemplo, o primeiro contacto via rede social pode servir para persuadir a vítima a clicar num *link* malicioso que instala um *software* de captura remota do ecrã ou do microfone ou para instalar uma aplicação aparentemente inofensiva que, na realidade funciona como *spyware* (Europol, 2023).

Neste contexto, o aproveitamento de funcionalidades legítimas dos sistemas operativos, utilizadas aqui para fins ilícitos, permite ao agressor manter controlo sobre o dispositivo da vítima sem desencadear sinais de alarme evidente. A sofisticação dessa prática aumenta quando se observa a sua utilização coordenada por grupos criminosos estruturados. Nestes casos, cada membro especializa-se em tarefas específicas. Uns constroem as narrativas persuasivas adaptadas ao perfil da vítima, outros, por exemplo, dedicam-se a replicar *interfaces* de páginas legítimas para obter credenciais ou conteúdos multimédia sob pretextos artificiais, como concursos falsos ou projetos artísticos simulados. Esta divisão de tarefas aumenta a taxa de sucesso, até porque o acesso a *kits* de *phishing* disponíveis no submundo digital, e a capacidade de replicar comunicações institucionais, estão ao alcance de qualquer pessoa sem conhecimentos avançados em programação informática (Europol, 2023).

1.2 Programas informáticos com fins maliciosos

A utilização de programas informáticos para fins maliciosos constitui um dos elementos mais caracterizadores do *modus operandi* do *Cibersextortion*. Estas ferramentas permitem aos ofensores ultrapassar as barreiras físicas e técnicas que, em circunstâncias normais, protegiam a intimidade e os dados pessoais das vítimas. A relevância de tais programas decorre não apenas da capacidade de obter conteúdos íntimos sem o consentimento do utilizador legitimo, mas também do potencial de amplificar o poder coercivo do ofensor nas fases seguintes do processo de extorsão. Ao contrário das práticas exclusivamente baseadas na engenharia social, que dependem em larga medida da colaboração involuntária da vítima, os programas maliciosos conferem ao agressor

meios de intrusão, como a recolha furtiva de dados ou o controlo remoto de dispositivos.

Nesta secção analisam-se as principais ferramentas empregues neste contexto. Abordam-se ferramentas de captura de teclas utilizadas e de ecrã, que permitem a apropriação de credenciais, mensagens privadas e imagens sem autorização. Em seguida, aborda-se o acesso remoto a dispositivos, que conferem ao agressor um controlo quase total sobre os sistemas comprometidos. E, por fim, examina-se a importância do *phishing*, não apenas como técnica de manipulação, mas igualmente como vetor de instalação de *software* malicioso de obtenção de credencias que facilitam as fases subsequentes do ataque.

1.2.1 *Keyloggers* e Captura de Ecrã

O recurso a *keylogger* é uma prática frequente no *Cibersextortion*. Trata-se de um tipo de *malware* que regista todas as teclas digitadas num dispositivo, permitindo ao ofensor o acesso a credenciais, mensagens privadas e outros dados sensíveis da vítima (Wittes et al., 2016; Liska & Gallo, 2017), também se utilizam programas de captura de ecrã, que funcionam como meios intrusivos de apropriação indevida de informação confidencial e de conteúdos potencialmente comprometedores.

Conteúdo esses que podem ser transmitidos em tempo real para dispositivos dos ofensores ou gravados nos dispositivos das vítimas e posteriormente recuperados pelos atacantes. A captura de ecrã permite recolher imagens, de forma periódica ou continua, do que se encontra visível no monitor da vítima, podendo abranger conversas privadas em redes sociais, fotografias pessoais ou mesmo sessões de videochamada. Ou ainda, ativar a *webcam* dos dispositivos sem o consentimento da vítima e dessa forma obter imagens do ambiente físico onde a vítima se encontra (Humelnicu, 2017).

O uso em simultâneo de *keylogger* e ferramenta de captura de ecrã aumenta significativamente a eficácia da abordagem à vítima. Vejamos, enquanto o primeiro

garante acesso total a *logins*, mensagens e pesquisas realizadas, a segunda fornece um acervo visual suscetível de ser explorado diretamente em ameaças de cariz íntimo (Justice, 2023) [21]. Esta combinação reduz a necessidade de colaboração voluntária da vítima. Essa característica é típica de estratégias baseadas apenas em engenharia social. O conteúdo recolhido de forma ilícita é transferido para quem gere o programa de *malware*. Em contexto de *Cibersextortion*, os ataques seguem geralmente uma lógica estável (Ramalho & Ramalho, 2020). O processo começa pela infeção do sistema da vítima, que pode ocorrer através de diversas técnicas de engenharia social (Ollmann, 2007). Entre estas o *phishing* é um dos métodos mais comum (Gomes, 2019). Esta técnica consiste no envio de mensagens fraudulentas, geralmente por correio eletrónico, que aparentam ser de fontes legítimas para induzir o utilizador a clicar em *links* maliciosos ou a descarregar anexos corrompidos (Liska & Gallo, 2017).

Outra forma de infeção ocorre através de meios físicos, como um *pen-drive USB* [22] infetado que é ligada aos equipamentos das vítimas (Gomes, 2019). Dessa forma o sistema informático fica comprometido e torna possível a instalação e configuração remota do *software* malicioso, como os já referidos *Keyloggers* ou outros programas de captura de dados (Gonçalves, 2015). A utilização destas ferramentas no *Cibersextortion* está frequentemente associada a mercados ilícitos. Nos quais se pode encontrar esses programas de *malware* e *spyware*. A utilização desta técnica aumenta significativamente o controlo psicológicos sobre a vítima.

Ao contrário das abordagens baseadas apenas em perfis falso, explorados mais adiante, em ataques por meio de *keyloggers* e captura de ecrã automática, a vítima é muitas vezes confrontada com ficheiros concretos, seja de imagens, transcrições completas de conversas íntimas ou capturas de conteúdos pessoais guardados nos dispositivos atacados (Gonçalves, 2015). Este *modus operandi* reduz de forma significativa a capacidade de reação da vítima devido ao estado de choque provocado por um lado pela abordagem do ofensor e, por outro pelo medo de exposição pública (Reis, 2024).

[21] Disponível no site da *U.S Department of Justice* em (https://www.justice.gov/d9/2023-06/*sextortion* crowdsourcing enticement and coercion 2.pdf) - Acedido em 17/09/2025

[22] Dispositivo de armazenamento físico de dados, portátil, que pode ser ligado diretamente nos dispositivos que possuam uma entrada USB (*Universal Serial Bus*)

Estas técnicas, embora, como já referido, se encontrem disponíveis no mercado programas de *malware* por medida, que permitem que indivíduos com pouca capacidade técnica consigam realizar ataques, parecem ser mais aptas a serem utilizadas no crime organizado e em situações de *Cibersextortion* praticado com motivações económicas.

1.2.2 Acesso remoto a dispositivos

O acesso remoto sem consentimento a dispositivos no contexto do *Cibersextortion*, constitui, à semelhança do uso *keyloggers* e *software* de captura de ecrã, uma das práticas mais graves do *modus operandi* dos ofensores pois combina o uso da tecnologia com elevado potencial coercivo sobre a vítima. No mercado negro existem programas designados *Remote Access Trojan* (RAT) [23]. Estes pacotes vêm prontos a ser enviados às vítimas e incluem funções de registo de teclado e captura de ecrã. Estão disponíveis por valores reduzidos e podem ser personalizados em função do sexo da vítima (Wittes et al., 2016). Tal como acontece com os *kits* de *phishing*, este mercado permite que indivíduos sem competências técnicas avançadas consigam implementar esquemas de elevada complexidade. Esta técnica baseia-se na exploração de falhas de segurança para obter controlo total ou parcial de computadores, *smartphones* ou outros dispositivos, quase sempre sem o conhecimento utilizador legítimo (Deodato, 2024).

O método inicial de ataque pode ocorrer pela instalação encoberta de *software* malicioso, frequentemente camuflado de utilitário, aparentemente inócuo, mas que funciona como uma porta que dá acesso ao atacante aos dispositivos. Não raras vezes este disfarce apresenta-se sob a forma clássica de cavalo-de-troia, RAT. Ou seja, um

[23] Um trojan de acesso remoto (RAT) é um tipo de malware que permite a um hacker controlar seu dispositivo de qualquer lugar do mundo, secretamente. Malware, aliás, é um termo para o programa de software invasivo usado por hackers – costumávamos chamar esse tipo de coisa de vírus de computador. Uma vez instalado, um RAT age como um espião digital. Ele pode dar a atacante acesso total ao seu computador, muitas vezes sem você perceber que está lá. Eles podem: Roubar senhas e arquivos sensíveis; Monitorar sua tela e tirar capturas de tela; Keylogging – o programa pode rastrear cada tecla que você pressiona;Ligar sua webcam ou microfone; Instalar mais malware;Usar seu computador para ataques adicionais. Mais perverso, os RATs são projetados para permanecer ocultos. Você pode não notar que algo está errado até que seus dados sejam roubados. Às vezes, um ex-cônjuge ou ex-parceiro irritado pode tentar usar um RAT para acessar seus dispositivos. Essa invasão de privacidade é uma forma de abuso e, além de prevenir e eliminar RATs, você deve denunciar a atividade à polícia. Disponível em - https://www.staysafeonline.org/pt/articles/can-a-hacker-take-over-your-computer-what-to-know-about-remote-access-trojans - acedido em 08/10/2025.

ficheiro partilhado por *e-mail*, mensagem instantânea ou *download* de aparência legitima que, ao ser executado, instala silenciosamente o *malware* no sistema (Humelnicu, 2017). A partir desse momento, o ofensor passa a ter a capacidade de aceder a ficheiros locais, incluindo fotografias e vídeos, e de ativar de forma oculta os periféricos como câmaras e microfones (Gonçalves, 2015).

Os RAT assumem um papel importante neste tipo de ações. Estas ferramentas estão equipadas com painéis de controlo que permitem aos ofensores observar ativamente as vítimas, transferir dados entre sistemas ou executar outros comandos à distância (Europol, 2018). *Softwares* como *Blackshades* [24] ou *DarkComet* [25], foram recorrentemente mencionados em investigações criminais pela sua capacidade de capturar imagens através da *webcam* sem consentimento, além de mapear detalhadamente as interações digitais da vítima (Wittes et al., 2016). Estas ações permitem aos ofensores construir um dossier contínuo sobre os dados *online* e *offline* da vítima. Acresce que, alguns RAT incorporam rotinas de reinstalação automática o que faz com que quando são detetados e parcialmente removidos procedam com reinstalação automática, resistindo até a antivírus convencionais (Deodato, 2024). Além disso, muitos comunicam com servidores remotos através de canais encriptados, dificultando a deteção por sistemas de inspeção de tráfego de rede.

Estas arquiteturas complexas, como veremos adiante, colocam obstáculos significativos à investigação forense digital como, por exemplo, localizar e neutralizar o servidor de

[24] O *malware* Blackshades — em particular, a Blackshades Remote Access Tool (RAT) — permite que criminosos roubem senhas e credenciais bancárias; invadam contas de mídia social; acessem documentos, fotos e outros arquivos de computador; registem todas as teclas digitadas; ativem webcams; sequestrem computadores para exigir resgate; e usem o computador em ataques distribuídos de negação de serviço (DDoS). (tradução nossa) - https://www.fbi.gov/news/stories/international-blackshades-malware-takedown-1 - Acedido em 18/09/2025

[25] O DarkComet é um trojan de acesso remoto (RAT) disponível gratuitamente, desenvolvido pelo programador independente "DarkCoderSC", que foi observado pela primeira vez em 2011 e ainda é considerado um dos RATs mais comuns utilizados. É comercializado como uma "ferramenta" em oposição a um "trojan", como é alegado para uso do administrador de rede; no entanto, a sua funcionalidade atrai os hackers. O trojan utiliza o Crypters para escapar às ferramentas antivírus e pode desativar o Gestor de Tarefas, o Editor de Registo, as Opções de Pasta, a Firewall do Windows e o Controlo de Conta de Utilizador (UAC) do Windows. O DarkComet é também capaz de registar toques de teclas, fornecer acesso ao sistema de ficheiros e ao controlo remoto - incluindo o controlo de dispositivos como microfones e webcams, e tem uma funcionalidade de negação de serviço distribuída (DDoS). Além disso, o trojan tem uma série de "funções divertidas", incluindo o Gestor de Diversão - diferentes tipos de funções divertidas, incluindo: ocultar o ambiente de trabalho, bloquear, ícones de tarefas, ícones da bandeja do sistema, barra de tarefas, botão Iniciar, gestor de tarefas e abrir/fechar a bandeja do CD. A funcionalidade de ambiente de trabalho remoto permite que o atacante visualize o ecrã ativo do utilizador infetado, além de assumir o controlo do rato e do teclado. O DarkComet é mais comummente disseminado através de ataques drive-by e *links* nas redes sociais. Os sistemas podem ser protegidos mantendo-os atualizados e utilizando *software* antivírus. (tradução nossa) - https://www.cyber.nj.gov/threat-landscape/malware/trojans/dark-comet - Acedido em 18/09/2025

comando e controlo que pode exigir cooperação Internacional, especialmente quando este se encontra em jurisdições pouco colaborativas (O' Malley, 2023). O processo pericial visa, essencialmente, a obtenção, prevenção e análise rigorosa das evidências digitais, elementos indispensáveis para a demonstração de nexo causalidade entre o agente e o ato ilícito (Wittes et al., 2016). É através deste processo que rastreiam as ferramentas tecnológicas e os métodos de intrusão utilizados, como instalação de difusão de *malware*, o acesso remoto a *webcams* sem consentimento ou a realização de gravações ocultas (Liggett, 2019; Wittes et al., 2016). Embora em muitos casos as vítimas partilhem voluntariamente os seus ficheiros íntimos, existe uma percentagem significativa em que são obtidos de forma furtiva (O'Malley & Smith, 2024). Assim, a análise deve concentrar-se na recolha de dados voláteis e não voláteis [26] provenientes dos dispositivos terminais, com o objetivo de estabelecer a ligação entre ofensor e atos praticados. Aspeto particularmente relevante num ambiente digital marcado pelo anonimato e pela fraude nas comunicações online (Edwards & Hollely, 2023). Acresce que os dados de comunicação entre ofensores e vítimas encontram-se frequentemente protegidos por sistemas de encriptação *end-to-end* (ponto por ponto) [27], restringindo o acesso direto às provas e exigindo que a recolha se concentre nos dispositivos de origem ou destino das comunicações (Edwards & Hollely, 2023).

Em termos preventivos, medidas como atualização constante dos sistemas operativos e utilização de antivírus com deteção comportamental avançada podem mitigar alguns riscos, embora não constituam soluções definitivas, especialmente quando o *modus operandi* combina vulnerabilidade técnica com manipulação social (Pethers & Bello, 2023). A consciencialização sobre sinais indiretos, como ativação espontânea da *webcam* ou degradação anómala do desempenho do dispositivo, pode ajudar na

[26] A Análise de Memória Volátil refere-se ao processo de examinar a memória RAM de um dispositivo para coletar dados que podem ser cruciais em investigações forenses digitais. A memória volátil é aquela que perde suas informações quando o dispositivo é desligado, tornando a análise em tempo real uma prática essencial para a recuperação de evidências digitais. Este tipo de análise é frequentemente utilizado em cenários de resposta a incidentes, onde a captura de dados em estado transitório pode revelar informações sobre atividades maliciosas, processos em execução e até mesmo senhas temporárias. Disponível em https://forense.io/glossario/o-que-e-analise-de-memoria-volatil/ - Acedido em 09-10-2025.

[27] A criptografia de ponta a ponta, ou End-to-End Encryption (E2EE), é uma técnica de segurança que garante que apenas as partes envolvidas em uma comunicação possam acessar o conteúdo das mensagens trocadas. Isso significa que, mesmo que os dados sejam interceptados durante a transmissão, eles permanecerão inacessíveis para qualquer entidade não autorizada, incluindo provedores de serviços e hackers. A E2EE é amplamente utilizada em aplicativos de mensagens, e-mails e transferências de arquivos, proporcionando um nível elevado de privacidade e proteção de dados. Disponível em https://forense.io/glossario/o-que-e-analise-de-memoria-volatil/ - Acedido em 09-10-2025.

detenção precoce. Contudo, muitos RAT modernos já conseguem ocultar completamente qualquer indício visual durante a sua operação (Wittes et al., 2016).

1.2.3 *Phishing*

O *phishing*, enquanto *modus operandi*, constitui uma das práticas mais recorrentes no âmbito do *Cibersextortion*, em virtude da sua capacidade de induzir a vítima a fornecer dados confidenciais ou a executar ações que facilitam o acesso a conteúdos íntimos. Esta técnica levada a cabo através da criação de comunicações fraudulentas que imitam entidades legítimas, são difundidas sobretudo por correio eletrónico, mas também por mensagens – *smishing,* ou mais recentemente por códigos QR maliciosos denominados *quishing*. Onde o objetivo passa por recolher credenciais, extrair informações pessoais ou induzir a instalação de *software* malicioso (Europol, 2023). A eficácia do método resulta da conjugação entre a técnica de engenharia social e os artifícios técnicos dissimulados que conseguem ultrapassar barreiras psicológicas e tecnológicas. Estas situações acontecem mesmo perante utilizadores com alguma consciência do risco.

Na fase inicial o atacante constrói um pretexto convincente, replicando com elevado detalhe visual e textual interfaces familiares como páginas institucionais ou formulários de autenticação, de modo a obter credenciais que, por regra, acabam por ser reutilizadas noutras plataformas. Muitos destes esquemas são, tal como acima referido, disponibilizados em *kits* de *malware* amplamente disponíveis no mercado ilícito. Incluindo no modelo *phishing-as-a-service,* que permite a qualquer indivíduo organizar campanhas credíveis sem dispor de conhecimentos técnicos aprofundados (Europol, 2024).

Esta verdadeira industrialização do fenómeno traduz-se na proliferação de pacotes vendidos na *Dark Web*, que incluem não apenas código-fonte das páginas, mas também bases de dados segmentadas de potenciais vítimas, mecanismos automáticos de resposta e técnicas para contornar filtros *anti-spam*.

No contexto específico do *Cibersextortion*, o *phishing* assume formatos adaptados ao objetivo final. É frequente o envio de mensagens fraudulentas que alegam a violação da conta da vítima, acompanhadas da ameaça de divulgação de vídeos íntimos supostamente obtidos a partir do dispositivo comprometido. Para reforçar a credibilidade, os ofensores recorrem, em alguns casos, a "provas" manipuladas, como capturas de ecrã falsificadas das redes sociais da vítima, ou combinam essas narrativas com credenciais reais extraídas de fugas de dados previamente conhecidas. Esta combinação de falsificação com autenticidade parcial intensifica o impacto psicológico e gera uma perceção de inevitabilidade que precipita decisões impulsivas das vítimas (Wittes et al., 2016).

O *smishing* acrescenta um elemento particular. O canal SMS, mais imediato e com taxas médias de leitura muito superiores, é utilizado para encaminhar as vítimas para páginas falsas ou induzi-las e descarregar aplicações maliciosas disfarçada de utilitários legítimos. Já o *quishing*, variante emergente, substituiu o *link* tradicional por um código QR que redireciona o utilizador para páginas controladas pelo agressor. Esta técnica manifesta relevância acrescida pela confiança que certos contextos físicos e digitais inspiram, como cartazes, estabelecimentos comerciais ou partilhas em redes sociais (Europol, 2024).

O cruzamento entre *phishing* e *malware* é igualmente recorrente. Em muitos casos, após recolha de credenciais numa página falsa, elas são usadas para aceder diretamente a contas reais da vítima – *e-mail* ou redes sociais - e procurar conteúdos íntimos. Noutros contextos, o simples ato de carregar a página maliciosa desencadeia descargas invisíveis (*drive-by download*) que instalam *keylogger*s ou *spyware,* assegurando uma vigilância prolongada sobre o sistema (Europol, 2023)

1.3 Redes Sociais *online*

A seleção das plataformas utilizadas para as abordagens iniciais e subsequentes no *Cibersextortion* não ocorrem por acaso, resulta da combinação entre o alcance

demográfico, as funcionalidades técnicas e as perceções de segurança ou privacidade cultivada pelos próprios utilizadores. Estudos empíricos mostram que redes sociais generalistas como *Facebook*, *Tagged* ou *Instagram* concentram a maioria dos contactos reportados, sendo identificados por mais de metade das vítimas como pontos de abordagem preferencial dos ofensores (Wolak & Finkelhor, 2016). Este predomínio explica-se tanto pelo volume elevado de utilizadores ativos como pela facilidade de acesso a conteúdos públicos ou semipúblicos como fotografias, listas de amigos ou detalhes biográficos, que fornece ao agressor material suficiente para construir narrativas convincentes durante as fases preliminares de engenharia social.

Aplicações de mensagens instantâneas e de partilha de fotografias, como *Kik* ou *Snapchat*, constituem a segunda categoria mais mencionada, abrangendo cerca de 41% dos casos registados (Humelnicu, 2017). Estas plataformas oferecem comunicação direta. Muitas utilizam ligações encriptada e suportam conteúdos efémeros. Isso reduz as pistas públicas das interceções e limita a perceção por terceiros, familiares, professores ou colegas.

É comum observar uma migração intencional. Após o primeiro contato em rede aberta, o agressor passa conduzir a vítima para canais privados, imediatamente antes da recolha do material íntimo (Wittes et al., 2016). Este deslocamento estratégico, assegura-lhe o controlo unilateral da comunicação e reduz os riscos de denúncia precoce.

Serviços de chamadas de vídeo, como *Facetime*, *Skype* ou *websites* com funcionalidades de *Webcam*, também assumem relevância nos padrões documentados. Cerca de 23% das vítimas relatam que a interação transitou para este tipo de ambiente, provavelmente em virtude da possibilidade de captar imagem em tempo real sem deixar registos textuais diretos (Wolak & Finkelhor, 2016; Ray & Henry, 2023). A capacidade de gravação oculta destas sessões confere valor imediato ao material obtido, uma vez que pode colocar maior pressão à vítima na fase de extorsão devido ao seu carácter audiovisual explícito.

As plataformas de encontros *online* como *Okcupid* ou *Tinder*, representam cerca de 9% dos casos registados (Humelnicu, 2017). Nesses contextos, os ofensores exploram expectativas de natureza romântica. Os pedidos de troca de imagens íntimas surgem como prolongamento da relação virtual em desenvolvimento. Depois de recolhido o material, os mesmos espaços podem ser reutilizados para localizar novas vítimas e replicar práticas já testadas com sucesso. O correio eletrónico, embora associado a práticas mais antigas, continua presente em cerca de 12% dos relatos (Wolak & Finkelhor, 2016; Ray & Henry, 2023). A sua utilização surge muitas vezes articulada com esquemas de *phishing*. Estes casos mostram que os métodos tradicionais continuam viáveis. A eficácia aumenta quando os ofensores usam contas previamente comprometidas em fugas de dados, pois o histórico confere às mensagens uma aparência de legitimidade.

Os ambientes digitais associados a videojogos *online* apresentam uma prevalência baixa, cerca de 4% (Humelnicu, 2017). Documentos judiciais descrevem casos em que adolescentes foram pressionados a fornecer imagens provocatórias. Estas surgiam como contrapartida ilícita para obter itens virtuais necessários à progressão no jogo (Humelnicu, 2017). O enquadramento lúdico reduz a suspeição inicial. Ao mesmo tempo, cria condições favoráveis à aproximação de menores em contextos aparentemente inócuos.

Importa destacar que muitas ocorrências envolvem múltiplos canais. Cerca de 45% dos inquiridos referiram ter sido contactados em mais de uma plataforma no mesmo esquema (Wolak & Finkelhor, 2016; Ray & Henry, 2023). Estas abordagens multiplataforma aumentam as hipóteses de sucesso. Isto acontece porque diversificam os pontos de contato e dificultam a reação defensiva da vítima. O bloqueio num serviço não impede que o agressor volte a atuar noutro espaço digital já explorado. A escolha das plataformas está, portanto, intimamente relacionada com as suas características técnicas e contextuais. Redes generalistas proporcionam uma base populacional ampla e acesso à informação pública em abundância. Plataformas de mensagens privadas garantem confidencialidade operacional. Serviços audiovisuais possibilitam a captura

direta e, ecossistemas lúdicos oferecem pretextos para relações descontraídas. Já as plataformas de encontros exploram motivações afetivas.

Esta segmentação tática revela o conhecimento prático dos ofensores sobre as *affordances* tecnológicas de cada ambiente digital e o seu potencial enquanto capital coercivo. A *Internet* oferece oportunidades únicas para atividades criminosas, em especial pela facilidade de divulgação e pelo anonimato que proporciona aos ofensores (Guedes et al., 2022). Finalmente, é de reconhecer que algumas destas dinâmicas são potenciadas pelos próprios modelos económicos das plataformas, concebidos para maximizar o tempo de permanência dos utilizadores e favorecer a descoberta algorítmica de novas interações sociais. As mesmas condições que sustentam a sua atividade e sucesso podem ser instrumentalizadas por agentes maliciosos (Goncalves, 2023). Ao alearem familiaridade cultural a funcionalidades que privilegiam comunicação privada imediata, estas estruturas mediáticas consolidam-se como alvos consistentes e prioritários nas campanhas contemporâneas de *Cibersextortion*.

1.4 Manipulação Psicológica

O fenómeno do *Cibersextortion* assenta, em regra, em estratégias de manipulação psicológica concebidas para explorar vulnerabilidades emocionais, cognitivas e contextuais das vítimas. Estas práticas encontram na sua matriz o princípio basilar da engenharia social. Ou seja, induzir comportamentos específicos através de apropriação de informações disponíveis e da construção da narrativa capazes de comprometer a capacidade crítica da vítima (Pethers & Bello, 2023).

Como já referido nas motivações económicas do ponto 1.3.1, uma das técnicas mais recorrentes consiste na criação deliberada de uma sensação de urgência artificial. No decorrer da extorsão, os ofensores impõem prazos extremamente curtos para o cumprimento das exigências. Normalmente acompanhadas de ameaças de divulgação imediata do material Íntimo (Liggett, 2019). Este encurtamento do prazo decisório coloca a vítima sob intensa pressão psicológica, o que reduz a margem da ponderação

racional e conduz a respostas impulsivas, frequentemente traduzidas na cedência às imposições (Humelnicu, 2017). Outro fator importante é o apelo ao medo, intensificado pela personalização da ameaça. A ver, como já referido, muitos ofensores recolhem previamente a informações sobre as rotinas, relações pessoais nas redes sociais das vítimas, que posteriormente utilizam como prova aparente de vigilância. Este detalhe reforça a credibilidade no discurso, ainda que parte da informação seja obtida em fontes públicas ou mesmo fabricadas. O objetivo ultrapassa a intimidação imediata, procura antes instaurar uma perceção duradoura de controlo, desencorajando a denúncia e limitando a procura de apoio (Justice, 2023) [28].

Outra técnica privilegiada é o uso da chantagem emocional (Ray & Henry, 2023). Em alguns casos iniciadas sob pretextos românticos ou de amizade, o agressor constrói uma ligação aparente, ou ilusória, até obter conteúdos sensíveis, convertendo essa relação numa arma de pressão. O discurso é adaptado entre ameaças explícita de exposição pública e insinuações sutis que cultivam sentimentos de culpa e vergonha na vítima. Não raras vezes simula-se a empatia momentânea antes da imposição da ameaça, reforçando dessa forma um ciclo abusivo marcado pela oscilação entre proximidade manipulada e intimação severa (Wolak & Finkelhor, 2016). Outra forma identificada, é o recurso intencional a erros gramaticais ou ortográficos nas mensagens iniciais. Tal prática visa dois propósitos, por um lado filtrar os indivíduos com menor literacia digital (considerados mais suscetíveis à manipulação) e, por outro, projetar uma abordagem amadora que desvie a atenção dos objetivos criminosos da operação (Pethers & Bello, 2023).

Acontece ainda o recurso ao estigma social, que constitui igualmente uma tática expressiva em contextos culturais mais conservadores ou em grupos minoritários sujeitos a forte discriminação. Aqui as ameaças podem centrar-se na revelação da orientação sexual ou de práticas íntimas contrárias às normas comunitárias. Nesses casos, a simples possibilidade de divulgação transcende o dano na reputação individual,

[28] Disponível no site da *U.S Department of Justice* em (https://www.justice.gov/d9/2023-06/*sextortion* crowdsourcing enticement and coercion 2.pdf) - Acedido em 17/09/2025

podendo traduzir-se em riscos concreto de exclusão social ou mesmo em violência física (Henry & Umbach, 2024).

Posto isto, facilmente se conclui, que a manipulação pode assumir formas híbridas, articulando espaço público e privado. Alguns ofensores recorrem a interações públicas como comentários insinuantes em perfis abertos ou publicações ambíguas dirigidas à rede social da vítima para evidenciar capacidade de afetar a sua reputação. Para, de seguida, regressam ao canal privado para propor uma saída condicionada ao cumprimento imediato de exigências (Wolak & Finkelhor, 2016). A oscilação entre exposição pública e intimidação privada instala um ambiente de incerteza permanente que reforça a sensação de vulnerabilidade na vítima.

1.5 Perfis falsos como instrumento estruturante da manipulação

A utilização de perfis falsos constitui mais uma estratégia do arsenal e engenharia social utilizadas em esquemas de *Cibersextortion*. Trata-se de um processo intencional e calculado, no qual o agressor constrói identidades digitais fictícias cuidadosamente desenhadas para inspirar a confiança e atrair as vítimas (Justice, 2023) [29]. Estes perfis não são contas descartáveis, mas sim estruturas consistentes que recorrem a elementos visuais e textuais extraídos de fontes legítimas. Tais como fotografias reais ou excertos biográficos plausíveis. Mais uma vez, o objetivo é passar para a vítima uma imagem convincente com vista a reduzir suspeitas nas fases iniciais do contato. Acresce, tal como igualmente já referido noutras formas de atuar, que os ofensores podem assumir o perfil que mais se adequa à vítima. Por exemplo, em situações que envolvam jovens do sexo masculino, é comum os ofensores assumam identidades femininas atraentes ou perfis de adolescentes, padrões esses valorizados por este grupo demográfico (Ray & Henry, 2023).

[29] Disponível no site da *U.S Department of Justice* em (https://www.justice.gov/d9/2023-06/*sextortion*_crowdsourcing_enticement_and_coercion_2.pdf) - Acedido em 17/09/2025

Noutros contextos, utilizam figuras que transmitem proximidade e credibilidade, como professores, amigos ou autoridades locais, explorando dessa forma o princípio da familiaridade, amplamente documentada na literatura sobre persuasão digital (Papathanasiou et al., 2025). Princípio esse que diz que um rosto conhecido funciona como um fator psicológico facilitador do envolvimento emocional das vítimas. Em alguns casos os ofensores recorrem à clonagem de perfis reais, prática designada por "perfil fantasma" ou o já referido *Catfishing* (Reis, 2024). Nestes casos, a conta autêntica é replicada quase integralmente, transmitindo uma sensação de legitimidade e, uma vez conquistada a confiança da vítima, surgem as ameaças e as extorsões características do *Cibersextortion*.

Este *modus operandi* é igualmente utilizado por grupos de crime organizado, que tal como acontece nos casos em que é utilizado *malware*, dividem tarefas. Alguns criam e mantêm os perfis ativos, outros abordam diretamente os alvos, enquanto equipas técnicas asseguram a recolha e o armazenamento dos conteúdos (Edwards & Hollely, 2023). Esta forma de agir, consiste igualmente numa recolha de informações das vítimas de modo lento, mas consistente ao longo de semanas antes de avançarem para a extorsão explicita. E, quando as exigências surgem, os ofensores já estão na posse de material capaz de sustentar as suas exigências (Edwards & Hollely, 2023).

Esta abordagem causa igualmente um impacto psicológico severo, sobretudo quando as interações simulam uma relação afetiva. Ao choque provocado pela revelação das reais intensões dos ofensores, ao medo de exposição pública e às exigências financeiras, soma-se a perceção de ter sido alvo de manipulação prolongada. Estas situações geram vergonha, humilhação e desconfiança generalizada em futuras interações em linha (Ray & Henry, 2023).

1.6 Criação afetiva ofensor vítima

A construção e confiança afigura-se como um momento crucial no processo do *Cibersextortion*. Funciona como a base que sustenta a eficácia das etapas subsequentes.

Os ofensores investem tempo para elaborar estratégias e amealhar recursos nesta etapa inicial, tendo em vista não levantar suspeitas na vítima para consolidar um vínculo que facilita a obtenção de material comprometedor e de dados pessoais (Açar, 2016). Este processo manifesta-se de diferentes formas, moldadas ao perfil da vítima e às motivações do agressor. Uma prática recorrente consiste em iniciar o contato em plataformas de utilização massiva, como as já referidas redes sociais, as aplicações de mensagens ou até os ambientes de jogos *online*. Nestas interações preliminares, o ofensor apresenta-se sob uma identidade fictícia ou cuidadosamente elaborada. Em alguns casos, tal como vimos antes, com o intuito de Inspirar confiança e dessa forma fomentar o envolvimento emocional da vítima. A escolha da *persona*, ou seja, da imagem da pessoa abusivamente apresentada nos perfis das redes sociais, não é aleatória. Tende a refletir os interesse a idade ou conteúdo cultural próximo do da vítima, funcionando como catalisador para o aprofundamento da interação (Justice, 2023) [30].

No *Cibersextortion*, ganhar a confiança implica mobilizar mecanismos psicológicos usados noutras tipologias de fraude. Que pode incluir demonstrar interesse pela vida quotidiana da vítima, validar opiniões ou partilhar supostas experiências pessoais semelhantes. Estas ações têm potencial para criar um ambiente de proximidade e promover a partilha voluntária de informação. De forma gradual, o diálogo evolui de tópicos superficiais para temas mais íntimos, permitindo ao agressor sondar vulnerabilidades emocionais ou sociais suscetíveis de exploração futura (Reis, 2024). Quando estas práticas envolvem menores, observa-se com frequência o encorajamento subtil à partilha de fotografias aparentemente inofensivas, sem carácter sexual explicito, mas que funcionam como etapa inicial para pedidos progressivamente mais intrusivos (Justice, 2023) [31].

O Tempo despendido nesta fase é variável. Alguns ofensores procuram ganhos rápidos, acelerando a narrativa de modo a estabelecer confiança em apenas alguns dias. Outros,

[30] Disponível no site da *U.S Department of Justice* em (https://www.justice.gov/d9/2023-06/*sextortion*_crowdsourcing_enticement_and_coercion_2.pdf) - Acedido em 17/09/2025

[31] Disponível no site da *U.S Department of Justice* em (https://www.justice.gov/d9/2023-06/*sextortion*_crowdsourcing_enticement_and_coercion_2.pdf) - Acedido em 17/09/2025

pelo contrário, investem em abordagens prolongadas no tempo, sobretudo quando o objetivo é sustentar uma manipulação continuada, em vez de uma ação pontual. Neste caso, recorrem a técnicas típicas de *grooming online* (Açar, 2016). Como demonstrações encenadas de vulnerabilidade, por exemplo, a partilha de "segredos pessoais", que alimentam uma lógica de reciprocidade. Esta dinâmica conduz a vítima a perceber o ofensor como autêntico e digno de confiança, reduzindo igualmente a resistência perante eventuais pedidos intrusivos. Dessa forma, à medida que o vínculo se fortalece, o agressor constrói um quadro afetivo em que determinados pedidos passam a parecer aceitáveis ou até naturais.

A avaliação social indireta controlada pelos ofensores constitui outro recurso frequente. Esta tática consiste em colocar perfis falso a interagirem publicamente entre si, projetando nas vítimas uma aparente interação genuína. Esta pseudo aprovação social reduz igualmente a vigilância da vítima, que interpreta os sinais como indícios externos de legitimidade (Wittes et al., 2016).

Nos cenários em que o objetivo último é a exploração financeira, a fase de confiança tende igualmente a passar por tentativas de criação de vínculos emocionais ou sexualizados. Este investimento acrescenta valor coercivo ao material obtido, no sentido em que, quanto maior o envolvimento emocional da vítima, maior a dificuldade em romper a relação quando surgem as primeiras exigências. A adaptação dinâmica do discurso é aqui essencial. Os ofensores monitorizam sinais de hesitação e ajustam o tom das interações em função das reações das vítimas. Assim, um silêncio prolongado, por exemplo, pode ser contrariado com mensagens amistosas ou justificações improvisadas destinadas a restabelecer a dinâmica (Justice, 2023) [32]. Quando estas práticas são dirigidas contra adolescentes, destaca-se ainda o recurso a códigos linguísticos próprios da faixa etária. Tais como, gírias atualizadas, referências culturais e rotinas escolares que reforçam a perceção de proximidade geracional e aumentam a credibilidade face à idade dos ofensores (Wittes et al., 2016). Em muitos casos, observa-se igualmente a transição deliberada para canais privados como aplicações de videochamadas ou

[32] Disponível no site da *U.S Department of Justice* em (https://www.justice.gov/d9/2023-06/*sextortion* crowdsourcing enticement and coercion 2.pdf) - Acedido em 17/09/2025

aplicações que permitem interações encriptadas, sob o pretexto de procurar "privacidade". Este movimento marca um ponto critico, pois reduz o risco de detenção por parte das plataformas reguladas (Europol, 2024).

Quando as vítimas se mostram mais cautelosas, os ofensores recorrem a incentivos positivos, como a promessas de oportunidades profissionais ou artísticas que implicam o envio de material gráfico, com vista á promoção da imagem pessoal da vítima. Embora não sexual na origem, este material pode ser manipulado e subsequentemente instrumentalizado como base para pressões futuras (Açar, 2016).

Pelo aqui exposto, percebe-se que esta etapa depende, em última instância, da capacidade de construir uma narrativa coerente em que a cedência às solicitações pareça decorrer naturalmente do histórico de interações. Uma vez consolidado este enquadramento abre caminho para as fases subsequentes do processo de extorsão, seja pela captura direta de conteúdo íntimo em conversas gravadas clandestinamente, seja através de pedidos explícitos após semanas ou meses de condicionamento psicológico.

IV. Perspetiva jurídica

A análise do *Cibersextortion* não se pode esgotar na sua caracterização tecnológica ou criminológica, exige igualmente um exame ao quadro jurídico aplicável. A ausência de uma tipificação penal autónoma obriga a reconduzir este fenómeno a tipos legais preexistentes, o que levanta desafios interpretativos e operacionais, sobretudo pela multiplicidade de bens jurídicos lesados como sejam a liberdade e autodeterminação sexual, a intimidade da vida privada, ou dos dados pessoais e patrimoniais ou ainda daqueles que tutelam a confiança nos sistemas informáticos.

1 Enquadramento jurídico do *Cibersextortion*

O enquadramento jurídico revela-se, assim, crucial para compreender como as normas penais e de proteção de dados respondem à diversidade de condutas associadas ao *Cibersextortion*, desde o acesso ilegítimo a dispositivos e dados, até à chantagem sexual ou económica exercida através da ameaça de divulgar conteúdos íntimos. A evolução legislativa portuguesa, espelha a necessidade de adaptar o sistema de justiça penal à realidade dinâmica e transnacional do ciberespaço. Esta secção aborda, em primeiro lugar, a qualificação do *Cibersextortion* à luz do conceito de cibercrime, explorando os conceitos de cibercrime em sentido estrito e em sentido amplo. Segue-se para uma análise da influência de instrumentos internacionais, com destaque para a Convenção de Lanzarote, na proteção de menores e na incriminação das práticas associadas ao aliciamento e à exploração sexual de crianças. Posteriormente, procede-se a uma avaliação do enquadramento no direito português, destacando-se a aplicação simultânea de normas do CP, da LC e da LPDP, bem como os desafios decorrentes do concurso de crimes, da recolha e preservação da prova digital e da cooperação internacional.

1.1 *Cibersextortion* à luz do cibercrime

O avanço exponencial das tecnologias digitais e a massificação do uso da *Internet* enquanto Tecnologia de Informação e Comunicação (TIC), têm trazido benefícios muito importantes à comunicação, ao acesso à informação e à partilha de conteúdos entre as pessoas (De Andrade et al., 2020). Contudo, este novo paradigma tecnológico potenciou igualmente o surgimento de novas formas de criminalidade, muitas delas desmaterializadas, transfronteiriças e altamente sofisticadas (Ribeiro, 2015). Assim, o cibercrime deve ser entendido como um constructo jurídico tecnológico dinâmico, sujeito a revisão legislativa e doutrinal à medida que surgem novas técnicas de ataque no ciberespaço. De assinalar ainda, ao contrário de outros contextos internacionais, é o facto da Constituição da República Portuguesa (CRP) na versão de 10 de abril de 1976, já prever, e sob alçada do catálogo dos Direitos Liberdades e Garantias (DLG), a utilização

da informática no artigo 35º o que demonstra um avanço significativo à época e a preocupação com o surgimento de novas tecnologias (Venâncio, 2022). O nº 2 do referido artigo 35º da CRP garantia que a informática não podia ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se tratasse de dados não identificáveis para fins estatísticos.

A definição do cibercrime não é simples, revela-se complexa e multifacetada, variando consoante a perspetiva disciplinar, as prioridades políticas e os quadros normativos das jurisdições de referência mundial. Tal diversidade reflete a dificuldade em verter num conceito unitário a vasta gama de condutas ilícitas mediadas por tecnologias (Hedidi, 2023).

Na doutrina portuguesa, essa diversidade conceitual traduz-se sobretudo na distinção entre cibercrime em sentido estrito e em sentido amplo. O termo "cibercrime" surge na doutrina para grosso modo, definir um conjunto de crimes praticados com recurso às TIC, onde se entendia que cabiam nesse conceito crimes novos a par de crimes antigos mediados pelas TIC. Ou seja, à já tradicional distinção entre "criminalidade informática" e "criminalidade praticada com recurso a meios informáticos" e, por isso, a separação entre a vertente das tecnologias de informação como meio de execução e alvo de crime (Verdelho et al., 2003).

Assim, o cibercrime em sentido estrito refere-se às situações em que o elemento digital constitui parte integrante do tipo legal ou apresenta-se como objeto de proteção. Esta acessão engloba, por exemplo, crimes em que o sistema informático integra o tipo do crime, ou se assume como bem jurídico protegido. Caso dos crimes previstos a Lei nº 109/2009, de 15 de setembro, LC. No sentido amplo, a tecnologia surge apenas como um instrumento ou meio para a prática de crimes tradicionais. Assim, considera-se crime informático em sentido amplo qualquer conduta ilícita em que os computadores, redes ou dispositivos digitais desempenham um papel instrumental, sem que o elemento tecnológico integre o tipo legal de crime (Nunes, 2024) Venâncio, 2023a). E, este entendimento corresponde ao que no plano Internacional se designa frequentemente como crimes facilitados ou cometidos por via de computadores, redes ou dispositivos

(Hedidi, 2023). Nesta perspetiva holística incluem-se a utilização instrumental da tecnologia – qualquer atividade criminosa realizada por meios informáticos -, crimes tradicionais potenciados pela tecnologia - como o já referido crime se Cyberstalking, ou melhor, de perseguição do artigo 154º-A, ou do crime de pornografia de menores do artigo 176º , ambos do CP -, processamento automático de dados – comportamentos ilegais e penalmente mensuráveis resultantes de manipulação de sistemas automatizados -, ou condutas lesivas de bens jurídico penalmente tutelados – como acesso, recolha, alteração ou destruição de dados, atentando contra a privacidade ou o património.

No plano comparado, Hedidi reforça que, numa acessão geral, o cibercrime corresponde a qualquer atividade que envolva computadores, redes, ou sistemas de telecomunicações como alvo ou ferramenta essencial (Hedidi, 2023). Esta definição, permite operar a distinção entre crimes *ciberdependentes* - que não existiriam sem o suporte digital, como *hacking*, ataques de negação de serviços (DoS) [33] ou disseminação de *malware*. E crimes *ciberpotenciados,* em que a tecnologia apenas amplia métodos pré-existentes, como a fraude *online*, o *phishing* ou o *Cibersextortion* (Leukfeldt & Holt, 2020). Esta tipologia dialoga com as definições de (Venâncio, 2023) e (Nunes, 2024) acima citados. Ao mesmo tempo que se articula com modelos normativos que descrevem o cibercrime como um fenómeno plurifacetado. Abrange, assim, tanto direitos tradicionais praticados com recurso a meios digitais, como novas tipologias derivadas da própria essência do ciberespaço. (Hedidi, 2023). No mesmo sentido já em 2011 a doutrina portuguesa fazia referência à deslocação dos crimes tradicionais para o espaço digital e a novos crimes com elementos de natureza digital.

Ao encarar-se o ciberespaço simultaneamente como um espaço informacional, ou seja, centrado na manipulação de dados, e, como espaço de rede, assim caracterizado pela interligação global, compreende-se o porquê de as fronteiras físicas perderem

[33] Um ataque de negação de serviço (DoS) ocorre quando usuários legítimos não conseguem acessar sistemas de informação, dispositivos ou outros recursos da rede devido às ações de um agente cibernético malicioso. Os serviços afetados podem incluir e-mail, sites, contas *online* (por exemplo, bancárias) ou outros serviços que dependem do computador ou rede afetados. Uma condição de negação de serviço é realizada inundando o host ou a rede alvo com tráfego até que o alvo não consiga responder ou simplesmente trave, impedindo o acesso de usuários legítimos. Ataques de negação de serviço podem custar tempo e dinheiro a uma organização enquanto seus recursos e serviços permanecem inacessíveis- https://www.cisa.gov/news-events/news/understanding-denial-service-attacks - Acedido em 17/09/2025

relevância. Tal dimensão transnacional exige, portanto, harmonização legislativa e cooperação Internacional eficaz (Deodato, 2024). Acresce que no plano jurídico formal persiste ainda uma significativa heterogeneidade. Algumas jurisdições optam por leis gerais sobre criminalidade informática, com tipos penais abertos relativos ao acesso ilegítimo, ao dano informático e à falsidade informática. Assim, apesar dos avanços significativos a nível tecnológico e legislativo, continua a observar-se heterogeneidade teleológica e normativa em relação aos meios de obtenção de prova (Andrade, 2009). Noutras os preceitos encontram-se dispersos por vários diplomas, dificultando o enquadramento coerente das condutas. Essa diversidade agrava-se nos fenómenos híbridos que integram crimes dispersos em legislação penal extravagante. Ou seja, lei penal não prevista no CP, mas em legislação que prevê e pune crimes. Por exemplo, a Lei 58/2019 de 8 de agosto, conhecida como a Lei de Proteção dos Dados Pessoais (DPDP) que assegura a execução, na ordem jurídica nacional, do Regulamento (EU) 2016/679 de 27 de abril 2016, conhecido como Regulamento Geral de Proteção de Dados (RGPD) [34]. O *Cibersextortion* é igualmente um exemplo paradigmático, pois pode configurar burla informática, coação ou ameaça, pornografia infantil – crimes previstos no CP -, crime de acesso ilegítimo previsto no artigo 6º da LC, crime de acesso indevido previsto no artigo 47º da Lei 58/2019 de 8 de agosto, ou até violação do Código dos Direitos de Autor e Direitos Conexos (CDADC) [35], consoante as circunstâncias do caso. Acresce que as diferentes abordagens conceptuais, umas reservando "cibercrime" apenas em ilícitos contra sistemas computacionais, outras adotando critérios mais amplos e funcionalistas, refletem tradições académicas e prioridades políticas nacionais distintas (Hedidi, 2023). Esta falta de consenso gera dificuldades operacionais sérias. Desde logo, dificulta a recolha uniforme de dados estatísticos o que pode comprometer o reconhecimento mútuo de decisões judiciais e cria entraves, por exemplo, à extradição, especialmente em virtude da natureza transnacional dos crimes digitais. Ainda assim, o mesmo ato pode ser punível numa jurisdição e irrelevante noutra. Situação que no caso do *Cibersextortion* é agravada pela facilidade com que os ofensores operam fora do país das vítimas (O' Malley, 2023).

[34] RGPD - Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679&qid=1759592995928

[35] CDADC - **Decreto-Lei n.º 63/85** - Diário da República n.º 61/1985, Série I de 1985-03-14 – disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1985-34475475

Observa-se ainda uma evolução marcada por ciclos tecnológicos. Inicialmente dominados por vandalismo digital e intrusões de natureza não monetária, os cibercrimes transformaram-se em atividades altamente lucrativas envolvendo, entre outros, "roubo" de dados pessoais, fraude eletrónica sofisticada e exploração sexual por meio digital. Este percurso evidencia a adaptabilidade dos ofensores. Acontece ainda que a evolução das tecnologias como um todo não cessa, e ferramentas criadas para fins legítimos como VPN ou comunicações encriptadas ponto a ponto, convertem-se em recursos logísticos de base, usadas para promover o anonimato durante as atividades ilícitas. A nível criminológico, distingue-se ainda entre o *modus operandi* técnico, baseado na exploração de vulnerabilidades computacionais, e o *modus operandi* social, assente na manipulação do utilizador - engenharia social. Frequentemente ambos se combinam em ameaças híbridas complexas, como no próprio *Cibersextortion*, que pode iniciar-se nas redes sociais abertas e evoluir, como já se disse, para canais encriptados de difícil rastreabilidade.

Posto isto, é oportuno referir que durante a prática de *Cibersextortion* podem ocorrer ações que cabem no catálogo de cibercrimes em sentido amplo - naqueles casos que abarcam atos ilícitos criminais mediados pelas TIC, mas onde estas não constam do tipo penal, por exemplo, os crimes de ameaça do artigo 153º ou de coação do artigo 154º, ambos do CP. E, ao mesmo tempo podem ocorrer atos no decorrer do *Cibersextortion* que cabem no catálogo de cibercrimes em sentido restrito, ou seja, crimes cujos tipos legais incluem a informática tanto como meio para praticar crimes, como alvo dos ofensores. Por exemplo, o crime de acesso ilegítimo do artigo 6º da LC, ou o crime de devassa através de meio de comunicação social, da *Internet* ou de outros meios de difusão publica generalizada, do artigo 193º do CP. Acresce que na grande maioria dos casos de *Cibersextortion* são praticados crimes de ambos os catálogos, o que causa dificuldades de enquadramento neste campo.

1.2 Convenção de Lanzarote

A Convenção do Conselho da Europa para o Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais assinada em Lanzarote em 25 de outubro de 2007, conhecida como "Convenção de Lanzarote"[36]. Tem como objetivos principais prevenir e combater a exploração sexual e os abusos sexuais de crianças, proteger os direitos das crianças vítimas de exploração sexual e abuso sexual e promover a cooperação internacional para combater estas práticas. Nas definições, a alínea a) do artigo 3º da Convenção de Lanzarote, designa "criança" como sendo qualquer pessoa com idade inferior a dezoito anos e, no nº 2 do artigo 20º, define a expressão "pornografia de menores" para designar todo o material que represente visualmente uma criança envolvida em comportamentos sexualmente explícitos, reais ou simulados, ou qualquer representação dos órgãos sexuais de uma criança, com fins sexuais. A sua elaboração decorreu, em parte, de um Plano de Ação adotado pela 3º Cimeira de Chefes de Estado e de Governos do Concelho da Europa em 2005 em Varsóvia, que apelava ao fim da exploração sexual de crianças.

Portugal, enquanto Estado membro da União Europeia e signatário da Convenção de Lanzarote, assumiu a obrigação de transpor as suas disposições para a ordem jurídica interna. Essa transposição foi realizada através de diversas alterações legislativas ao CP e a leis complementares, com destaque para a Lei nº 113/2009, de 17 de setembro, a lei nº 103/2015, de 25 de agosto, e a lei 101/2019, de 8 de setembro. Um dos tipos penais influenciados pela convenção de lanzarote é o crime de abuso sexual de crianças do artigo 179º do CP. As sucessivas reformas legislativas visaram alargar o âmbito do abuso sexual e outras infrações contra a autodeterminação sexual de crianças, com um foco particular nas idades das vítimas e nas circunstâncias agravadas (Mouraz & Milheiro, 2023).

[36] Convenção do Conselho da Europa para a Proteção das crianças contra a Exploração Sexual e os Abusos sexuais, que teve lugar em Lanzarote a 25 de outubro de 2007. Consultada em linha em: https://rm.coe.int/168046e1d8 - Acedido em 19/09/2025

Como vimos antes, na prática do *Cibersextortion*, dependendo do *modus operandi*, pode estar em causa o preenchimento de tipos penais diversos. Que depois podem ou não estar em concurso para determinação medida concreta da pena. O artigo 18º da Convenção de Lanzarote, prevê a criminalização de atos sexuais com uma criança abaixo da idade legal ou através de coação, violência, ameaça, abuso de confiança ou autoridade, ou de vulnerabilidades. O CP português, no processo de aproximação às disposições da Convenção foi sendo reformulado, nomeadamente o já referido artigo 179º, que criminaliza a prática de ato sexual com crianças menores de 14 anos, ou até 16 anos em situações de particular vulnerabilidade ou abuso de autoridade ou confiança, ou por meio de coação ou violência. As alterações introduzidas pela Lei nº 101/2019 ampliam a tutela de vítima no âmbito do artigo 179º, estabelecendo um regime de agravantes para situações em que a vítima é particularmente vulnerável (Mouraz & Milheiro, 2023). O artigo 20º da Convenção, referente à pornografia de menores, obriga os Estados signatários a criminalizar a produção, oferta, difusão, transmissão, procura, posse ou acesso a essa pornografia, especialmente través das tecnologias de informação e comunicação.

Em Portugal, o crime de pornografia de menores está previsto no artigo 176º do CP, que foi igualmente reformulado para abranger estas disposições, criminalizando a aquisição, detenção, acesso, produção, difusão e transmissão de material pornográficos envolvendo menores. A Lei 101/2019, por exemplo, alargou o âmbito da aplicação das normas relativas aos crimes de pornografia de menores.

Outras previsões de relevância da convenção são o da participação de uma criança em espetáculos pornográficos do artigo 21º da Convenção. Aqui prevê-se a criminalização do recrutamento, coação ou exploração de uma criança para participar em espetáculos pornográficos, bem como assistir a esses espetáculos conscientemente e, as agravantes previstas no artigo 28º da Convenção. Estas circunstâncias foram incorporadas na legislação penal portuguesa, nomeadamente no artigo 177º do CP, que estabelece o regime de agravamento das penas para crimes sexuais, refletindo a importância destas condições para determinar a pena a aplicar (Mouraz & Milheiro, 2023).

Algumas dessas disposições ainda não foram completamente vertidas no CP, como, por exemplo, a da alínea e) quando a infração é cometida por várias pessoas em conjunto, ou no caso da alínea f) quando a infração for cometida no âmbito de uma organização criminosa – situações que, como vimos antes, se enquadrariam nos casos de *Cibersextortion* operados por organizações criminosas com motivações económicas. No entanto, o artigo 23º da Convenção com epigrafe "Abordagem de crianças para fins sexuais" impõe a cada parte que tome as medidas legislativas necessárias ou outras para qualificar como infração penal o facto de um adulto propor de forma dolosa, através de tecnologias de informação e comunicação, um encontro a uma criança que não tenha atingido a idade estabelecida, em aplicação do nº 2 do artigo 18º. Com finalidade de cometer nesse encontro qualquer uma das infrações estabelecidas em conformidade com a alínea a) do nº 1 do artigo 18º ou com a alínea a) do nº 1 do artigo 20º, desde que essa proposta seja seguida de atos materiais que visem a tal encontro.

Para além das disposições de Direito penal, a Convenção de Lanzarote contempla ainda disposições de proteção e assistências à vítima no Capítulo IV, onde enfatiza a criação de programas sociais eficazes e estruturas multidisciplinares para prestar o apoio necessário às vítimas, aos familiares próximos e a outras pessoas a quem as crianças estejam confiadas.

No Capítulo II, a Convenção exige que os Estados tomem medidas para prevenir a exploração e abusos sexuais, nomeadamente através da sensibilização e formação de pessoas que contactam regularmente com crianças ou, ainda, garantias de que os candidatos a profissões com contacto regular com crianças não foram condenados por crimes sexuais contra crianças.

No Capítulo VIII, quanto ao registo e armazenamento de dados de pessoas condenadas por infrações penais de natureza sexual, a Convenção estabelece a obrigação de os Estados coligirem e armazenarem dados relativos à identidade e ao perfil genético (ADN) de pessoas condenadas por infrações sexuais contra crianças, para efeitos de prevenção, investigação e processamento. Aqui, Portugal, através da Lei n.º 113/2009, de 17 de setembro, entre outras, estabeleceu medidas de proteção de menores em

cumprimento desta obrigação, incluindo o registo criminal definitivo (Mouraz & Milheiro, 2023).

Quanto à cooperação internacional e jurisdição o Capítulo IX da Convenção, promove a cooperação entre as partes na prevenção e combate à exploração sexual e aos abusos sexuais de crianças, na proteção e assistência às vítimas e nas investigações e procedimentos penais. Permite que as vítimas apresentem queixa junto das autoridades do seu Estado de residência, mesmo que o crime tenha sido cometido noutro território. E aqui, a legislação portuguesa reflete este princípio ao prever a aplicação da lei penal portuguesa a factos cometidos no estrangeiro quando o agente se encontre em Portugal e não possa ser extraditado, ou quando a vítima resida em Portugal (Mouraz & Milheiro, 2023).

1.3 Enquadramento jurídico do *Cibersextortion* no direito português

A inexistência de uma tipificação autónoma de *Cibersextortion* no ordenamento jurídico português obriga a reconduzir estas condutas a tipos penais já existentes. Aplicados em conformidade com as circunstâncias factuais e os bens jurídicos tutelados. Esse enquadramento pode variar substancialmente, consoante estejam envolvidas vítimas maiores ou menores de idade, a natureza das ameaças utilizadas ou os meios técnicos empregues. Por essa razão, a prática forense tem recorrido a diferentes figuras típicas para lidar com este fenómeno. Ainda que de forma fragmentada. Quando os factos envolvem ameaça de divulgação não consentida de imagens íntimas - fotografias ou vídeos de ato sexual -, a incriminação é frequentemente feita com base nos crimes contra a liberdade e autodeterminação sexual, crimes contra a liberdade pessoal e crimes contra a reserva da intimidade da vida privada. Alterações legislativas recentes reforçaram esta vertente. Destaca-se a revisão do artigo 193º do CP [37]. Estas alterações procuraram reforçar a proteção contra ameaças no ciberespaço, reconhecendo os

[37] Alterado pelo/a Artigo 2.º do/a Lei n.º 26/2023 - Diário da República n.º 104/2023, Série I de 2023-05-30, em vigor a partir de 2023-06-01

efeitos duradouros da perpetuidade dos ficheiros digitais e o agravamento do impacto decorrente da velocidade de propagação das novas tecnologias.

Em contextos em que os conteúdos são obtidos através de engano ou no âmbito de uma relação amorosa, com subsequente chantagem, o enquadramento pode assumir a forma de violência doméstica da alínea b), do nº2 do artigo 153ºdo CP, sempre que haja relação íntima entre vítima e agressor, circunstância que pode ser agravante (Pires, 2022). Fora deste contexto de intimidade, a conduta tende a ser reconduzida a molduras mais genéricas, como a coação do artigo 154º ou da extorsão do artigo 223º, ambos do CP, ou outros tipos penais mais abrangentes que permitem enquadrar ofensas que combinam dimensões sexuais e digitais. O crime de perseguição previsto no artigo 154º-A do CP, conhecido, como anteriormente referido por *stalking*, também pode servir de enquadramento sempre que o *modus operandi* inclua contactos insistentes por via digital com conteúdo sexualizado. A norma prevê que tal crime pode ser cometido por qualquer meio, abrangendo expressamente a perseguição *online* através de novas tecnologias (Goncalves, 2023). Situações em que o agressor insiste em aproximações ameaçadoras associadas a exigências sexuais podem, assim, refletir elementos típicos do *Cibersextortion*.

Quando estão envolvidos menores, especialmente em contexto de pornografia infantil do artigo 176º do CP, este assume-se como núcleo central da incriminação. No entanto, parte da doutrina questiona se todas as condutas abrangidas por essa disposição protegem efetivamente a liberdade e autodeterminação sexual dos menores ou se resultam de soluções excessivamente moralistas. Caso de mera detenção passiva de material pornográfico infantil sem indícios de produção ou distribuição são apontados como problemáticos em termos de dignidade penal (Rodrigues, 2023).

Independentemente do tipo penal aplicável, persiste um desafio probatório significativo relativamente ao consentimento e à intenção. É necessário demonstrar que a ameaça tinha um potencial extorsivo concreto e serviu de meio causal para constranger a vítima à prática ou omissão pretendida. Este requisito torna-se particularmente sensível quando o conteúdo ameaçado nunca chega a ser divulgado. Nesse caso cumpre provar

que o método gerado era credível atendendo às circunstâncias objetivas de cada caso em concreto. Outro aspeto crítico reside nas sobreposições normativas, frequentemente identificadas em situações de *Cibersextortion*. A coexistência de múltiplos tipos aplicáveis gera divergências jurisprudenciais e insegurança jurídica quanto à qualificação mais adequada (Pires, 2022). Acrescem ainda, diferenças relevantes no quadro sancionatório. Os factos enquadrados como violência doméstica do artigo 152º do CP, são punidos de forma mais gravosa do que quando tratados como coação do artigo 154º ou extorsão do artigo 223º ambos do CP. o que pode levar parte da doutrina a defender o ajuste das penas às condutas praticadas, justificado ainda, pela crescente prevalência e pela necessidade de uma resposta ao nível tento da prevenção geral como da prevenção especial.

Outra vertente a ter em conta é a modalidade de *Cibersextortion* ligada ao abuso institucional ou funcional. Esta modalidade aproxima-se de crimes de corrupção previstos na lei portuguesa. Nestes casos, um agente Público pode instrumentalizar o seu cargo em troca ilícita de favores sexuais, configurando o que tem sido designado no plano internacional como corrupção, sexualizada (France, 2022). Contudo, nem sempre os elementos típicos da corrupção tradicional, como a exigência de vantagem patrimonial ou equiparada, abrangem vantagens de natureza não pecuniária. Adaptar a previsão normativa poderia assim permitir um enquadramento mais claro destas situações também em Portugal. As dificuldades práticas não se esgotam no plano substantivo. Em termos processuais, persistem lacunas como a inexistência de mecanismos eficazes para receção rápida e preservação segura de denúncias relacionadas com *Cibersextortion*, o que fragiliza a recolha de prova volátil. A dimensão transacional destes crimes, frequentemente praticados por ofensores localizados no estrangeiro que recorrem a técnicas de anonimização, torna indispensável recorrer a instrumentos internacionais, como a Convenção do Cibercrime, para viabilizar a cooperação judiciária (O’ Malley, 2023).

1.4 Código Penal

O direito penal, e em particular o direito penal sexual, deve manter-se afastado de juízos éticos ou morais sobre sexualidade, uma vez que os valores sociais nesta matéria são mutáveis e variam de cultura para cultura. Assim, costumes ou práticas culturais não podem servir como critério rígido para definir ilícito, devendo a tutela centrar-se na liberdade sexual do indivíduo e não na de uma comunidade. Acresce que sempre que o CP recorre a conceitos de índole moral, como sucede com a pornografia e a pornografia de menores, a sua interpretação deve ser restritiva e limitada ao conteúdo expressamente previsto na lei, especialmente após a reforma de 2007 (Mouraz & Milheiro, 2023). O enquadramento do *Cibersextortion* no Código Penal português carece, no seguimento do acima exposto, de uma análise direcionada ao modo como disposições já existentes podem ser mobilizadas para conter o fenómeno dada a inexistência de uma tipificação autónoma. Assim, tal como noutras geografias a nível mundial, a subsunção das condutas a tipos penais pré-existentes depende da natureza concreta da ameaça e do constrangimento sexual exercido, o que conduz frequentemente à aplicação combinada de crimes de natureza sexual patrimonial ou contra a honra (Wittes et al., 2016).

Recorde-se que, segundo o princípio da legalidade, só pode haver crime se existir lei anterior ao facto que preveja a conduta típica, ilícita, culposa e punível (Dias, 2001). No caso do *Cibersextortion,* a imputação criminal resulta do preenchimento de vários tipos penais, permitindo punir o agente por condutas isoladas, como as previstas nos artigos 154º, 193º, ou o 223º todos do CP, bem como em crimes previstos na LC e na Lei nº 58/2019, de 8 de agosto, conhecida como de a Lei de Proteção de Dados Pessoais (LPDP).

Ainda a este respeito, Figueiredo Dias e Costa Andrade, ensinam que o conceito de dignidade penal implica um princípio de imanência social e um princípio de consenso. Significando o primeiro que não deve ser assegurado através das sanções criminais a prossecução das finalidades socialmente transcendentes, designadamente moralistas ou ideológicas. E, o segundo, por seu turno, postula a redução do direito criminal ao núcleo irredutível, ainda que historicamente dinâmico, dos valores ou interesses que

contam com o apoio generalizado da comunidade. Adiantam ainda que existe um largo consenso na doutrina na aceitação da tese de que é ilegítimo criminalizar por razões exclusivamente moralistas. Concluindo que o conceito de carência de tutela corresponde ao princípio da subsidiariedade do direito penal, princípio segundo o qual o direito penal deve constituir a último ratio do controlo social (Dias & Andrade, 1997).

Esta forma de incriminação das condutas associadas às várias tipologias de *Cibersextortion* não se fundamentam em considerações moralistas, mas antes na tutela de bens jurídicos centrais, social e juridicamente reconhecidos como dignos de proteção penal. Com efeito, tais práticas afetam de modo grave a liberdade e autodeterminação sexual, a reserva da vida privada e da intimidade, bem como, em determinadas situações, o património, encontrando-se, por isso, no âmbito legítimo de intervenção do direito penal. Assim, à luz dos princípios da dignidade penal e da subsidiariedade, mostra-se inteiramente justificada a qualificação do *Cibersextortion* como fenómeno merecedor de tutela penal. Seja em tipos penais existentes ou num eventual crime autónomo.

Nos casos em que o conteúdo coercivo é de natureza sexual e envolve contacto obtido mediante fraude quanto à identidade – nos casos de *Catfishing* -, abre-se a possibilidade de enquadramento pelo crime de coação sexual do artigo 163º do CP ou pela fraude sexual do artigo 167ºdo CP. Figura que exige dolo específico e é qualificado como crime de mão própria (Reis, 2024). Quando os factos envolvem menores, o artigo 176º do CP - aliciamento de menores com vista à prática de atos sexuais - e disposições conexas sobre pornografia infantil, artigo 176º - A e ss., impõe-se como núcleo da incriminação, mesmo que o elemento extorsivo seja predominante, devido ao regime imperativo desta matéria (Da Silva, 2016). Em contextos em que a ameaça incide sobre a divulgação Ilícita de imagem da vítima previamente obtidas sem consentimento o enquadramento jurídico pode assentar no crime de devassa da vida privada do artigo 192º ou no crime de gravação de fotografias ilícitas do artigo 199º, ambos do CP, agravados sempre que a difusão ocorra por meio informático (Ribeiro, 2015).

Após a alteração ao CP, promovida pela Lei n.º 26/2023, de 06/01 [38], o artigo 192º do CP, sofreu alterações ao nível da moldura penal. Na redação anterior, todas as condutas proibidas eram punidas com pena de prisão até 1 ano ou multa até 240 dias. Na nova redação, essas penas mantêm-se para as alíneas a) e c). Já para as alíneas b) e d), foram agravadas para pena de prisão até 3 anos ou multa. A alínea d) fica, contudo, isenta de pena quando o facto praticado se mostre adequado para realizar um interesse público legitimo e relevante. O regime prevê ainda a agravação estabelecida no artigo 197º do CP, igualmente alterado. Nesses casos, a pena aumenta em um terço quando o facto for praticado para obter recompensa ou enriquecimento, para si ou para terceiro, ou para causar prejuízo a outra pessoa ou ao Estado.

A referida alteração ao CP promoveu ainda alterações nos artigos 193º [39] e 198º do CP. Quanto ao artigo 193º do CP, sob a epigrafe "Devassa através de meio de comunicação social, da *Internet* ou de outro meio de difusão pública generalizada" prevê agora o seguinte, "Quem, sem consentimento, contribuir para a disseminação, através de meio de comunicação social, da *Internet* ou de outros meios de difusão pública generalizada, de imagens, fotografias ou gravações que devassem a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual, é punido com pena de prisão até 5 anos.". Esta nova redação, para além de continuar a tutelar dados sensíveis, dá agora mais importância à tutela da intimidade da vida privada. Importância essa que se justifica devido à crescente migração de atos violadores deste bem jurídico para o ciberespaço (Venâncio, 2025).

O Acórdão Tribunal da Relação de Coimbra de 12 de março [40], que analisou um caso de múltiplas vítimas, no qual uma delas foi filmada durante o ato sexual, tendo os

[38] Lei n.º 26/2023, de 6 de janeiro - Diário da República n.º 104/2023, Série I de 2023-05-30, em vigor a partir de 2023-06-01 – disponível em https://diariodarepublica.pt/dr/detalhe/lei/26-2023-213706993

[39] O artigo 193.º do Código Penal: que previa o crime de devassa por meio de informática, foi redenominado; prevê agora o crime de devassa através de meio de comunicação social, da *Internet* ou de outros meios de difusão pública generalizada; não exige para o seu preenchimento, como anteriormente, a criação, manutenção, ou utilização de ficheiro automatizado de dados individualmente identificáveis; nem a difusão das imagens recolhidas por um número alargado de destinatários; prevê, agora, uma punição com pena de prisão até 5 anos, quando anteriormente o crime do art.º 193.º era punido com pena de prisão até 2 anos ou com pena de multa até 240 dias. **Tribunal da Relação de Coimbra - Processo nº 69/22.7JAGRD.C1 - Relator:** ALEXANDRA GUINÉ **Sessão:** 12 março 2025 disponível em: https://diariodarepublica.pt/dr/detalhe/acordao/69-2025-930039275 - Acedido em 19/09/2025

[40] O mesmo Acórdão acima, do **Tribunal da Relação de Coimbra - Processo nº 69/22.7JAGRD.C1 - Relator:** ALEXANDRA GUINÉ **Sessão:** 12 março 2025 disponível em: https://diariodarepublica.pt/dr/detalhe/acordao/69-2025-930039275 - Acedido em 19/09/2025

conteúdos íntimos sido posteriormente publicados num grupo fechado na *Internet*. Inconformado com a condenação na pena de dois anos e seis meses de prisão, pela prática de um crime de devassa da vida privada através da internet, previsto e punível (p.p.) pelo artigo 193º do CP, o arguido recorreu. O seu principal argumento era não estar preenchido o elemento objetivo – disseminar, através da *internet*. Que justifica pelo número limitado de pessoas que tiveram acesso ao conteúdo e à sua visualização limitada a uma única vez [41]. Enquadrando antes as condutas nos elementos no crime de devassa da vida privada p.p. pelo artigo 192º do CP.

Uma análise dogmática ao crime p.p. pelo no artigo 193º do CP, permite decompor os seus elementos constitutivos. No plano objetivo, a conduta punível consiste em "contribuir para a disseminação", um elemento descritivo que abrange um vasto leque de ações que potenciam a partilha de conteúdos ilícitos. Esta ação incide sobre "imagens, fotografias ou gravações que devassem a vida privada das pessoas, designadamente a intimidade da vida familiar sexual", um elemento normativo que carece de valoração judicial para determinar a violação da intimidade. A ilicitude da conduta é ainda determinada pela ausência de consentimento da vítima "Quem, sem consentimento", outro elemento normativo central na configuração do crime. No que ao elemento subjetivo diz respeito, o tipo penal não exige qualquer dolo específico, sendo, contudo indispensável que o agente atue com dolo, nos termos gerais do artigo 13º do CP. Por último, no plano processual, e por força da nova redação do artigo 198º do CP, dada pela mesma Lei 26/2023, o procedimento criminal depende de queixa, salvo nas situações em que do crime resultem o suicídio ou morte da vítima ou quando o interesse da vítima o aconselhe. Casos em que o procedimento adquire natureza publica (Venâncio, 2025).

Do ponto de vista patrimonial, quando o objetivo é a obtenção de vantagem económica, o crime de extorsão do artigo 223º do CP, pode ser o tipo legal aplicável, isoladamente ou em concurso com crimes sexuais, caso se comprove o uso de material íntimo como

[41] Conteúdos multimédia de visualização única. As fotos e os vídeos de visualização única não são guardados nas Fotos ou na Galeria dos destinatários. Não podem ser reencaminhados, partilhados ou copiados. Os destinatários não podem fazer capturas ou gravações de ecrã do ficheiro multimédia de visualização única. É possível tirar uma foto ou gravar um vídeo dos conteúdos multimédia antes de estes desaparecerem, por exemplo, com uma câmara ou outro dispositivo. disponível em: https://faq.whatsapp.com/578442220724722/?locale=pt_PT&cms_platform=iphone – Acedido em 05/10/2025.

meio coercivo (Deodato, 2024). Em situações em que se verifica manipulação fraudulenta de sistemas ou dados informáticos, poderá haver concurso real ou aparente com a burla informática do artigo 221º do CP (Ribeiro, 2015). Importa notar que as alterações legislativas desde o Decreto-Lei nº 400/82 já previam crimes cometidos por meios informáticos, embora apenas posteriormente se tenham integrado disposições que abrangem práticas contra a autodeterminação sexual mediadas por tecnologias (Deodato, 2024). No plano processual, aplica-se a regra geral de punição da tentativa do artigo 23º nº1, do CP, válida sempre que o crime consumado corresponda a pena superior a três anos, o que abrange casos em que o ato é interrompido, mas já atinge idoneidade para constranger a vítima (Ribeiro, 2015). A jurisprudência portuguesa tem reconhecido a validade probatória de ameaças digitais quando estas revelam capacidade real de afetar a liberdade sexual ou moral (Reis, 2024).

Por fim, cumpre sublinhar que a resposta penal enfrenta dificuldades adicionais perante condutas híbridas e transnacionais, que exigem articulação entre normas internas e compromissos internacionais, como a Convenção sobre o Cibercrime. Em qualquer dos casos, as circunstâncias agravantes, como várias vítimas em simultâneo, crime organizado ou ofensas à integridade física graves, permitem, nos termos gerais do CP, um agravamento substancial da moldura da pena aplicável. A coerência e eficácia desta resposta dependeram, porém, de uma interpretação judicial consistente e de uma estratégia acusatória baseada em prova digital solida (Deodato, 2024).

1.5 Lei do Cibercrime

A Lei nº 109/2009, de 15 de setembro, conhecida como “Lei do Cibercrime” (LC), constitui o diploma estruturante do ordenamento jurídico português para fazer face à criminalidade informática. Estabelece tipos penais específicos e mecanismos processuais adaptados à natureza volátil e transnacional da prova digital, transpondo para a ordem jurídica interna a Convenção sobre o Cibercrime do Conselho da Europa, adotada em e Budapeste a 23 de novembro de 2001, e por isso, conhecida como “Convenção de Budapeste”. Esta, foi aprovada em Portugal pela Resolução de

Assembleia da República nº 88/2009 de 15 de setembro e entrou em vigor em 1 de julho de 2010. Abrange um leque variado de condutas ilícitas cometidas através ou contra sistemas informáticos.

No contexto do *Cibersextortion*, embora o núcleo típico não seja diretamente criminalizado por esta Lei – dado que a conduta incide sobretudo sobre bens jurídicos ligados à liberdade e autodeterminação sexual –, várias das suas previsões assumem relevância sempre que os atos envolvem acesso indevido a sistemas ou dados informáticos com vista à obtenção do material usado na coação. Dos crimes previstos na LC, destaca-se o artigo 6º, que tipifica o acesso ilegítimo, definido como a ação de, sem permissão legal ou autorização do titular legitimo, aceder por qualquer meio a um sistema informático ou parte dele. Esta norma tem particular pertinência nos casos em que os ofensores invadem dispositivos das vítimas – computadores pessoais, telemóveis ou contas *claud* – para capturar, às ocultas, imagens ou vídeos íntimos. Tal intrusão pode ocorrer de forma direta, mediante autenticação fraudulenta, ou indireta, através de instalação remota de *malware*.

Relevam igualmente as normas relativas à interceção e recolha de dados associados a comunicações eletrónicas, que permitem às autoridades captar o histórico e o contexto de acessos ilícitos, servindo como ponte probatória entre a intrusão técnica e o subsequente uso desse material no quadro coercivo típico do *Cibersextortion*. Contudo, estas medidas só podem ser utilizadas mediante autorização judicial expressa e dentro dos limites estritos previstos para escutas e interceções nas comunicações (Ribeiro, 2015), o que exige equilíbrio entre celeridade investigativa e respeito pelas garantias constitucionais e os meios de obtenção de prova legal.

A sabotagem informática do artigo 5º e a falsidade informática do artigo 3º, podem ter implicação com os métodos usados em crimes desta natureza. Naqueles casos em que os ofensores alteram ou destroem ficheiros relevantes ao processo judicial, enquadráveis no crime de sabotagem informática, numa prática anti forense que visa eliminar vestígios digitais e dessa forma comprometer a cadeia de custódia da prova (Deodato, 2024).

A LC, contempla ainda disposições processuais destinadas à cooperação judiciária internacional, alinhadas com a Convenção de Budapeste. Estas disposições são cruciais face à dimensão transnacional do fenómeno, mas enfrentam limitações operacionais decorrentes da morosidade dos pedidos remetidos às instâncias formais. Agravada pela facilidade com que os dados informáticos podem ser apagados ou transferidos. Neste sentido, ganha destaque o regime de recolha expedita de dados conservados, que permitem obter rapidamente informação essencial, como endereços IP e registos de *login*, antes da sua eliminação automática pelos prestadores de serviços. Este mecanismo é decisivo em contextos em que os ofensores recorrem a identidades falsas ou a plataformas encriptadas para manter o anonimato (Europol, 2018).

Apesar destes instrumentos, persistem desafios decorrentes da sofisticação tecnológica dos agentes, que parecem estar sempre um passo à frente, como o uso de redes privadas virtuais, canais encriptados ou novas técnicas anti forenses. A aplicabilidade da LC também suscita frequentemente problemas de concurso aparente ou real com tipos penais clássicos [42], o que requer uma análise jurídica cuidada para delimitar a moldura penal aplicável ao caso concreto.

1.6 Lei da Proteção de Dados Pessoais

A proteção de dados pessoais em Portugal encontra o seu primeiro respaldo na CRP, cujo artigo 35º consagra expressamente este direito fundamental. Embora essa consagração surja logo na primeira versão da CRP de 1976 e densificada nas revisões constitucionais de 1982, 1989 e 1997. A sua concretização legislativa ocorreu apenas com a Lei nº 67/98, de 26 de outubro, conhecida como a Lei de Proteção de Dados Pessoais (LPDP), que transpôs a Diretiva 95/46/CE. A evolução normativa europeia, com a aprovação do RGPD, (UE) 679/2016, determinou a revogação da antiga LPDP e a sua

[42] Os bens jurídicos violados pela burla e pela falsificação são, respetivamente, o património do burlado e a fé pública dos documentos necessária à normalização das relações sociais – portanto, diversos e autónomos. Por isso, entre os crimes de burla informática (Artigo 221º do Código Penal) e o crime de falsidade informática (Artigo 3º da Lei Cibercrime), existe concurso real de infrações - Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_15_jurisprudencia_penal_substantiva_2.pdf - Acedido em 19/09/2025

substituição pela Lei nº 58/2019, de 8 de agosto que, por sua vez, assegura a execução do regulamento em Portugal. No domínio penal, a Lei nº 67/98, de 26 de outubro já previa tipos criminais específicos, como o crime de acesso indevido do artigo 44º ou o crime de viciação ou destruição de dados pessoais do artigo 45º que, embora com alterações pontuais, foram posteriormente incluídos na Lei nº 58/2019, de 8 de agosto. Na esfera da influência do Direito privado, os avanços repercutem-se também nos direitos de personalidade (Cordeiro, 2020). Direitos esses tutelados no catálogo dos DLG, nos artigos 26º e 27º da CRP.

Com efeito, a prática do *Cibersextortion* pode preencher tipos penais previstos na Lei nº 58/2019 de 8 de agosto. Um exemplo é o crime de acesso indevido, p.p. pelo artigo 47º do referido diploma, cuja conduta típica consiste no acesso a dados pessoais, por qualquer modo, sem a devida autorização ou justificação legal. O bem jurídico tutelado é a autodeterminação informativa, enquanto manifestação do direito à reserva da intimidade da vida privada, protegendo-se a esfera de controlo do titular dos dados contra intrusões não consentidas. No plano subjetivo, a conduta é punível a título de dolo, sendo suficiente o dolo genérico, nos termos do artigo 13º do CP, não se exigindo qualquer intenção específica por parte do agente. Configurado como um crime de dano, a sua consumação ocorre com o próprio acesso não autorizado, que materializa a lesão do direito à privacidade, independentemente de se verificar um prejuízo subsequente. Trata-se de um crime público, sendo a tentativa punível. A sua forma simples é punida com pena de prisão até um ano ou pena de multa até 120 dias, sendo a pena agravada, nos termos do nº 2, para o dobro dos seus limites quando o acesso incida sobre dados sensíveis, nos termos do nº 3 a), se houver violação de regra de segurança e, nos termos do nº 3 b), se houver benefício ou vantagem económica (Venâncio, 2025). Ora, como facilmente se compreende, no caso do *Cibersextortion*, este pode ser um crime praticado, principalmente, durante a fase de obtenção dos ficheiros. Pensemos, por exemplo, naqueles casos em que os ofensores, depois de estarem na posse de senhas de acesso aos dispositivos, obtidas através *malware*, acedem aos ficheiros íntimos das vítimas sem autorização.

Naquelas situações em que as vítimas fornecem os dados voluntariamente, por exemplo, fotografias ou vídeos de cariz mais íntimo para uma suposta oferta de trabalho na área da moda, em que na sequência os ficheiros são utilizados como ferramenta de extorsão ou coação, podemos estar perante o crime de utilização de dados de forma incompatível com finalidade da recolha p.p. pelo artigo 46º da DPDP. O elemento objetivo do tipo preenche-se com a utilização de "dados pessoais de forma incompatível com a finalidade determinante da recolha". Do tipo legal não constam igualmente elementos subjetivos, exigindo-se apenas o dolo genérico do artigo 13º do CP. Trata-se igualmente de um crime de dano que se consuma com a falta de legitimidade para tratar os dados pessoais - veja-se que foram cedidos tendo em vista o acesso a um trabalho, mas, depois utilizados para outra finalidade. A sua forma simples prevê uma moldura penal de até um ano de prisão ou pena de multa até 120 dias, sendo a pena agravada pelo seu nº 2, para o dobro nos seus limites caso se trate de dados pessoais sensíveis dos artigos 9º e 10º do RGPD. Não está prevista a punibilidade da negligência e, tratando-se da previsão de pena de prisão inferior a três anos, mesmo que agravada pelo nº 2, apenas é punido na forma dolosa. Ter em conta que o artigo 53º da LPDP prevê a punibilidade da tentativa para todos os seus crimes. Trata-se de um crime publico, não está prevista a necessidade de queixa ou acusação particular para a ação penal (Venâncio, 2025).

Imagine-se agora um caso onde o agente, através da prática do crime de acesso indevido, tratado acima, do artigo 47º da LPDP, acede ao sistema informático da vítima. E, através desse acesso copia, subtrai, cede a outrem ou transfere dados pessoais sem consentimento da vítima. Comete o crime de desvio de dados p.p. pelo artigo 48º da LPDP. O elemento objetivo do tipo legal preenche-se justamente pela ação de "Copiar, subtrair, ceder ou transferir" dados pessoais, "sem a previsão legal ou consentimento". Também aqui não é exigido qualquer elemento subjetivo específico "independentemente da finalidade prosseguida" exigindo mesmo assim que a atuação do agente seja dolosa, artigo 13º do CP. Estamos novamente perante um crime de dano, que se consuma com a violação da privacidade dos dados pessoais. Na sua forma simples prevê pena de prisão até um ano ou pena de multa até 120 dias. O nº 2 prevê agravação das penas para o dobro nos seus limites quando se trate dos dados sensíveis, previstos

nos artigos 9º e 10º do RGPD. O nº 3, na alínea a), prevê igual agravação quando o acesso for conseguido através de violação de regra de segurança e, na alínea b), quando o agente obtiver benefício ou vantagem patrimonial.

2 Das ações típicas

A análise das ações típicas do *Cibersextortion* revela-se essencial para compreender de que modo este fenómeno se materializa em condutas que podem preencher tipos penais dispersos por diversos diplomas. Apesar de não existir no ordenamento jurídico português um crime autónomo de *Cibersextortion*, a sua repressão é frequentemente determinada pela violação de bens jurídicos como a liberdade e autodeterminação sexual, da reserva da intimidade da vida privada e, em muitos casos, do património das vítimas. A compreensão criminológica e a resposta jurídico-penal, dada a pluralidade de estratégias usadas pelos ofensores, torna necessário sistematizar as etapas decorrentes do processo criminológico. Com efeito, a prática do *Cibersextortion* desenvolve-se habitualmente em três fases interligadas. Uma primeira, a recolha de ficheiros ou dos elementos íntimos da vítima, por meios lícitos ou ilícitos. Uma segunda, a fase das exigências, em que os ficheiros são convertidos em instrumentos de ameaça ou extorsão. E, por fim, uma terceira, a fase de cumprimento das exigências ou de publicação, que representa a consumação do *Cibersextortion*, seja pela submissão da vítima às imposições do ofensor, seja pela efetiva difusão dos conteúdos. A estruturação destas fases não só permite compreender a dinâmica criminosa como facilita a identificação dos tipos legais de crime aplicáveis em cada momento.

2.1 Breves considerações

Como vimos acima o *Cibersextortion* pode ocorrer por várias formas e por isso envolver tipos penais dispersos por legislação extravagante além do CP. Neste trabalho, devido às múltiplas formas que a prática do *Cibersextortion* pode seguir, não é possível abordar todos os crimes praticados em cada uma delas. Posto isto, iremos em seguida tentar expor os crimes mais comumente praticados nas várias fases que contemplam a

execução do *Cibersextortion*. Para tanto identificamos três fases principais. São elas, a fase de recolha de ficheiros – sejam obtidos de forma lícita ou ilícita, reais ou manipulados -, fase das exigências – pedido de dinheiro, mais ficheiros ou encontros presenciais – e, por fim, a fase de cumprimento das exigências – receção de ficheiros comprometedores, dinheiro ou encontros presenciais - ou a publicação dos ficheiros – nas redes sociais digitais ou junto de familiares, amigos ou colegas.

Assim, tendo em vista o enquadramento da prática do *Cibersextortion* nos tipos penais existentes, apresentamos um conjunto de normas previstas para facilitar, por um lado, esse enquadramento e, por outro, expor o modo de execução durante todas as etapas ao longo deste processo criminológico.

2.1.1 Recolha dos ficheiros

Como referido anteriormente quando se tratou do *modus operandi* na secção (1), a recolha de ficheiros sexualmente comprometedores das vítimas pode ocorrer de várias formas. O método utilizado nesse processo depende em grande medida das informações detidas pelos ofensores [43] sobre as vítimas. Nesta fase de recolha de informações os ofensores podem recorrer a abordagem complexas, que vão desde esquemas de engenharia social a uso de *malware* em esquemas de crime organizado, ou a táticas mais simples que passam por, por exemplo, recolha de informações em redes sociais digitais ou aplicações digitais de promoção de encontros amorosos. Estas ações de recolha de informações podem ainda dar-se por contacto direto entre vítimas e ofensores. Seja por meio de relações afetivas onde são partilhados ficheiros íntimos em formato digital entre as pessoas envolvidas, ou na sequência de situações de captura ao vivo de fotografias ou vídeos que representem a vítima.

A recolha de ficheiros é assim o ponto de partida do *Cibersextortion*. Sem as fotografias, vídeos ou mensagens constrangedoras da vítima, o ofensor não tem elementos para

[43] note-se que quando falamos em "ofensores", utilizando o vocábulo na forma masculina, não estamos a delimitar a prática destas ações apenas a ofensores masculinos, mas sim a ambos os sexos, visto que no nosso idioma esta forma é suficiente para abranger tanto homens como mulheres, enquanto utilizar o termo "ofensoras" limita a ação apenas às mulheres.

impor a sua vontade. Ou seja, a posse desses materiais aliado à ameaça da sua divulgação convertem-se na arma utilizada para forçar a vítima a ceder nos seus bens jurídicos penalmente protegidos. Sejam eles pessoais ou patrimoniais.

Como acabamos de expor, a obtenção dos ficheiros pode ocorrer por diferentes vias. Desta forma, cada um daqueles métodos de obtenção de ficheiros pode preencher um ou vários tipos penais. Como os crimes previstos na LC - o de falsidade informática do artigo 3º, o de dano relativo a programas ou outros dados informático do artigo 4º, o de sabotagem informática do artigo 5º, o de acesso ilegítimo do artigo 6º ou o de intercepção ilegítima do artigo 7º -, os crimes previstos no CP como o de devassa da vida privada do artigo 192º do CP, o de violação de correspondência ou telecomunicações do artigo 194º ou o de gravações e fotografias ilícitas do artigo 199º e, os menos óbvios como o crime de fraude sexual do artigo 167º, o crime de aliciamento de menores para fins sexuais do artigo 176º-A ou o crime relativo a instrumentos de escuta telefónica do artigo 276º, enquanto atos preparatórios para obtenção dos ficheiros aptos a constranger a vitima. Os crimes previstos na Lei 58/2019 de 8 de agosto podem igualmente ser preenchidos no que à recolha de ficheiros diz respeito. Deste modo podem ser recolhidos na sequência do crime de acesso indevido artigo 47º e do crime de desvio de dados do artigo 48º, ambos da LPDP.

Passamos a expor de forma sucinta algumas situações. Em primeiro lugar, quando a vítima fornece voluntariamente os ficheiros ou dados pessoais, sem engano ou pressão, não se preenche, em regra qualquer tipo penal. A ilicitude apenas surge quando tais ficheiros são utlizados para fins de ameaça, coação ou extorsão. Já quando a obtenção dos ficheiros decorre de intrusão no sistema informático da vítima, com a utilização de *malware*, por exemplo, *Keyloggers* ou RAT, a conduta pode configurar o crime de acesso ilegítimo p.p. pelo artigo 6º da LC. Se os ficheiros recolhidos são dados pessoais, o que quase sempre acontece, a intrusão pode então, como vimos acima, preencher o crime de acesso indevido p.p. pelo artigo 47º e, caso haja cópia não autorizada, o crime de desvio de dados p.p. pelo artigo 48º ambos da LPDP. Quando os ofensores recorrem à interceção de comunicações eletrónicas, por exemplo, ao capturar mensagens ou vídeos enviados pela vítima através de plataformas de interações em linha, a conduta do

ofensor enquadra-se no crime de interceção ilegítima p.p. pelo artigo 7º da LC, podendo ainda assim configurar o crime de violação de correspondência ou telecomunicações p.p. pelo artigo 194º co CP.

Como se fez igualmente notar acima, se os dados obtidos foram inicialmente recolhidos de forma legitima para um determinado fim, mas o agente os usa para fins de chantagem, pode estar em causa o crime de utilização de dados pessoais para fins diversos dos da recolha, previsto no artigo 46º da LPDP.

Já nos casos em que a recolha envolve a gravação ou captura de imagens sem consentimento, é aplicável o crime de gravações e fotografias ilícitas, do artigo 199º do CP, bem como, em situações que afetem a esfera íntima da vida privada, o crime de devassa da vida privada p.p. pelo artigo 192º do CP. Ainda assim, se durante a obtenção dos ficheiros, o ofensor apagar ou danificar conteúdos no dispositivo da vítima, a conduta pode preencher o crime de dano relativo a programas ou outros dados informáticos p.p. pelo artigo 4º da LC ou, em situações de maior gravidade, o crime de sabotagem informática p.p. pelo artigo 5º da LC.

A fase de recolha de dados é determinante para avaliar a licitude das condutas. Dela depende não só a verificação do consentimento válido para o tratamento dos dados, mas também qualificação jurídica das eventuais ofensas, designadamente quando envolvem a violação de dados pessoais, a intrusão na segurança dos sistemas informáticos ou a devassa da intimidade.

2.1.2 Exigências dos agentes

A fase das exigências representa o momento em que os ofensores transformam os ficheiros íntimos previamente recolhidos em instrumentos de coação e extorsão. É nesta etapa que se podem materializar o crime de ameaça do artigo 153º, o crime de coação sexual do artigo 163º, o crime de perseguição do artigo 154º-A, o crime de extorsão do artigo 223º, ou ainda o crime de aliciamento de menores para fins sexuais do artigo

176º-A, todos do CP. O agressor procura obter da vítima atos sexuais, dinheiro, mais ficheiros íntimos ou mesmo o seu silêncio. Normalmente é nesta fase que a vítima é confrontada com a exigências de contrapartidas para que o agente não publique os seus ficheiros e dependendo do caso concreto podem ser preenchidos mais do que um tipo penal.

A conduta mais comum é a ameaça prevista no artigo 153º do CP. No plano objetivo, o ofensor comunica à vítima que divulgará o material íntimo caso ela não cumpra determinadas exigências. A ameaça é típica quando é idónea para provocar medo ou inquietação na vítima. O elemento subjetivo consiste no dolo, bastando que o agente tenha consciência de que a sua conduta é apta a constranger a vítima. Quando as exigências envolvem a práticas de natureza sexual, a conduta enquadra-se no crime de coação sexual p.p. pelo artigo 163º do CP. No plano objetivo o tipo exige que o agente constranja a vítima, mediante violência ou ameaça grave, a suportar ou a praticar ato sexual de relevo. A ameaça de divulgar imagens íntimas preenche este requisito, uma vez que vicia a liberdade da vítima. No plano subjetivo, exige-se igualmente dolo, ou seja, que o agente atue com consciência e vontade de obter a submissão da vítima para fins sexuais [44].

Nos casos em que o comportamento do agressor envolve um padrão de contactos persistentes, vigilância ou perseguição, capazes de afetar a liberdade ou a autodeterminação da vítima, pode preencher os elementos do crime de perseguição, *stalking*, p.p. pelo artigo 154º-A do CP. Objetivamente, exige-se a repetição de atos que provoquem medo ou ansiedade na vítima, exigindo-se qualquer forma de dolo do artigo 13º do CP.

Quando a exigência visa a obtenção de quantias em dinheiro, bens ou outra vantagem patrimonial, a conduta subsume-se ao crime de extorsão, p.p. pelo artigo 223º do CP. O elemento objetivo consiste em constranger a vítima, por meio de violência ou ameaça com mal importante, a praticar ato que cause prejuízo no seu património. A ameaça de

[44] Tribunal da Relação do Porto, de 06 de dezembro de 2023, relativo ao Processo (2071/21.7JAPRT.P1) disponível em https://diariodarepublica.pt/dr/detalhe/acordao/2071-2023-877985175 - Acedido em Acedido em 07/10/2025

divulgar conteúdos íntimos constitui o mal utilizado pelo agente para pressiona a vítima. O elemento subjetivo é o dolo específico, dirigido a obter enriquecimento ilegítimo e subsequente prejuízo da vítima [45].

Nos casos que envolvem vítimas menores, a exigência de produção de novas imagens íntimas ou solicitação e atos sexuais enquadra-se com crime de aliciamento de menores para fins sexuais, p.p. pelo artigo 176º do CP. No plano objetivo, exige-se aqui o aliciamento ou indução do menor, através de meios tecnológicos, para que pratique ou se preste a praticar ato sexual de relevo ou produza material com esse conteúdo. Aqui apenas se exige o dolo genérico.

Em muitos casos de *Cibersextortion*, estas condutas não surgem isoladas. O mesmo ato de ameaçar pode simultaneamente visar a obtenção de atos sexuais e de vantagem económica. Nestas situações, a ação do ofensor pode preencher mais do que um tipo penal, ocorrendo concurso real de crimes, a determinar consoante o caso concreto. Esta fase das exigências é aquela em que os ficheiros previamente obtidos passam a ser utilizados como ferramenta de constrangimento. É igualmente nesta fase que a violação da liberdade sexual, da reserva da intimidade da vida privada e do património da vítima se torna mais evidente, refletindo a gravidade da conduta do agente e a necessidade de uma resposta penal adequada.

2.1.3 Publicação dos ficheiros

A fase de cumprimento das exigências ou da publicação dos ficheiros marca a consumação do *Cibersextortion*. É nesta fase que os ofensores concretizam o objetivo das suas ações criminosas, seja pelo cumprimento das exigências por parte da vítima, seja pela execução das ameaças do ofensor de publicar os ficheiros íntimos delas. Tal como nas fases anteriores, também aqui se deve ter em conta que, dependendo do ato praticado, podem ser preenchidos tipos penais distintos porque tutelam bens jurídicos

[45] Tribunal da Relação do Porto, de 06 de dezembro de 2023, relativo ao Processo (2071/21.7JAPRT.P1) disponível em https://diariodarepublica.pt/dr/detalhe/acordao/2071-2023-877985175 - Acedido em Acedido em 07/10/2025

igualmente distintos. Pode ainda dar-se o caso de alguns tipos penais entrarem em concurso entre eles para determinação concreta da medida pena. Os crimes praticados até esta fase são potencialmente aptos a serem praticados também aqui. Ou seja, nesta fase, os ofensores podem continuar a recolher ficheiros íntimos das vítimas e até aumentar as exigências. Pois agora estão na posse de ficheiros que, aliados à ameaça da sua divulgação publica, são capazes de provocar medo e desespero nas vítimas e levá-las a cumprir com novas exigências.

Ainda assim, o catálogo de crimes que podem ser praticados nesta fase não se esgotam com os praticados até aqui. Pelo contrário abrem ainda mais o catálogo. Apenas para listar alguns, podemos desde logo referir aqueles que tutelam a liberdade e autodeterminação sexual, como o crime de violação p.p. pelo artigo 164º, ou o abuso sexual de crianças p.p. pelo artigo 171º, crimes contra a devassa da vida privada como o crime de devassa através de meio de comunicação social, da *Internet* ou de outro meio de difusão pública generalizada p.p. pelo artigo 193º e crimes contra o património como a extorsão p.p. pelo artigo 223º todos de CP.

No plano da liberdade e autodeterminação sexual, temos desde logo, os crimes de violação e de abuso sexual de crianças. O crime de violação, p.p. pelo artigo 164º do CP, exige, no plano objetivo, que o agente constranja a vítima, por meio de violência, ameaça grave ou depois de a ter colocado em estado de inconsciência ou incapacidade, a sofrer ou a praticar ato de cópula ou ato sexual de relevo. No contexto de *Cibersextortion*, a ameaça de divulgar imagens íntimas pode funcionar como instrumento de constrangimento bastante para preencher o elemento objetivo do tipo, anulando a liberdade de decisão da vítima. No plano subjetivo, exige-se o dolo, ou seja, que o agente atue com consciência e vontade de forçar a vítima à prática de ato sexual (Mouraz & Milheiro, 2023). Quando a vítima é menor de 14 anos, a conduta enquadra-se no crime de abuso sexual de crianças, p.p. pelo artigo 171º do CP, que tutela de forma reforçada a autodeterminação sexual dos menores. Este tipo penal dispensa a prova de violência ou de ameaça grave, bastando a prática de atos sexuais de relevo com ou perante menor, dado o seu estado de especial vulnerabilidade. O dolo do agente

configura-se, neste caso, a satisfazer instintos ou fins libidinosos, pela exploração da imaturidade da vítima.

No domínio da reserva da intimidade da vida privada, releva o crime de devassa através de meio de comunicação social, da internet ou de outro meio de difusão publica generalizada, p.p. pelo artigo 193º do CP. Como acima referido quanto a este tipo penal, no plano objetivo, exige que o ofensor contribua para a disseminação pública de imagens, fotografias ou gravações que revelem a intimidade da vida privada, familiar ou sexual de outrem, sem o seu consentimento. A publicação de ficheiros íntimos nas redes sociais, fóruns ou aplicações de mensagens preenche este requisito. Subjetivamente, basta o dolo genérico (Venâncio, 2025). Ou seja, a consciência e a vontade de difundir ou facilitar a difusão do conteúdo íntimo.

2.2 *Cibersextortion* na jurisprudência nacional

Passamos agora a explorar o modo como o *Cibersextortion* tem sido enquadrado pelos tribunais nacionais. A jurisprudência analisada permite apresentar diversas manifestações desta criminalidade. Entre elas, crimes contra a liberdade pessoal, contra a liberdade e autodeterminação sexual, crimes contra a reserva da intimidade da vida privada e crimes contra o património. Por força da nossa seleção, predominantemente processos cujos condutas criminais são praticadas por meios digitais, inserem-se no contexto do *Cibersextortion*. De modo a simplificar a compreensão do *Cibersextortion* vamos explorar apenas tipos penais que se observam em todos os casos deste fenómeno. Para tanto analisamos casos da jurisprudência nacional.

2.2.1 Caso 1 – Acórdão do Tribunal da Relação de Coimbra

O Acórdão do Tribunal da Relação de Coimbra de 13 de dezembro [46], julgou o caso no qual os arguidos eram companheiros, um homem (A) e uma mulher (B), e juntos

[46] https://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/a56438301c7769b780258209003e23a7?OpenDocument

decidiram montar um plano para obter dinheiro da vítima (C) que era igualmente ex-mulher do arguido (A). Para isso o arguido (A) convenceu a vítima a ir a sua casa com o pretexto de tomar café. O arguido (A), tinha colocado um dispositivo de gravação de som e imagem escondido e apontado para a cama, que foi ligado antes da chegada da vítima. Durante a visita, o arguido (A) manteve relações sexuais com a vítima que foram gravadas sem o consentimento desta. Pouco tempo depois a arguida (B) entrou em contacto com a vítima, exigindo-lhe dinheiro para evitar que o vídeo fosse divulgado. Pagamento que a vítima recusou. Face à recusa os arguidos publicaram o vídeo na conta de *Facebook* da vítima, expondo publicamente a sua intimidade e causando-lhe profundo vexame.

O tribunal condenou os arguidos pelo crime de gravações ilícitas p.p. pelo artigo 199º do CP, pelo crime extorsão na forma tentada, p.p. pelos artigos 223º, nº 1, 22º, 23º nºs 1 e 2, e 73º nº 1, b) todos do CP e, pelo crime de devassa da vida privada p.p. pelo artigo 192º nº 1, b) [47], pela divulgação efetiva do vídeo.

O MP, imputava aos arguidos, a prática em autoria material e concurso real, de um crime de extorsão na forma tentada, p.p. pelos artigos 21º e 223º, nºs 1 e 2, de dois crimes de devassa da vida privada p.p. 192º, nº 1, b) e d) e 197º, a), e de um crime de gravações ilícitas, p.p. pelo artigo 199º, nºs 1 e 2 b), todos do CP.

Na sentença recorrida os arguidos vinham condenados pela prática do crime de extorsão, na forma tentada e de um crime de devassa da vida privada agravada em concurso aparente com o crime de gravações e fotografias ilícitas, o arguido (A), nas

[47] Ter em conta que o acórdão em referência data de 2017/12/13. Data onde o artigo 192º tinha a seguinte redação "Artigo 192.º Devassa da vida privada;
1 - Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:
a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio electrónico ou facturação detalhada;
b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos;
c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou
d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa; é punido com pena de prisão até um ano ou com pena de multa até 240 dias.
2 - O facto previsto na alínea d) do número anterior não é punível quando for praticado como meio adequado para realizar um interesse público legítimo e relevante.
Redacção dada pelo seguinte diploma: Lei n.º 59/2007, de 04 de Setembro
Disponível em - https://www.pgdlisboa.pt/leis/lei_busca_art_velho.php?nid=109&artigonum=109A0192&n_versao=2&so_miolo= Acedido em 18/09/2025

penas parcelares de 16 meses de prisão e 6 meses de prisão, respetivamente e, em cúmulo, na pena única de 1 ano e 7 meses de prisão. A arguida (B), nas penas parcelares de 12 meses de prisão e 120 dias de multa à taxa diária de € 5 e, em cúmulo, na pena única de 12 meses de prisão, suspensa na respetiva execução por igual período, e 120 dias de multa à taxa diária de € 5, perfazendo a multa global de € 600.

A decisão final foi no sentido de absolver os arguidos da agravação prevista na alínea a) do artigo 197º do CP, dando razão ao recorrente. Considerou o tribunal que o enriquecimento ilegítimo integra o tipo do crime de extorsão do artigo 223º, nº 1, e que usar o mesmo enriquecimento para preencher a agravação prevista no artigo 197º para o crime de devassa da vida privada do 192º significava uma dupla valoração da mesma circunstância. Entende ainda o tribunal que o crime de devassa da vida privada, p.p. no artigo 192º do CP, tutela o bem jurídico privacidade em sentido material, enquanto o crime de gravações ilícitas, p.p. no artigo 199º do CP, tutela os bens jurídicos direito à palavra e direito à imagem. Acrescenta que, em regra, deve ser considerada a existência de um concurso de normas, quando a filmagem ilícita é feita para permitir a devassa da intimidade, os crimes estão numa relação de concurso aparente. Porém, quando, como acontece neste caso, a filmagem ilícita é efetuada, não para devassar a intimidade da ofendida, mas para lhe extorquir dinheiro, e só porque esta não fez o pagamento pretendido, frustrando a extorsão, é que o filme é, posteriormente, publicitado numa rede social, devassando a sua intimidade, deve entender-se a existência de um concurso real entre o crime de gravações e fotografias ilícitas e o crime de devassa da vida privada.

2.2.2 Caso 2 – Acórdão do tribunal da Relação do Porto

Este caso, pela diversidade de vítimas e ações que analisa, é importante para se perceber as nuances do *Cibersextortion*.

O Acórdão do Tribunal da Relação do Porto [48], proferido a 6/12/2023, representa um caso relevante da jurisprudência portuguesa sobre o fenómeno do *Cibersextortion*. A decisão articula crimes sexuais, ilícitos contra o património e infrações praticadas por via informática, demonstrando a capacidade do direito penal português para enfrentar a criminalidade mediada por tecnologia. O acórdão permite ainda examinar de forma concreta a correspondência entre as condutas do agente e os tipos penais aplicados, bem como os fundamentos jurídicos que sustentam a decisão.

O Tribunal identificou um padrão de atuação reiterado e metódico do arguido, designado nos autos como BB. Durante vários anos, BB utilizou plataformas digitais como *Instagram*, *Snapchat*, WhatsApp e *Telegram* para contactar jovens mulheres, incluindo menores de idade. O *modus operandi* consistia na criação de perfis falsos e na apresentação de falsas promessas, como a obtenção de avultadas quantias monetárias ou a possibilidade de conhecer jogadores e empresários de futebol. O objetivo inicial era conquistar a confiança das vítimas e obter conteúdos íntimos. Posteriormente, esses conteúdos eram usados para as coagir a praticar atos sexuais, entregar dinheiro ou recrutar mais jovem. A ameaça de divulgação pública do material íntimo constituiu o ato principal de coação e extorsão na maioria das situações apreciadas.

A diversidade das condutas praticadas refletiu-se nos diferentes bens jurídicos lesados. No caso da vítima, identificada como AA, com apenas 13 anos de idade à data dos factos, o arguido limitou-se ao aliciamento, utilizando as redes sociais para prometer elevados ganhos financeiros em troca de encontros de cariz sexual. Não obstante, a ausência de contato físico e de obtenção de imagens íntimas, o Tribunal entendeu que tal conduta era suficientemente perturbadora da autodeterminação sexual da menor, subsumindo-a ao crime de importunação sexual p.p. no artigo 170º do CP.

A situação da vítima CC, com apenas 17 anos, ilustra um padrão mais típico do *Cibersextortion*. O arguido, fazendo-se passar por um conhecido jogador de futebol, obteve uma imagem de nudez da jovem e ameaçou com a sua publicação caso não

[48] Tribunal da Relação do Porto, de 06 de dezembro de 2023, relativo ao Processo (2071/21.7JAPRT.P1) disponível em https://diariodarepublica.pt/dr/detalhe/acordao/2071-2023-877985175 - Acedido em Acedido em 19/09/2025

cedesse às suas exigências. Sob coação, a vítima foi constrangida a praticar atos sexuais e a entregar-lhe 50€. O Tribunal qualificou os factos como violação agravada do artigo 164º nº 2, a), do CP, extorsão do artigo 223º do CP e, dada a idade da vítima e a posse de imagens íntimas da menor, no crime de pornografia de menor do artigo 176º do CP.

No caso da vítima DD, adulta à data dos factos, a atuação do arguido combinou diversas estratégias de manipulação. Inicialmente, a vítima foi levada a crer que obteria compensação financeira significativa por encontros com figuras do desporto profissional. Posteriormente foi filmada sem o seu consentimento em situação íntima. A partir daí, o arguido passou a ameaçar a vítima com a divulgação do vídeo para obter, não só novos encontros sexuais, mas também quantias monetárias que ascenderam a 4000€, e ainda a colaboração da vítima no aliciamento de outras jovens. Estes factos foram enquadrados como violação agravada do artigo 164º nº 2, a), devassa da vida privada do artigo 192º, burla do artigo 217º e coação do artigo 154º todos do CP.

A atuação do arguido contra FF e o seu companheiro GG, configura outro aspeto essencial no fenómeno do *Cibersextortion*, a combinação entre coação e difusão não consentida de conteúdos íntimos. Sob ameaça, de expor imagens privadas, o arguido obrigou a jovem a enviar vídeos de natureza sexual envolvendo ambos, que mais tarde foram partilhados em grupos do *Telegram*. Também acedeu de forma ilegítima às contas de redes sociais da vítima, comunicando com terceiros como se fosse a própria. O tribunal entendeu que estas condutas preencheram os crimes de devassa da vida privada do artigo 192º do CP e de acesso legítimo do artigo 6º da LC.

A vítima HH, foi alvo de múltiplas formas de exploração. Inicialmente aliciada com promessas de remuneração elevadas para se encontrar com profissionais de futebol e depois coagida a manter relações sexuais com o arguido e a entregar dinheiro sob ameaça de divulgar os conteúdos íntimos. Estas condutas foram enquadradas como crime de violação do artigo 164º, de burla do artigo 217º, de devassa da vida privada do artigo 192º, todos de CP e de acesso ilegítimo do artigo 6º da LC.

O caso da vítima II constituiu uma tentativa frustrada de obter dinheiro por meio semelhante, sendo enquadrado pelo tribunal como crime de extorsão na forma tentada p.p. pelos artigos 22º, 23º e 223º, todos do CP. As vítimas JJ e KK foram, por sua vez, sujeitas a coação de natureza sexual e à utilização abusiva de imagens íntimas, conduzindo à condenação do arguido por violação agravada do artigo 164º nº 2, a), e devassa da vida privada do artigo 192º, ambos do CP. Já as vítimas LL e MM, foram alvo de tentativa de aliciamento e de constrangimento, que, apesar de não terem resultado em atos sexuais consumados, configuraram o crime de coação p.p. pelo artigo 154º e importunação sexual p.p. pelo artigo 170º, ambos do CP.

Este acórdão do Tribunal da Relação do Porto, de 06 de dezembro de 2023, destaca a preocupação crescente com os crimes contra a liberdade e autodeterminação sexual mediados pela informática, com referência expressa ao *Cibersextortion, " Os crimes contra a liberdade e autodeterminação sexual são objeto de clara reprovação geral, sendo que em especial tal criminalidade ligada à utilização de meios informáticos, mormente via Internet e redes sociais, assume uma dimensão cada vez mais alarmante em termos comunitários, atenta a proliferação de acesso a tais meios por jovens e crianças, que tantas vezes se veem expostos à manipulação por terceiros, e envolvidos assim em situações denominadas de sextortion e de exploração sexual, das quais, depois revelam dramáticas dificuldades em escapar, por via dos sentimentos de vergonha com que são chantageados, numa espiral de desespero tantas vezes de resultados trágicos - pois que este tipo de devassa da vida privada tem um efeito psicológico devastador sobre as vítimas*.".

2.2.3 Caso 3 – Acórdão do Tribunal da Relação de Évora

No Acórdão do Tribunal da Relação de Évora de maio de 2024 [49], embora verse sobre questões de apreensão de saldos bancários, o Ministério Público (MP) enquadra os factos ocorridos como *Cibersextortion*. Ou seja, o ofendido ter recebido mensagens de supostas mulheres com quem trocou conteúdos íntimos, seguidas de contactos

[49] https://diariodarepublica.pt/dr/detalhe/acordao/89-2024-878619275 - Acedido em 17/09/2025

telefónicos efetuados a partir de números estrangeiros, via *WhatsApp*, com ameaças de divulgar aqueles conteúdos caso não pagasse certas quantias em dinheiro, o MP sustenta que tais factos preenchem um crime de extorsão agravada, p.p. pelo artigo 223º, nº 1 e 3, alínea a), por referência aos artigos 202º, alínea b) e 204º, nº 2, alínea a), todos do CP.

V. Conclusões

O fenómeno do *Cibersextortion* é indissociável do ambiente digital em que ocorre. A utilização das TIC é central desde a fase inicial de aproximação à vítima até à fase de execução das ameaças. A recolha de ficheiros íntimos e comprometedores pode resultar de ações diretas da vítima, partilhando voluntariamente os materiais, ou de meios ilícitos, como o uso de *malware* ou outras formas de intrusão e apropriação indevida de dados. A captura de imagens durante chamadas de vídeo e a possibilidade de armazenar conteúdo íntimos das vítimas, fazem deste um fenómeno híbrido. Ou seja, trata-se de um fenómeno de manipulação psicológica mediado pela tecnologia.

Uma primeira nota que, de início, ficou patente tem que ver com a própria utilização do termo "*sextortion*". Parece fazer mais sentido utilizar-se os termos, "*Cibersextortion*" no contexto português e, "*Cybersextortion*" em contexto internacional. Na verdade, não se trata de uma inovação extraordinária, mas antes de fazer corresponder os atos ao espaço onde são praticados, tal como acontece com, por exemplo, o *Cyberstalking* ou o *Cyberbullying*. Práticas originárias do mundo físico e replicadas no mundo digital. Motivo pelo qual apontemos o termo "*Cibersextortion*" como o mais adequado - para fazer referência aos atos de constrangimento, coação ou ameaça de exposição publica de imagens que visem devassar a vida sexual das pessoas, através de meios de comunicação social, *Internet* ou outras formas de divulgação publica, para obter contrapartidas.

O *Cibersextortion* caracteriza-se por um conjunto de ações que combinam práticas tradicionais de extorsão com estratégias específicas do cibercrime. A sua execução

depende do uso das TIC, *softwares* maliciosos – *malware*, *keylogger*, RAT e técnicas de *phishing* – e elementos de manipulação psicológica, baseados muitas vezes em perfis falsos para a construção de uma relação de confiança com as vítimas. Esta consciência do carácter multifacetado do fenómeno ajuda a fundamentar a necessidade de encontrar soluções técnicas e jurídicas, promover ações de sensibilização e prevenção junto de crianças e jovens e reforçar a cooperação institucional. Do ponto de vista jurídico, constata-se que o ordenamento jurídico português não consagra um tipo penal autónomo de *Cibersextortion*, levando a que os atos praticados na sua execução sejam enquadrados em tipos penais dispersos pelo CP e legislação extravagante como a LC ou LPDP.

A análise efetuada ao longo da dissertação permitiu ainda identificar três fases fundamentais do *Cibersextortion*. A primeira, de recolha de ficheiros, pode não configurar qualquer infração penal quando a vítima partilha voluntariamente os seus conteúdos. Contudo, sempre que a recolha resultar de intrusão em sistemas informáticos ou interceção de comunicações, podem estar em causa crimes previstos na LC como, o de acesso ilegítimo p.p. pelo artigo 6º ou interceção ilegítima p.p. pelo artigo 7º, crimes previstos na LPDP, como o do artigo 47º e o artigo 48º, ou ainda, entre outros os crimes de devassa da vida privada p.p. pelo artigo 192º ou o de gravações e fotografias ilícitas p.p. pelo artigo 199º, ambos do CP. A segunda fase, corresponde às exigências do ofensor, trata-se da transformação dos ficheiros em "arma" de coação e extorsão, preenchendo, consoante os casos, os tipos legais, por exemplo, de ameaça p.p. pelo artigo 153º, coação sexual p.p. pelo artigo 163º, extorsão p.p. pelo 223º ou de perseguição p.p. pelo artigo 154º-A todos do CP. Por fim, a fase de cumprimento ou de publicação, que ocorre quando a vítima cede às exigências ou quando o agressor difunde os conteúdos, pode envolver crimes como, por exemplo, de violação p.p. pelo artigo 164º, o crime de abuso sexual de crianças p.p. pelo artigo 171º ou ainda o crime de devassa através de meio de comunicação social p.p. pelo artigo 193º, todos do CP. Pode, ainda nesta última fase, ocorrer crimes contra o património.

No que diz respeito à necessidade de autonomização do crime de *sextortion* em lei penal nacional, encontramos nos casos de corrupção institucional ou funcional, uma

fragilidade de enquadramento passível de melhor enquadramento. Face a esse quadro admitimos o alinhamento de uma resposta normativa específica para o *Cibersextortion*. Entre elas destacam-se a clarificação dos elementos típicos adaptados ao ambiente digital, harmonização do tratamento processual quando estejam em causa fatores agravantes – idade da vítima, dependência económica, relação de poder -, e previsão expressa para condutas híbridas que combinem ameaça de teor sexual com exigências patrimoniais. Entendemos que sem estes ajustes estruturais, mantem-se o risco de interpretações díspares pelos tribunais portugueses perante factos semelhantes, comprometendo a coerência punitiva e a proteção das vítimas destes atos que causam danos profundos nas esferas pessoal e social. Importa ainda referir a este respeito, a complexidade em colocar o *Cibersextortion* no catálogo dos cibercrimes em sentido amplo ou sentido restrito (Nunes, 2020; Venâncio, 2023b), uma vez que durante a sua execução pode, para punir os atos praticados, ser necessário recorrer tanto a uma categoria como à outra ou a ambas. Dependendo do caso em concreto.

Como sugestões para trabalhos futuros, com vista melhorar a resposta tecnológica e jurídica ao fenómeno do *Cibersextortion* em Portugal, aponta-se para a realização de estudos de prevalência do fenómeno em Portugal. Alguns relatórios, como os RASI, apontam para uma subida ao longo dos últimos anos, no entanto a falta de informação leva a que ainda se considere a existência de cifras negras elevadas. Estudar mais aprofundadamente os meios de obtenção de prova digital, a sua cadeia de custódia e formas de garantir a sua admissibilidade em tribunal. Isto podia ajudar tanto no combate como na condenação dos ofensores. Por fim, seria igualmente pertinente, perceber-se com maior rigor as respostas que outras jurisdições dão na repressão e prevenção do *Cibersextortion*. E, que respostas de coordenação internacional estão atualmente disponíveis e o impacto que a I.A. Generativa pode ter neste fenómeno.

VI. Bibliografia

Açar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology (IJCC)*, *10*(2), 110–126. https://doi.org/10.5281/zenodo.163398/IJCC

Andrade, M. C. (2009). *Bruscamente no Verão passado: A reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*. Coimbra Editora.

Casa Branca, C. M., Grangeia, H., & Cruz, O. (2016). Grooming online em Portugal: Um estudo exploratório. *Análise Psicológica*, *34*(3), 249–263. https://doi.org/10.14417/ap.978

Coelho, C. F. (2013). *ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO*. 34–44. https://doi.org/10.25242/885X305201387

Cordeiro, A. B. M. (2020). *Direito da Proteção de Dados*. Almedina.

Da Silva, A. G. (2025, January 24). *Os perigos decorrentes das relações pessoais e sexuais e a intervenção judicial - Burla no amor, sextortion - extorsão sexual, aliciamento sexual. cyberbulling, perseguição e violência doméstica*.

De Andrade, F. P., Fonseca, I., E Silva, J. A., De Abreu, J. C., Jerónimo, P., Venâncio, P. D., & Freitas, P. M. (2020). *Relatório Cibersegurança em Portugal: Ética & Direito*. https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriocibersegurança-cncs.pdf

Deodato, B. R. L. (2024). *A INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL E A UTILIZAÇÃO DE MALWARE COMO MEIO DE OBTENÇÃO DE PROVA ENTRE A INEFICÁCIA E A ILEGALIDADE* [Universidade de Coimbra]. https://hdl.handle.net/10316/118220

Dias, J. de F. (2001). *Temas Básicos da Doutrina Penal - Sobre os Fundamentos da Doutrina Penal Sobre a Doutrina Geral do Crime* (Coimbra Editora, Ed.).

Dias, J. de Figueiredo., & Andrade, M. da Costa. (1997). *Criminologia O Homem delinquente e a Sociedade criminógena*. Coimbra Editora.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, *2*, 1–9. https://doi.org/10.1016/j.jeconc.2023.100038

Europol. (2018). *Iocta, Internet Organised Crime Threat Assessment: 2018*. Europol. https://doi.org/10.2813/858843

Europol. (2023). *IOCTA, internet organised crime threat assessment 2023*. Europol. https://doi.org/10.2813/587536

Europol. (2024). *IOCTA - Internet Organised Crime Threat Assessment (IOCTA) 2024*. https://doi.org/10.2813/442713

Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of Online Sexual Offenses Against Children in the US. *JAMA Network Open*, *5*(10), E2234471. https://doi.org/10.1001/jamanetworkopen.2022.34471

France, G. (2022). *Criminalising sextortion: challenges and alternatives*. https://www.jstor.org/stable/resrep41907?seq=1

Gomes, V. A. N. (2019). *A Engenharia Social e os Perigos do phishing* [Instituto Universitário de Lisboa]. https://repositorio.iscte-iul.pt/bitstream/10071/20286/1/Master_Vanessa_Nunes_Gomes.pdf

Gonçalves, J. M. A. (2015). *Pharming: Análise dogmático-penal, em especial enquanto forma de lesão do património* [ED UMinho]. https://repositorium.sdum.uminho.pt/bitstream/1822/40931/1/Joana%20Margarida%20Andrade%20Gon%c3%a7alves.pdf

Goncalves, M. M. dos S. (2023). *A influência das redes sociais na vitimação por cyberstalking em estudantes universitários* [ED Uminho]. https://repositorium.uminho.pt/bitstream/1822/93474/1/Monica%20Maria%20dos%20Santos%20Goncalves.pdf

Guedes, I. S., Martins, J., & Moreira, S. (2025). Explaining fear of cybercrime: A focus on interpersonal and property cybercrime differences. *European Journal of Criminology*, *22*(4), 578–602. https://doi.org/10.1177/14773708241312820

Guedes, I. S., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: an empirical study. *Security Journal*, *36*(3), 472–497. https://doi.org/10.1057/s41284-022-00350-5

Hedidi, M. (2023). *Perspective Chapter: Sexual Cybercrime-The Transition from the virtual aggression to the physical Aggression*. IntechOpen. https://doi.org/10.5772/intechopen.108786

Henry, N., & Umbach, R. (2024). Sextortion: Prevalence and correlates in 10 countries. *Computers in Human Behavior*, *158*. https://doi.org/10.1016/j.chb.2024.108298

Humelnicu, I. V. (2017). Sextortion – The Newest Online Threat. In *AGORA International Journal of Administration Sciences* (Issue 1). http://univagora.ro/jour/index.php/aijas

Justice, U. S. D. of. (2023). *Sextortion, Crowdsourcing, Enticement, and Coercion*. https://www.justice.gov/d9/2023-06/sextortion_crowdsourcing_enticement_and_coercion_2.pdf

Leukfeldt, R., & Holt, T. J. (2019). *The Human Factor of Cybercrime* (1st ed.). Routledge. https://doi.org/10.4324/9780429460593

Liggett, R. (2019). Exploring Online Sextortion. *Sexual Assault Report*, 58–63. https://www.civicresearchinstitute.com/online/PDF/FIPV-1104-04-Sextortion.pdf

Liska, A., & Gallo, T. (2017). *Ransomware: Defendendo-se de Extorsão Digital* (Novatec Editora Ltda., Ed.; 1st ed.). https://books.google.pt/books/about/Ransomware.html?id=CS5yDgAAQBAJ&redir_esc=y

Mouraz, J. L., & Milheiro, T. C. (2023). *Crimes Sexuais: Análise Substantiva e Processual* (Edições Almedina, Ed.; 4th ed.).

Nilsson, M. G., Tzani-Pepelasis, C., Ioannou, M., & Lester, D. (2019). Understanding the link between Sextortion and Suicide. *International Journal of Cyber Criminology*, *13*(1), 55–69. https://doi.org/10.5281/zenodo.3402357

Nunes, D. R. (2024). *Os Crimes Previstos na Lei do Cibercrime* (Gestlegal, Ed.; 2nd ed.).

Ollmann, G. (2007). *The Phishing Guide Understanding & Preventing Phishing Attacks*. https://pt.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems

O'Malley, R. L. (2023). Short-Term and Long-Term Impacts of Financial Sextortion on Victim's Mental Well-Being. *Journal of Interpersonal Violence*, *38*(13–14), 8563–8592. https://doi.org/10.1177/08862605231156416

O'Malley, R. L., & Holt, K. M. (2022). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. *Journal of Interpersonal Violence*, *37*(1–2). https://doi.org/10.1177/0886260520909186

O'Malley, R. L., & Smith, K. (2024). Suicidal Ideation Among Male Victim-Survivors of Financial Sextortion. *Victims and Offenders*, 1–22. https://doi.org/10.1080/15564886.2024.2379818

Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V., & Glavas, E. (2025). Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era. *Journal of Information Security*, *16*(01), 1–43. https://doi.org/10.4236/jis.2025.161001

Paulsen, C., & Byers, R. (2019). *Glossary of key information security terms*. https://doi.org/10.6028/NIST.IR.7298r3

Pereira, F., & Matos, M. (2015). Cyberstalking entre adolescentes: uma nova forma de assédio e perseguição? *Scielo*. https://doi.org/10.15309/15psd160207

Pereira, Pinho, M., & Madureira, E. J. (2023). *Referencial de educação para os media* (Ministério da Educação, Ed.).

Pethers, B., & Bello, A. (2023). Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks. *Future Internet*, *15*(1). https://doi.org/10.3390/fi15010029

Pires, C. (2022). *A Pornografia não Consentida no Código Penal Português* [Universidade Nova de Lisboa]. https://run.unl.pt/bitstream/10362/159044/1/Pires_2023.pdf

Polícia Judiciária. (2015, September 11). *Prevenção Criminal "Sextortion."* https://www.policiajudiciaria.pt/alerta-ao-cidadao-prevencao-criminal-sextortion/

Ramalho, J., & Ramalho, S. (2023). *Sextortion: caracterização dogmática e delimitação da imputação criminal em Portugal* (O. Sanguiné, Ed.). Revista Eletrônica de Direito Penal e Política Criminal –REDPPC. https://seer.ufrgs.br/index.php/redppc/issue/view/5019/1429

RASI, S. de S. I. (2017). *RASI*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABAAzMTE2AgAWydNBBAAAAA%3d%3d

RASI, S. de S. I. (2018). *RASI*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABAAzNzU0AwBUqv9nBAAAAA%3d%3d

RASI, S. de S. I. (2019). *RASI*. https://ssi.gov.pt/publicacoes/relatorio-anual-de-seguranca-interna/RASI_2019.pdf

RASI, S. de S. I. (2020). *RASI*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3d

RASI, S. de S. I. (2021). *RASI*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNLI0NgcAIUgtZwUAAAA%3d

RASI, S. de S. I. (2022). *RASI*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d

RASI, S. de S. I. (2023). *RASI*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDEyNgEApqka1wUAAAA%3d

RASI, S. de S. I. (2024). *RASI*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDExNwYAs4WfKQUAAAA%3d

Ray, A., & Henry, N. (2023, January 1). Sextortion: A Scoping Review. *Trauma, Violence, and Abuse*, *26*(1), 138–155. https://doi.org/10.1177/15248380241277271

Reis, S. S. (2024). *A criminalidade sexual online: o fenómeno do Catfishing* [ED Uminho]. https://www.uminho.pt/PT/ensino/apoioaaprendizagem/Paginas/repositorium.aspx

Ribeiro, M. da C. F. (2015). *Cibercrime e Prova Digital* [Instituto Superior Bissaya Barreto]. http://hdl.handle.net/10400.26/28946

Rodrigues, B. G. (2023). *O objeto de tutela da conduta típica de representação realista de menores: consequências para o regime da tentativa impossível* [Universidade de Coimbra].

https://estudogeral.uc.pt/retrieve/265836/Disserta%c3%a7%c3%a3o%20B%c3%a1rbara%20Rodrigues.pdf

Silva, J. M. A. da. (2016). *Imagem Cibercrime: O Crime de Pornografia Infantil na Internet* [Universidade de Coimbra]. https://estudogeral.uc.pt/bitstream/10316/34801/1/Cibercrime_o%20Crime%20de%20Pornografia%20Infantil%20na%20Internet.pdf

Tavares, T. K. da C. (2017). *O Fator Humano na Segurança de Informação nas Organizações* [Faculdade de Direito da Universidade de Lisboa]. https://fenix.tecnico.ulisboa.pt/cursos/msidc/dissertacao/1409728525631990

Tzani, C., Ioannou, M., Fletcher, R., & Williams, T. J. V. (2024). Psychological factors leading to sextortion: The role of personality, emotional factors and sexual needs in victimisation. *Computers in Human Behavior*, *159*. https://doi.org/10.1016/j.chb.2024.108323

Venâncio, P. D. (2022). *Lições do Direito do Cibercrime - E da Tutela Penal dos Dados Pessoais* (1st ed.). Editora D`ideias.

Venâncio, P. D. (2023). *Lei do Cibercrime. Anotada e Comentada*. Editora d'Ideias.

Venâncio, P. D. (2025). *Lições de Direito da Cibercrime - E da Tutela Penal dos Dados Pessoais* (Editora D'Ideias, Ed.; 2nd ed.). Editora D'Ideias.

Verdelho, Pedro., Bravo, R., Rocha, M. Lopes., & Veiga, Paula. (2003). *Leis do cibercrime* (1st ed.). Centro Atlântico.

Winnefeld Jr., J., Kirchhoff, C., & Upton, D. M. (2015, September). *Cybersecurity's Human Factor: Lessons from the Pentagon*. https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016, May). Sextortion: Cybersecurity, teenagers, and remote sexual assault 1. *The Brookings Institution*, 1–47. https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf

Wolak, J., & Finkelhor, D. (2016). *Sextortion: Findings from a survey 1,631victims*. https://respect.international/sextortion-findings-from-a-survey-of-1631-victims/

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, *62*(1), 72–79. https://doi.org/10.1016/j.jadohealth.2017.08.014