

Sextortion ou Cybersextortion; delimitação do termo ***Sextortion or Cybersextortion; delimitation of the term***

[10.29073/j2.v8i1.1118](#)

Recebido: 04 de março de 2026.

Aprovado: 01 de abril 2026.

Publicado: 04 de abril de 2026.

Autor/a: Paulo Lourenço , ESTG-IPP, Portugal, paulo.enes.lourenco@hotmail.com.

Resumo

Em Direito, e em Direito Penal em particular, os termos, designações e conceitos devem ser de tal forma específicos que só por si já sejam capazes de afastar interpretações dúbias. Desta forma este artigo tem como objetivo refletir sobre a utilização do termo *Cybersextortion* em detrimento do termo *Sextortion* de forma a tornar mais clara a utilização de cada um deles na identificação do fenómeno que se pretenda analisar.

Palavras-Chave: Cybercrime; *Cybersextortion*; Crime; *Sextortion*.

Abstract

In Law, and in Criminal Law in particular, terms, designations, and concepts must be so specific that they alone are capable of avoiding ambiguous interpretations. Therefore, this article aims to reflect on the use of the term *Cybersextortion* instead of *Sextortion* in order to clarify the use of each in identifying the phenomenon being analyzed.

Keywords: Crime; Cybercrime; *Cybersextortion*; *Sextortion*.

1. Introdução

Os termos utilizados para os crimes praticados com recurso a tecnologias de informação e comunicação (TIC) ou sobre estas, são precedidos do prefixo “*Ciber*”. Logo à partida o termo cybercrime deriva da palavra crime, mas, por ser praticado no ciberespaço ou por meio das TIC, ganhou o prefixo “*Ciber*”. Por isto, toda a doutrina diz que é cybercrime o crime praticado através das TIC ou contra estas. No entanto, todas as condutas criminais praticadas sem recurso às TIC, são designadas como crime, sem o prefixo “*Ciber*”.

Desta forma o vocábulo “*Cybersextortion*”, faz mais sentido do que “*Sextortion*”, uma vez que, à letra, esta última se refere apenas à extorsão sexual. Podendo ser praticada sem recurso às TIC e, dessa forma, induzir o leitor em erro. Já o termo *Cybersextortion*, não deixa margem para dúvidas. O prefixo “*Ciber*” coloca imediatamente esta prática no ciberespaço.

2. Metodologia

O presente estudo adota uma abordagem qualitativa, de natureza jurídico-dogmática, assente na análise crítica da doutrina nacional e internacional relevantes, bem como do enquadramento normativo aplicável ao fenómeno em estudo. Recorre-se, adicionalmente, a contributos da criminologia e dos estudos sobre cybercrime, com o objetivo de integrar diferentes perspetivas analíticas na delimitação conceptual proposta.

A metodologia utilizada baseia-se, assim, em três eixos fundamentais: (i) análise conceptual dos termos *Sextortion* e *Cybersextortion* na literatura científica; (ii) enquadramento jurídico-penal das condutas subjacentes à luz do ordenamento jurídico português; e (iii) problematização das implicações práticas decorrentes da adoção de diferentes opções terminológicas.

Não se trata, portanto, de um estudo empírico, mas antes de uma reflexão teórico-sistemática orientada para a clarificação conceptual e para a sua relevância na aplicação do Direito Penal.

3. Cibersextortion / Sextortion

Para Wolak e Finkelhor, o *Sextortion* é definido como fundamentalmente a ameaça de expor uma imagem sexual, real ou falsa, de modo a coagir a vítima a realizar algo ou por outros motivos, como vingança ou humilhação.

No contexto específico de envolvimento de menores, definem *Sextortion* como a ameaças de exposição pública para forçar a entrega de fotografias adicionais, à prática de atos sexuais ou outros favores. A essência reside na ameaça, independentemente de a exposição da imagem chegar a ocorrer (Wolak & Finkelhor, 2016).

Wittes e Popelin, por sua vez, descrevem *Sextortion* como uma forma de chantagem ou extorsão realizada através de uma rede informática, onde o item ou serviço exigido é a participação em um ato sexual. Caracterizam o crime como um “assalto remoto”, destacando que a conectividade global permite que um agressor ameace sexualmente alguém sem estar no mesmo país. Distinguem ainda o *Sextortion* de esquemas que visem apenas dinheiro, colocando a “coação remota de sexo” como o elemento inovador deste crime (Wittes et al., 2016).

Para Liggett, *Sextortion* é definido como a ameaça de distribuir imagens ou vídeos íntimos a menos que a vítima satisfaça uma exigência, focando-se no processo de obtenção do conteúdo, como *grooming*¹ ou *hacking*² (Liggett, 2019). Posteriormente, O'Malley e Smith enquadram o “*Sextortion* financeiro” como uma forma de abuso sexual baseado em imagens (IBSA), onde o agressor ameaça a divulgação pública dos conteúdos a menos que a vítima pague um resgate (O'Malley & Smith, 2024).

Igualmente em 2024, o grupo de trabalho de Tzani, classifica o *Sextortion* como um tipo de IBSA e violência sexual facilitada pela tecnologia (TFSV). Segundo os autores, o *Sextortion* ocorre quando um perpetrador ameaça distribuir material sexualmente explícito da vítima para a coagir a cumprir exigências como partilha de mais imagens, a prática de atos sexuais ou pagamentos financeiros (Tzani et al., 2024).

Desta forma, como já defendido em 2025³, o *Cibersextortion* é tido como o ato de constranger, coagir ou ameaçar de expor publicamente imagens, vídeos ou mensagens que visem devassar a vida sexual das pessoas, através de meios de comunicação social, *Internet* ou outras formas de divulgação pública, para obter contrapartidas ilegítimas (Lourenço, 2025). Ao contrário do que acontece com crimes praticados sem recurso às TIC ou onde estas são visadas, esta prática utiliza “meios de comunicação social ou *Internet*”.

Mesmo que se considere que “outros formas de divulgação pública” se refira a meios físico, flyers, panfletos ou cartazes, este elemento objetivo pode ser preenchido por, por exemplo, recurso às redes sociais. Onde até pode significar um impacto maior tanto no poder coercivo como nas consequências psicológicas nas vítimas deste tipo de ações (Wall, 2024). Observou-se ainda que o *Cibersextortion* pode decorrer de variadas motivações como sejam, as motivações económicas, sexuais, pessoais ou integradas.

De forma simples, entendeu-se enquadrar nas motivações económicas aquelas em que o agente age visando a obtenção de dinheiro. Nas motivações sexuais, aquelas em que o agente age com o objetivo de obter, por qualquer forma, gratificação sexual.

¹ O aliciamento online, também designado por *grooming* em inglês, pode ser definido como um processo de manipulação, geralmente aplicado em cenários em que as vítimas são crianças e/ou jovens menores. Em circunstâncias onde a vítima é maior de idade utilizam-se outras terminologias como *catfishing*, *romance scam*, entre outras. <https://www.internetsegura.pt/grooming> - Acedido em 31-03-2026.

² Hacking é o termo utilizado para descrever uma reprogramação de um sistema, programa ou dispositivo, de maneira não prevista e não autorizada pelo seu proprietário ou administrador. Com esta reprogramação o atacante pode obter acesso não autorizado a recursos e/ou ferramentas, anteriormente indisponíveis. <https://www.internetsegura.pt/Hacking> - Acedido em 31-03-2026.

³ Ver a dissertação de Mestrado “O Fenómeno do Sextortion – Perspetivas jurídica e Tecnológica” - disponível em: <https://recipp.ipp.pt/entities/publication/03cfd41c-afe5-4c43-96d6-fe134c27d70b> - acedido em 31-03-2026.

Quanto às motivações pessoais entendeu-se enquadrar aquelas em que ofensor e vítima se conhecem caso, por exemplo, da pornografia de vingança. Já as motivações integradas, enquadra aquelas que abarcam dois ou mais dos pontos anteriores ou daqueles com outros menos expressivos (Lourenço, 2025).

Apesar da diversidade de definições apresentadas, importa sublinhar que a maioria das abordagens analisadas não distingue de forma clara entre contextos digitais e não digitais, privilegiando antes a natureza da ameaça e a finalidade coerciva da conduta. Esta ausência de diferenciação revela uma limitação conceptual relevante quando se pretende transpor estas definições para o domínio jurídico-penal.

Com efeito, ao não autonomizar o elemento tecnológico, estas definições tendem a diluir especificidades próprias do ambiente digital, nomeadamente o efeito multiplicador da exposição pública, a persistência dos conteúdos e a dificuldade de controlo sobre a sua disseminação. Tais fatores não apenas agravam o impacto sobre a vítima, como também alteram significativamente o equilíbrio de poder entre o agente e a vítima.

Neste sentido, a distinção entre *Sextortion* e *Cibersextortion* não deve ser entendida como meramente terminológica, mas como uma diferenciação com relevância material, capaz de influenciara interpretação e aplicação das normas penais.

4. Delimitação dogmática do conceito

A delimitação dogmática do conceito de *Cibersextortion* exige a identificação dos elementos estruturais que o distinguem de figuras afins, nomeadamente da extorsão clássica, da coação e de formas de abuso sexual baseado em imagem.

Neste sentido é possível identificar três elementos essenciais: (i) a existência de um conteúdo de natureza sexual, real ou simulado; (ii) a ameaça de divulgação desse conteúdo como forma de pressão; e (iii) a finalidade de obtenção de uma vantagem ilegítima, que pode assumir natureza patrimonial, sexual ou outra.

O elemento distintivo central reside, contudo, na mediação tecnológica da conduta. Ao contrário da extorsão tradicional, em que a ameaça pode assumir múltiplas formas, no *Cibersextortion* a capacidade coerciva decorre, em larga medida, do potencial de difusão massiva e instantânea, proporcionado pelas tecnologias digitais.

Deste modo, o conceito afasta-se de uma mera adaptação terminológica, assumindo relevância dogmática autónoma, na medida em que a dimensão digital não constitui apenas um meio, mas um fator que reconfigura a própria natureza da ameaça ampliando exponencialmente os seus efeitos (Venâncio, 2023; Wall, 2024; Lourenço, 2025).

4.1. Enquadramento jurídico-penal

Do ponto de vista jurídico-penal, o *Cibersextortion* não corresponde, no ordenamento jurídico português, a um tipo legal autónomo, sendo antes enquadrado numa pluralidade de tipos penais já previstos, em função das circunstâncias concretas do caso (Lourenço, 2025). Entre os tipos penais potencialmente aplicáveis incluem-se, desde logo, os crimes de ameaça do artigo 153º, e de coação do artigo 154º, ambos do Código Penal (CP), sempre que a conduta vise constranger a vítima à adoção de determinado comportamento.

Em situações em que exista obtenção de vantagem patrimonial, poderá igualmente estar em causa o crime de extorsão do artigo 223º, do CP. Paralelamente, quando a conduta envolve o acesso ou obtenção ilícita de conteúdos íntimos, poderá verificar-se a prática de crimes previstos da Lei do Cibercrime, nomeadamente o acesso ilegítimo do artigo 6º.

Acresce ainda a eventual aplicação do crime da devassa da vida privada do artigo 193º do CP, particularmente nos casos em que ocorre efetiva divulgação dos conteúdos.

Esta dispersão normativa destaca a natureza fragmentada da resposta ao fenómeno, levantando questões relevantes ao nível do concurso de crimes, da delimitação da pena e da coerência do sistema jurídico-penal face a novas formas de criminalidade digital (Ramalho & Ramalho, 2023). Importa, portanto, salientar que esta



multiplicidade de enquadramentos legais levanta dificuldades ao nível do concurso de crimes, nomeadamente na distinção entre concurso efetivo e aparente, bem como na delimitação do tipo legal prevalente.

Acresce que a dispersão normativa pode gerar incerteza na prática judiciária, conduzindo a soluções divergentes em casos materialmente semelhantes. Tal realidade reforça a necessidade de uma interpretação sistemática e teleologicamente orientada, capaz de assegurar coerência na aplicação do Direito Penal como defendido pela doutrina.

4.2. Cibercrime

Como já referido, o conceito de cibercrime encontra-se associado à prática de ilícitos em ambiente digital. O desenvolvimento exponencial das tecnologias digitais, aliado à massificação da *Internet* enquanto tecnologia de informação e comunicação, tem produzido transformações estruturais profundas nas dinâmicas sociais contemporâneas (Wall, 2024). Estas inovações proporcionaram ganhos inequívocos ao nível da comunicação, do acesso à informação e da partilha de conteúdos (F. P. De Andrade et al., 2020).

Todavia, em paralelo, catalisaram o aparecimento de novas formas de criminalidade, frequentemente desmaterializadas, transnacionais e tecnologicamente sofisticadas (Ribeiro, 2015). Neste sentido, o cibercrime surge como um fenómeno jurídico-criminal dinâmico, cuja delimitação conceptual e enquadramento normativo se encontram em constante mutação, acompanhando a evolução das técnicas e dos meios utilizados no ciberespaço (Venâncio, 2023).

A definição unívoca de cibercrime tem sido dificultada pela heterogeneidade de fenómenos que se pretende abranger. Na doutrina portuguesa, esta diversidade tem sido sistematizada através da distinção entre cibercrime em sentido estrito e em sentido amplo. O conceito de cibercrime surge de forma abrangente para designar um conjunto de ilícitos praticados com recurso às TIC, englobando tanto crimes novos como crimes tradicionais adaptados ao ambiente digital (Verdelho et al., 2003). Cibercrime em sentido estrito, refere-se às condutas em que o elemento informático integra o próprio tipo legal ou constitui o bem jurídico protegido, como sucede com os ilícitos previstos na Lei nº 109/2009, de 15 de setembro.

Já os cibercrimes em sentido amplo, são aqueles que abrangem todas as condutas ilícitas em que as tecnologias digitais assumem um papel meramente instrumental, funcionando como meio para a prática de crimes tradicionais (Venâncio, 2023; Nunes, 2024). Este entendimento corresponde, no plano internacional, ao que frequentemente se designa como crimes facilitados por tecnologias digitais (Hedidi, 2023). Distinção realizada entre crimes ciberdependentes e crimes ciberpotenciados.

Os primeiros são aqueles cuja existência depende intrinsecamente do ambiente digital, como o *hacking*, os ataques de negação de serviço (*DoS*)⁴ ou a disseminação de *malware*⁵. Os segundos correspondem a crimes tradicionais cuja execução é ampliada ou facilitada pelas tecnologias, como a fraude *online*, o *phishing*⁶ ou o *Cibersextortion* (Leukfeldt & Holt, 2019).

⁴Um ataque de negação de serviço (DoS) inunda um servidor com tráfego, tornando um site ou recurso indisponível. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/dos-vs-ddos> - Acedido em 31-03-2026.

⁵*Malware* é um termo genérico para qualquer tipo de software malicioso concebido para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável. Os cibercriminosos normalmente utilizam-no para extrair dados que podem ser utilizados nas vítimas para obter ganhos financeiros. Esses dados podem variar entre dados financeiros, registos de assistência médica, correio eletrónico e palavras-passe. Disponível em: <https://www.mcafee.com/pt-pt/antivirus/malware.html> - Acedido em 31-03-2026.

⁶*Ophishing* 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. Disponível em: <https://www.internetsegura.pt/Phishing> - Acedido em: 31-03-2026.

Esta tipologia articula-se com a doutrina nacional de (Venâncio, 2023) e (Nunes, 2024), e reforça a ideia de que o cibercrime constitui um fenómeno plurifacetado, abrangendo tanto ilícitos tradicionais adaptados ao meio digital como novas formas e criminalidade emergentes (Hedidi, 2023).

Assim, importa sublinhar que o *Cibersextortion* constitui um exemplo paradigmático de interceção entre cibercrime em sentido amplo e em sentido estrito. Durante a sua execução, podem verificar-se simultaneamente condutas que se enquadram em crimes tradicionais, como ameaça artigo 153º ou a coação do artigo 154º ambos do Código Penal, mediados por tecnologias. E, ilícitos em que o elemento informático integra o tipo legal, como o acesso ilegítimo do artigo 6º da Lei 106/2009 de 15/09 (Lei do Cibercrime - LC) ou a devassa da vida privada por meios digitais artigo 193º do CP.

Esta sobreposição contribui para a complexidade do seu enquadramento jurídico e torna evidente a necessidade de respostas normativas e investigatórias mais articuladas (Venâncio, 2023):

5. Natureza do Ciberespaço

O ciberespaço, é simultaneamente um espaço informacional e uma rede global interconectada, contribui para a diluição das fronteiras físicas, colocando desafios significativos ao direito penal tradicional. A dimensão transnacional destas condutas exige, por conseguinte, mecanismos eficazes de cooperação internacional e esforços de harmonização legislativa (Deodato, 2024).

Contudo, persiste uma considerável heterogeneidade entre ordenamentos jurídicos, quer ao nível da tipificação penal, quer no que respeita aos regimes de obtenção e admissibilidade da prova digital, refletindo dificuldades já assinaladas na doutrina em 2009 (M. C. Andrade, 2009) e que, apesar do tempo decorrido, ainda não foram mitigadas.

Esta fragmentação normativa torna-se particularmente evidente em fenómenos híbridos como o *Cibersextortion*. Trata-se de uma realidade criminológica complexa que pode integrar múltiplos tipos penais, consoante as circunstâncias do caso em concreto, incluindo crimes previstos no Código Penal, na Lei do Cibercrime e em legislação e penal extravagante. Por exemplo, a Lei de Proteção de Dados Pessoais (Lei nº58/2019) que executa o Regulamento Geral sobre a Proteção de Dados (RGPD) de 2016. Tal pluralidade de enquadramentos jurídicos evidencia a dificuldade de subsunção destas condutas a categorias tradicionais e reforça a necessidade de abordagens integradas (Hedidi, 2023).

Acresce que a ausência de consenso conceptual a nível internacional gera constrangimentos operacionais relevantes. Desde logo, dificulta a produção de estatísticas comparáveis e compromete mecanismos de cooperação judiciária, como o reconhecimento mútuo de decisões ou a extradição de criminosos. Esta problemática é assim agravada pela natureza transnacional do *Cibersextortion*, em que os agentes operam frequentemente a partir de jurisdições distintas das da vítima (O'Malley & Smith, 2024)..

6. Problematização jurídica

A distinção entre *Sextortion* e *Cibersextortion* produz consequências práticas relevantes no plano jurídico, que ultrapassam a mera precisão conceptual. Desde logo, ao nível da qualificação jurídica dos factos. A utilização do termo *Cibersextortion* permite evidenciar a presença de elementos típicos associados ao cibercrime, facilitando a identificação de normas aplicáveis, nomeadamente as constantes da Lei do Cibercrime.

Em contraste, a utilização indistinta do termo *Sextortion* pode conduzir a uma subsunção excessivamente genérica a tipos legais tradicionais, desvalorizando a especificidade dos meios digitais.

Por outro lado, a distinção assume particular relevância em sede de investigação criminal. A identificação precoce da dimensão digital da conduta permite a adoção de mecanismos específicos de recolha de prova, como a preservação de dados informáticos ou a cooperação com plataformas digitais, cuja eficácia depende frequentemente da celeridade da intervenção.

Acresce ainda o impacto ao nível da cooperação internacional. A qualificação de determinados comportamentos como cibercrime pode facilitar a ativação de instrumentos jurídicos específicos, como convenções internacionais ou mecanismos de assistência mútua, particularmente relevantes em contextos transnacionais.

Por fim, a clareza terminológica contribui para uma melhor produção de dados estatísticos e para a definição de políticas mais eficazes, permitindo uma resposta mais ajustada à realidade do fenómeno. Não obstante, importa reconhecer que a adoção de uma terminologia mais precisa não resolve, por si, as dificuldades estruturais associadas ao fenómeno.

A eficácia da reposta jurídico-penal dependerá sempre da capacidade da adaptação dos mecanismos de investigação, da formação especializada dos operadores judiciais e da cooperação entre entidades públicas e privadas. Ainda assim, a clarificação conceptual constitui um primeiro passo para construção de um enquadramento jurídico mais coerente e eficaz.

7. Conclusões

A análise desenvolvida ao longo do presente artigo permite sustentar que a utilização indistinta dos termos *Sextortion* e *Cibersextortion* não é meramente uma questão semântica, mas antes um problema com implicações dogmáticas, jurídicas e operacionais no âmbito do Direito Penal.

Desde logo, verificou-se que o termo *Sextortion*, tal como definido na literatura internacional, apresentam uma natureza ampla e ambígua, podendo abranger condutas praticadas tanto em ambiente digital como fora dele. Esta amplitude conceptual, embora útil em contextos sociológicos, revela-se insuficiente quando transposta para o domínio jurídico-penal, onde a precisão terminológica constitui um requisito essencial.

Por outro lado, o termo *Cibersextortion* demonstra maior adequação técnico-jurídica, na medida em que incorpora expressamente o elemento digital como componente essencial da conduta. O prefixo “ciber” não apenas delimita o espaço de atuação, como também permite enquadrar o fenómeno no âmbito mais amplo do cibercrime, facilitando a sua integração sistemática nas categorias já consolidadas pela doutrina e legislação. Adicionalmente, conclui-se que o *Cibersextortion* constitui um fenómeno híbrido, situado na interseção entre cibercrimes em sentido estrito e em sentido amplo.

Tal característica traduz-se na coexistência de múltiplos tipos legais aplicáveis, desde crimes tradicionais mediados por tecnologias, como ameaça ou coação, até ilícitos especificamente informáticos, como o acesso ilegítimo ou a devassa da vida privada por meios digitais. Esta sobreposição gera dificuldades de enquadramento jurídico e exige uma abordagem interpretativa integrada.

Verificou-se ainda que a natureza transnacional do ciberespaço agrava os desafios associados à investigação e repressão deste fenómeno, nomeadamente ao nível da cooperação internacional, da recolha de prova digital e da harmonização legislativa. A ausência de consenso terminológico contribui, neste contexto, para a fragmentação das respostas jurídicas e para a ineficácia de mecanismos de cooperação.

Por fim, considera-se que a adoção do termo *Cibersextortion* no discurso jurídico e académico constitui um contributo relevante para a clarificação conceptual do fenómeno, promovendo maior rigor dogmático e facilitando a sua operacionalização prática. Tal opção terminológica revela-se particularmente importante num contexto em que a evolução tecnológica continua a desafiar as categorias tradicionais do Direito Penal.

Referências

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.

De Andrade, F. P., Fonseca, I., Silva, J. A., De Abreu, J. C., Jerónimo, P., Venâncio, P. D., & Freitas, P. M. (2020). *Relatório Cibersegurança em Portugal: Ética & direito*. <https://www.cnscs.gov.pt/docs/relatorio-eticaDireito2020-observatoriociberseguranca-cnscs.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* [Master's thesis, Universidade de Coimbra]. <https://hdl.handle.net/10316/118220>

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>

Leukfeldt, R., & Holt, T. J. (2019). *The human factor of cybercrime* (1st ed., Vol. 3). Routledge. <https://doi.org/10.4324/9780429460593>

Liggett, R. (2019). Exploring online sextortion. *Sexual Assault Report*, 22(11), 58–63. <https://www.civicsresearchinstitute.com/online/PDF/FIPV-1104-04-Sextortion.pdf>

Lourenço, P. (2025). *O fenómeno do sextortion: Perspetivas jurídica e tecnológica* [Master's thesis, Escola Superior de Tecnologia e Gestão, Politécnico do Porto]. <http://hdl.handle.net/10400.22/31195>

Nunes, D. R. (2024). *Os crimes previstos na lei do cibercrime* (2nd ed.; Gestlegal, Ed.).

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>

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>

Ribeiro, M. da C. F. (2015). *Cibercrime e prova digital* [Master's thesis, Instituto Superior Bissaya Barreto]. <http://hdl.handle.net/10400.26/28946>

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, 108323. <https://doi.org/10.1016/j.chb.2024.108323>

Venâncio, P. D. (2023). *Lei do cibercrime: Anotada e comentada*. Editora d'Ideias.

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

Wall, D. (2024). *Cibercrime: A transformação do crime na era da informação*.

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 of 1,631 victims*. <https://respect.international/sextortion-findings-from-a-survey-of-1631-victims/>

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.



Todo o conteúdo do *J² — Jornal Jurídico* é licenciado sob [Creative Commons](https://creativecommons.org/licenses/by/4.0/), a menos que especificado de outra forma e em conteúdo recuperado de outras fontes bibliográficas.