



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
PROJETO DE TRABALHO DE CURSO

ANÁLISE DA “SEXTORSÃO” FINANCEIRA NO AMBIENTE VIRTUAL

ORIENTANDA: MARIA ELVIRA BRANCO SANTANA
ORIENTADORA: PROF. DR. MARCELO BAREATO

GOIÂNIA-GO

2025

MARIA ELVIRA BRANCO SANTANA

ANÁLISE DA “SEXTORSÃO” FINANCEIRA NO AMBIENTE VIRTUAL

Projeto de Artigo Científico apresentado à disciplina de Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Profa. Orientador: Dr. Marcelo Bareato.

GOIÂNIA-GO

2025

MARIA ELVIRA BRANCO SANTANA

ANÁLISE DA “SEXTORSÃO” FINANCEIRA NO AMBIENTE VIRTUAL

Data da Defesa: _____ de _____ de _____

BANCA EXAMINADORA

Orientador(a): Prof. Dr. Marcelo Bareato

Nota

Examinador(a) Convidado(a): Prof.(a): Titulação e Nome Completo Nota

ANÁLISE DA “SEXTORSÃO” FINANCEIRA NO AMBIENTE VIRTUAL

ANALYSIS OF FINANCIAL SEXTORTION IN THE ONLINE ENVIROMENT

RESUMO

O artigo analisou o fenômeno denominado “*sextorsão*”, debruçando-se na vertente estritamente patrimonial, com o objetivo de compreender sua configuração jurídico-penal, além de implicações às vítimas e às instituições. Para esse intuito, empregou-se a pesquisa de natureza básica, método dedutivo e abordagem exploratória, além de predominância em revisão de literatura e estudo de casos. Inferiu-se que se trata de fenômeno carente de tipificação autônoma, assumindo, portanto, capacidade de adequação típica plural, cuja subsunção à norma penal incriminadora dependerá da finalidade pretendida pelo agente. Foi possível classificá-lo como crime cibernético impróprio. Apurou-se a transacionalidade do imbróglio, além do uso de criptomoedas para dificultar o rastreamento e a atuação especializada de associações criminosas. Concluiu-se, ao final, pela necessidade de aprimoramento investigativo, assim como suporte às vítimas e aperfeiçoamento normativo, com a finalidade de conferir maior segurança na interpretação da miscelânea jurídica correlata ao fenômeno analisado.

Palavras-chave: “*Sextorsão*” financeira; crime cibernético; associação criminosa. “Hacker”.

ABSTRACT

The article analyzed the phenomenon of “*sextortion*,” focusing on its strictly patrimonial dimension, with the aim of clarifying its criminal-law configuration and its implications for victims and institutions. It employed basic research, a deductive method, and an exploratory approach grounded in a literature review and case studies. The study found that the conduct lacked autonomous typification and exhibited plural normative adequacy, so its subsumption into incriminating provisions depended on the perpetrator’s purpose. It classified the conduct as an improper cybercrime and identified its transnational reach, the use of cryptocurrencies to hinder tracing, and the participation of specialized criminal associations. It concluded by underscoring the need to strengthen investigative capacities, expand victim support, and refine the legal framework to enhance certainty in interpreting the complex legal matrix surrounding the phenomenon.

Keywords: Financial sextorsion; cybercrime; criminal association; *Hacker*.

SUMÁRIO

INTRODUÇÃO	5
1 ALUSÃO HISTÓRICA À “SEXTORSÃO”	6
1.1 EVOLUÇÃO HISTÓRICA NO PLANO INTERNACIONAL	7
1.2 EVOLUÇÃO HISTÓRICA NO PLANO NACIONAL	9
1.3 CONSOLIDAÇÃO DO FENÔMENO	10
2 “SEXTORSÃO”: CONDUTA DE ADEQUAÇÃO TÍPICA PLURAL	10
2.1 A “SEXTORSÃO” ENQUANTO CRIME CIBERNÉTICO IMPRÓPRIO	13
2.1.1 Definição de crime cibernético	14
2.1.2 Crime cibernético próprio	15
2.1.3 Crime cibernético impróprio.....	16
3 O APERFEIÇOAMENTO DA “SEXTORSÃO” FINANCEIRA	17
3.1 CASO “GABRIEL PAZZINATTO LIPSKI”	18
3.2 AMBIENTE VIRTUAL: “LOCUS PERFECTUS”	20
CONCLUSÃO	22
REFERÊNCIAS	27

INTRODUÇÃO

A atualidade do tema repousa, principalmente, em torno da capacidade de transnacionalidade do fenômeno conhecido como “*sextorsão*”. Essa conduta detém aptidão para se subsumir a diversos preceitos primários do Código Penal Brasileiro. A norma penal incriminadora que incidirá no caso concreto dependerá do elemento subjetivo pretendido pelo agente infrator do bem jurídico penalmente relevante.

Em razão dos avanços exponenciais no nicho das tecnologias, a “*sextorsão*” com a finalidade de obtenção de vantagem econômica tornou transponível qualquer limitação geográfica. Tornou-se prescindível o consenso prévio ao compartilhamento dos conteúdos íntimos das vítimas com os seus algozes, eis que a utilização de “*malwares*”, dentre outros meios, viabilizou aos criminosos, não necessariamente “*hackers*”, o acesso aos conteúdos íntimos.

A relevância temática orbita ao redor das consequências potencialmente irreversíveis às vítimas, que, nem sempre, conseguirão obliterar os rastros desses conteúdos na internet a partir do momento que forem alocados na internet indexada e não indexada. Existem casos de repercussão nacional que resultaram no suicídio de algumas jovens, principalmente em decorrência do temor do “por vir” em suas vidas ao saberem dos compartilhamentos de seus conteúdos íntimos de forma não consentida na internet.

A “*sextorsão*”, após a fase da satisfação da lascívia própria ou de outrem; da vingança por não aceitação do término de um relacionamento íntimo de afeto; deu brecha à profissionalização da conduta àqueles que viram, no ambiente virtual, um caminho para obtenção de indevida vantagem econômica, valendo-se da violação à intimidade de algumas pessoas.

Ademais, destaque-se que a pesquisa realizada tem natureza básica e será orientada pelo método dedutivo. Quanto aos objetivos que são intrínsecos ao tema delimitado anteriormente, eles serão alcançados por intermédio da pesquisa de fim exploratório.

A pesquisa é preponderantemente bibliográfica, notadamente por meio do emprego da revisão de literatura, no que tange ao procedimento técnico. Para isso,

serão utilizadas, além de obras doutrinárias, legislações afetas à matéria proposta, além de outras produções científicas, assim como análise de casos concretos.

Destaque-se que a primeira seção do artigo científico analisará o contexto histórico da “*sextorsão*”, minudenciando a evolução global do fenômeno objeto de estudo, além de sua inserção e consolidação em âmbito nacional.

A segunda seção apresentará o conceito de “*sexortsão*” à luz da doutrina penalista pátria, além de expor a capacidade desse fenômeno em exsurgir como um crime cibernético, especificamente na modalidade imprópria, em razão de se tratar de um crime de forma livre, dependendo da finalidade almejada pelo agente infrator da norma penal incriminadora.

A terceira seção demonstrará o aperfeiçoamento da “*sextorsão*” financeira no ambiente virtual, por meio da análise de caso concreto no direito brasileiro, além de cotejar as suas similitudes com o “*leading case*” que ocorreu nos Estados Unidos da América (EUA), evidenciando a atualidade e relevância do tema eleito para esta análise.

Ademais, demonstrar-se-á que a “*sextorsão*” financeira tem se configurado como uma prática criminosa encampada pelas associações criminosas que passaram a se especializar nessa perpetração delituosa com a finalidade de obter indevidas vantagens econômicas. Observou-se que esses valores auferidos têm sido exigidos por meio de pagamento em criptomoedas para dificultar a localização dos autores dos crimes.

1 ALUSÃO HISTÓRICA À SEXTORSÃO

A evolução histórica macro/micro apresenta a passagem do abuso sexual ancorado em relações assimétricas de poder — formalizado pela Organização das Nações Unidas (ONU) e sistematizado pela “*International Association of Women Judges*”¹ (IAWJ) — para ecossistemas criminais digitais caracterizados por extorsão sexual mediada por tecnologia, ora com finalidade sexual, ora patrimonial.

¹ Em português significa associação internacional de mulheres juízas.

Essa trajetória exige atualização contínua de tipificações penais, protocolos investigativos e políticas públicas, com atenção particular aos riscos decorrentes da inteligência artificial (CONSELHO DA EUROPA, 2001; INTERPOL, 2024; EUROPOL, 2023; IC3/FBI, 2025).

1.1 EVOLUÇÃO HISTÓRICA NO PLANO INTERNACIONAL

Desde a década de 1990, foram relatados diversos casos de exploração e abuso sexual atribuídos a “*peacekeepers*”² e a trabalhadores humanitários, o que trouxe à tona a discussão sobre o manejo do poder em relações interpessoais assimétricas como recurso de obtenção de favores de naturezas sexuais (DEFÉIS, “*apud*” FAGANELLO, 2013, p. 197; SOPRANI, 2018, p. 01).

Em 2002, a Organização das Nações Unidas (ONU) abriu debate específico sobre o tema, culminando, em 2003, na edição do Boletim ST/SGB/2003/13 por Kofi Annan, então Secretário-Geral, que estabeleceu medidas especiais de proteção contra exploração e abuso sexual no âmbito do sistema da ONU (ONU, 2003, p. 01). Esse ato inseriu formalmente a problemática no cenário internacional e permitiu políticas de “*naming and shaming*”³ (ONU, 2003, p. 01).

A consolidação conceitual ganhou força em 2012 com a IAWJ, patrocinada por Bósnia e Herzegovina, Filipinas e Tanzânia, que difundiu estudo aprofundado vinculando a sextorsão às infrações penais de corrupção.

De acordo com a IAWJ, a prática exige dois componentes: (a) sexual e (b) corrupção (IAWJ, 2012, p. 9). O componente sexual consiste em pedido, explícito ou implícito, de participação em atividade sexual, não restrito à conjunção carnal, abrangendo toques físicos inadequados, exposição de partes íntimas, concessão de fotos sexuais, participação em atos sexuais por dispositivo informático, entre outros (IAWJ, 2012, p. 9).

Quando houver solicitação de vantagem distinta da sexual, o agente incorrerá em corrupção. Para fins deste trabalho, o termo é compreendido como

² É um termo em inglês que significa mantenedores da paz ou pacificadores. Eles fazem parte das Forças de manutenção da paz das Nações Unidas e podem incluir soldados, oficiais de polícia e pessoal civil. Eles também são conhecidos como capacetes azuis ou boinas azuis.

³ Nomear e envergonhar significa dizer publicamente que uma pessoa, grupo ou empresa fez algo errado. Trata-se de uma prática utilizada para desencorajar alguns tipos de atividades, as quais podem ocorrer no ambiente doméstico ou internacional. Ela é frequentemente usada para denunciar violações aos direitos humanos.

violação à integridade moral associada ao abuso de posição de poder. O componente corrupção deve conter três atributos: (a) abuso de autoridade; (b) troca de favores; (c) emprego de coerção psicológica em detrimento da força física (IAWJ, 2012, p. 9-11). Note-se que “abuso de autoridade” aqui tem acepção distinta da Lei Federal n.º 13.869/2019, não se limitando aos sujeitos por ela tipificados (BRASIL, 2019). A IAWJ (2012, p. 9) sintetiza que o sujeito ativo deve ocupar posição de autoridade e abusar dessa autoridade, exigindo ou aceitando favor sexual em troca do exercício do poder que lhe foi confiado (tradução nossa).

À luz dessa moldura, diversos perfis podem figurar como autores: agente público que condiciona ato de ofício; empregador que ameaça demitir ou negar promoção; docente que vincula aprovação à concessão de favor sexual (IAWJ, 2012, p. 10; SYDOW; CASTRO, 2017, p. 04). Em termos de consumação, a sextorsão clássica se perfaz no momento da exigência ou solicitação, ainda que implícita; o eventual atendimento da pretensão denota mero exaurimento (SYDOW; CASTRO, 2017, p. 04-05).

A partir de 2010, com a expansão de redes sociais e computação em nuvem, observa-se inflexão tecnológica do fenômeno: investigações do “*Federal Bureau of Investigation*” documentaram o uso de “*malware*” e controle remoto de “*webcams*” e microfones para coagir vítimas — como no emblemático caso Luis Mijangos — popularizando, por conseguinte, a leitura de sextorsão cibernética (FBI, 2010; FBI, 2011). Nesse contexto, o termo passou a abranger a ameaça de divulgar conteúdo íntimo para obter novos atos sexuais ou pagamento em dinheiro (FBI, 2010; FBI, 2011).

Agora, sob o prisma normativo-internacional, embora não utilizem a palavra “*sextorsão*”, dois instrumentos do Conselho da Europa tornaram-se centrais para a investigação, assim como para a cooperação: a Convenção de Budapeste sobre o Cibercrime (2001), que disciplina poderes processuais e cooperação para evidências eletrônicas, e a Convenção de Lanzarote (2007), que trata da proteção de crianças contra exploração e abuso sexual, inclusive online (CONSELHO DA EUROPA, 2001; CONSELHO DA EUROPA, 2007).

1.2 EVOLUÇÃO HISTÓRICA NO PLANO NACIONAL

Após os marcos internacionais (ONU/IAWJ) e a inflexão tecnológica global (FBI/IOCTA/INTERPOL), o recorte desloca-se para a experiência nacional.

A “*sextorsão*”, no ordenamento jurídico brasileiro, não pode ser considerada um “*nomen iuris*”, em decorrência da ausência de definição legal. Porém, é reputada como um neologismo oriundo da fusão das palavras sexo e extorsão.

Destaque-se que o termo anteriormente citado ganhou repercussão nacional quando o doutrinador e Promotor de Justiça do Ministério Público do Estado de São Paulo (MPSP), Rogério Sanches Cunha (2017, on-line), em publicação veiculada na plataforma de compartilhamento de vídeos denominada “*Youtube*”, o definiu como uma prática suscetível de adequação típica plural.

Na tentativa de definir “*sextorsão*” sob a ótica contemporânea, a SaferNet Brasil (2018, on-line) aduz que a prática retromencionada se trata de “ameaça de se divulgar imagens íntimas para forçar alguém a fazer algo – ou por vingança, ou humilhação ou para extorsão financeira. É uma forma de violência grave, que pode levar a consequências extremas como o suicídio”.

Embora não exista, atualmente, norma penal incriminadora, trazendo todo os elementos do preceito primário e secundário de “*sextorsão*”, os operadores do direito, em nome do Estado, único detentor do “*ius puniendi*” [direito de punir], por meio de minudente exegese, lograram meios de viabilizar o exercício da ação penal sem configurar violação ao princípio da reserva legal [legalidade e anterioridade].

No Brasil, entretanto, a resposta normativa ganhou densidade com a Lei Federal n.º 13.718/2018, que introduziu o art. 218-C do Código Penal Brasileiro e criminalizou a divulgação não consensual de cena de sexo, nudez ou pornografia, frequentemente associada a desfechos de sextorsão (BRASIL, 2018). Além do mais, medidas correlatas e ajustes investigativos recentes ampliaram a capacidade de enfrentamento quando a finalidade é patrimonial (BRASIL, 2018).

Saliente-se que a engendração de esforços para colmatar a lacuna existente no ordenamento jurídico brasileiro, especificamente no que tange à ausência de tipo penal prevendo o crime de “*sextorsão*”, além de relevante à salvaguarda de bens jurídicos penalmente importantes, também permanece atual, principalmente porque a prática da referida conduta tem condão de ocasionar lesividade exponencial à

vítima quando praticada em ambiente virtual, cuja capacidade de propagação das informações ultrapassa as barreiras geográficas é acompanhada da capacidade de atemporalidade.

1.3 CONSOLIDAÇÃO DO FENÔMENO

A década de 2020 consolidou a “*financial sextortion*”, modalidade em que o objetivo é exclusivamente econômico. Relatórios do IC3/FBI registram crescimento expressivo das perdas financeiras, com adolescentes e jovens adultos — especialmente homens — entre os principais alvos (IC3/FBI, 2025).

Oportunamente, também urge dizer que o IOCTA 2023 da Europol descreve campanhas transnacionais de engenharia social digital (EUROPOL, 2023). A Interpol destaca a emergência de mídias sintéticas (“*deepfakes*”⁴) como vetor de chantagem, com material sexual fabricado a partir de imagens públicas (INTERPOL, 2024).

No campo científico e da saúde pública, inquéritos e revisões sistemáticas indicam prevalência não considerada desprezível de vitimização por sextorsão entre adolescentes (≈5% em amostras norte-americanas), que é associada a depressão, ansiedade, além da ideação suicida (PATCHIN; HINDUJA, 2020; RAY et al., 2024).

Em contraponto a isso, organismos como a Organização Mundial da Saúde e o UNICEF recomendam respostas multissetoriais, combinando educação digital, apoio psicossocial e cooperação entre plataformas e autoridades (OMS, 2022; UNICEF, 2021).

2 SEXTORSÃO: CONDOTA DE ADEQUAÇÃO TÍPICA PLURAL

Destaque-se que uma das razões do pouco enfrentamento da “*sextorsão*” no Brasil advém do fato de que o direito penal brasileiro adota o sistema garantista, em decorrência do princípio da legalidade, previsto no art. 1º do Código Penal (BRASIL,

⁴ Deepfakes são conteúdos (vídeos, áudios ou imagens) falsos e extremamente realistas, criados com o uso de inteligência artificial (IA). A palavra “deepfake” é uma junção dos termos em inglês deep learning (“aprendizagem profunda”) e fake (“falsificação”). Eles utilizam algoritmos de deep learning para sobrepor ou sintetizar o rosto, a voz e as expressões de uma pessoa em um conteúdo já existente. O resultado é uma manipulação tão convincente que se torna muito difícil distinguir o que é real do que é fabricado.

1940), e art. 5º, inciso XXXIX, da Constituição da República Federativa do Brasil (BRASIL, 1988), servindo como limitador ao poder punitivo estatal.

O referido princípio compõe o gênero da reserva legal que, além de abarcar a legalidade, também encampa o princípio da anterioridade, garantindo que nenhuma conduta será considerada crime e passível de punição sem existência prévia de uma norma penal incriminadora (CAPEZ, 2015, p. 54).

Aliado ao óbice anteriormente consignado, existe também a vedação ao uso da analogia em normas penais incriminadoras, sob pena de violação ao princípio da reserva legal, sendo possível a sua aplicação somente às normas justificantes e as permissivas (CAPEZ, 2015, p. 53).

No entanto, esses axiomas não podem inviabilizar o dever do juiz de dizer o direito, sob o argumento de que a “*sextorsão*” não tem previsão legal. Afinal, existem nesses casos nítida lesão a bens jurídicos penalmente relevantes. Por isso, revela-se pertinente e necessária a minuciosa análise do verbo praticado pelo sujeito ativo, além da finalidade da conduta, possibilitando a identificação do bem jurídico violado e a subsunção da conduta às elementares de alguma norma penal incriminadora.

Destaque-se que o art. 2º da Lei de introdução às normas de Direito Brasileiro (Decreto-Lei n.º 4.657/1942), dispõe que “quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito”. Esses instrumentos colocados à disposição do juiz são conhecidos como meios de integração do direito, compreendendo tanto a interpretação analógica e extensiva.

A interpretação analógica possui o escopo de extrair o sentido da norma incriminadora através dos elementos fornecidos por ela. Para afastar dúvida quanto ao seu entendimento, imagine a fraude bancária, sobretudo aquela prevista no art. 171, “*caput*”, do Código Penal Brasileiro. O termo “qualquer outro meio fraudulento” do mencionado dispositivo é um exemplo clássico. Nesta modalidade interpretativa, existe norma regulando a hipótese expressamente, porém de forma genérica, o que torna essencial o recurso à via interpretativa (CAPEZ, 2015, p. 52).

Acerca da interpretação extensiva, que objetiva o verdadeiro anelo da norma, no caso a incriminadora, incumbe ao intérprete, ao confrontar o caso com a norma cabível, compreender o alcance desta. Para facilitar a compreensão, basta imaginar o clássico exemplo do crime previsto no art. 150 do Código Penal Brasileiro

[violação de domicílio], cuja redação tem a expressão “casa”, a qual não pode ser interpretada em seu sentido literal, afinal até a boleia de um caminhoneiro pode ser objeto deste crime.

Há que se destacar que essa atividade de subsunção da “*sextorsão*” a uma norma penal incriminadora se reveste de ainda mais laboriosidade quando praticada no ambiente virtual. Afinal, embora em sua definição legal não se trate de um crime cibernético próprio, pode ser definida como crime cibernético impróprio, partindo-se da premissa de que é um crime de forma livre, dependendo da norma incriminadora em que referida conduta se subsumir, e, por isso, também poderá ser praticado por meio de dispositivos eletrônicos, informáticos e no ambiente virtual.

Diz-se que a “*sextorsão*” é conduta de adequação típica plural (CUNHA, 2017, on-line) porque está condicionada à finalidade pretendida pelo agente, podendo se subsumir em vários preceitos primários da parte especial do Código Penal Brasileiro.

À vista disso, aduz-se que “*sextorsão*” consiste em constranger alguém, mediante ameaça de divulgação de conteúdo íntimo, adquirido por meios lícitos ou não, consensual ou não, de forma consciente e voluntária, dirigida à finalidade de: I – fazer com que a vítima pratique, não pratique ou tolere que se pratique ato que a lei não obriga ou proíbe [art. 146]; II – incutir temor ou receio na vítima [ameaça – art. 147]; III – obter indevida vantagem econômica [extorsão – art. 158]; IV – satisfazer o desejo ou a lascívia de natureza sexual [estupro virtual – art. 213]; e V – obter vantagem ou favorecimento sexual, prevalecendo-se o agente da condição de superior hierárquico ou ascendência inerente ao exercício de emprego, cargo ou função [art. 216-A]; VI – divulgar, por qualquer meio, inclusive eletrônico ou rede social), fotografia, vídeo ou outro registro que contenha cena de estupro, de estupro de vulnerável, de sexo, nudez ou pornografia, sem o consentimento da vítima [art. 218-C].

A “*sextorsão*” ocorrerá quando uma pessoa começa a constranger outra, por meio de grave ameaça consistente na promessa de tornar pública uma foto ou vídeo de natureza erótica, sexual ou pornográfica em que ela protagoniza, caso as suas exigências feitas não sejam atendidas (CUNHA, 2017, p. 206; FERNANDEZ, 2013, p. 84). Isso demonstra como se dá o uso do poder situacional sobre alguém. Vale lembrar que o material pode ter sido obtido de forma consensual ou não, e todo caso

concreto deve ser analisado para escoreita subsunção da conduta a uma norma penal incriminadora previamente existente.

2.1 A SEXTORSÃO ENQUANTO CRIME CIBERNÉTICO IMPRÓPRIO

Segundo matéria trazida no sítio do eletrônico do jornal “Correio Braziliense” (GIUSTI; TORRES; 2024, on-line), dados publicados do site denominado “*PornHub*” demonstrou que o Brasil ocupou, no ano de 2022, o 10º lugar no ranking global de consumo de pornografia, com 39% (trinte e nove por cento) de usuárias mulheres e 61% (sessenta e um por cento) de usuários homens, segundo dados do “*PornHub*”. A maioria dos consumidores está na faixa etária de 18 a 44 anos.

Aliado ao dado citado alhures, aduz-se que a “*SaferNet*” Brasil, associação civil de direito privado, com atuação nacional, cujo escopo é promover a defesa dos Direitos Humanos na internet, informa que:

Em 19 anos, a SaferNet recebeu e processou 4.936.655 denúncias anônimas envolvendo 1.175.339 páginas (URLs) distintas (das quais 818.393 foram removidas) escritas em 9 idiomas e hospedadas em 110.414 domínios diferentes, de 386 diferentes TLDs e conectados à Internet através de 122.425 números IPs distintos, atribuídos para 148 países em 6 continentes. Ajudou 39.517 pessoas em 27 unidades da federação e foram atendidos 10.077 crianças e adolescentes, 2.725 pais e educadores, 5.281 jovens e 21.434 outros adultos em seu canal de ajuda e orientação (SAFERNET, 2025, on-line).

Os dois primeiros casos que repercutiram na mídia brasileira ocorreram no ano de 2012, quando duas adolescentes domiciliadas no Estado do Rio Grande do Sul (RS) e Piauí (PI), cometeram suicídio depois de terem ciência de que fotos íntimas e imagens de ato sexual do qual participava foram publicados na “*internet*” e no aplicativo de mensagens denominado “*WhatsApp*”, respectivamente (ILHA, 2013, on-line).

Diante dos dados apresentados, verifica-se que as consequências na vida de quem é alvo de “*sextorsão*” podem ser devastadoras, sobretudo quando a prática se propaga na rede mundial de computadores. Afinal, a sua aptidão de romper as barreiras geográficas e temporais pode causar danos irreversíveis à vítima.

O “*sexting*”⁵ é outro comportamento que foi potencializado pelas facilidades oriundas do ciberespaço. Aqui, os interlocutores, geralmente, dispõem de forma consensual dos seus direitos constitucionais à intimidade, privacidade e imagem, acreditando que eles não serão violados. Entretanto, isso dá origem a um poder situacional que poderá ser utilizado para a perpetração da sextorsão, conforme visto nos casos concretos citados alhures.

No entanto, é necessário esclarecer que o “*sexting*” nem sempre é elemento antecedente para a ocorrência da “*sextorsão*”. Na ausência dele, o poder situacional surgirá de outras maneiras e as vítimas, geralmente, são escolhidas aleatoriamente, como é o caso “*Luis Mijangos*”, em que o FBI atuou em 2010, cuja utilização de “*malware*” e controle remoto de “*webcams*” e microfones possibilitava-lhe coagir as vítimas (FBI, 2010; FBI, 2011).

Naquela ocasião, a expressão “*sextortion*” foi utilizada oficialmente pelo FBI para definir a conduta que havia sido praticada pelo “*hacker*” anteriormente citado. Ele obteve acesso às conversas que suas vítimas tinham com terceiros, bem como às “*webcams*” para observá-las em tempo real e aos microfones. Posteriormente, Luis Mijangos as chantageava a fim de que enviassem fotos nuas, do contrário iria expor a intimidade delas (SYDOW; CASTRO, 2017, p. 08). Este caso é relevante por apresentar a prática de “*sextorsão*” como um crime cibernético, especificamente na espécie imprópria.

2.1.1 Definição de crime cibernético

Oportunamente, consigne-se que o crime cibernético, conhecido como crime virtual e cibercrime, pode ser compreendido como “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material” (ROQUE, 2007, p. 25). Referida acepção conduz à conclusão de que os dispositivos eletrônicos também podem ser utilizados como meio para a prática de crimes previstos em lei.

5 Expressão estrangeira referente à troca de mensagens que contenham conteúdo erótico ou sexual.

2.1.2 Crime cibernético próprio

O crime cibernético pode ser classificado como próprio ou impróprio. Serão próprios aqueles praticados contra o computador, ou seja, que atacam os dados e o sistema informático. Sua execução e consumação acontecem no próprio ambiente virtual.

Além dos crimes cibernéticos próprios introduzidos ao ordenamento jurídico pátrio pela Lei Federal nº 12.737/2012, comumente conhecida como Lei Carolina Dieckmann – que tipificou condutas como invasão de dispositivo informático [art. 154-A do Código Penal] e alterou os arts. 266 [interrupção de serviço telemático ou de informação de utilidade pública e 298 [falsificação de documento particular com uso de dados informáticos] – existem outros cuja estrutura típica exige um sistema computacional como objeto material ou meio essencial à sua prática e consumação e serão apresentados a seguir.

O art. 154-A do Código Penal – invasão de dispositivo informático, previsto pela Lei nº 12.737/2012, consiste em invadir dispositivo informático alheio ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, com o fim de obter, adulterar ou destruir dados ou informações.

O art. 154-B do Código Penal – divulgação, comercialização ou transmissão de dados obtidos por invasão, também introduzido ao ordenamento jurídico pela lei Carolina Dieckmann, trata da conduta de quem produz, oferece, distribui, vende ou divulga dados obtidos mediante a prática do crime do art. 154-A citado alhures.

O art. 266, § 1º, do Código Penal – interrupção ou perturbação de serviço telegráfico, informático, telemático ou de informação de utilidade pública, modificado pela Lei Federal nº 12.737/2012, é aplicado a ataques cibernéticos como “DdoS”⁶, que prejudicam a prestação de serviços essenciais.

O art. 298, parágrafo único, do Código Penal – falsificação de cartão ou documento eletrônico, também alterado pela Lei Federal nº 12.737/2012, estende o conceito de documento particular a cartão de crédito ou débito e qualquer outro documento eletrônico que possa servir como prova de direito, criando espaço para o combate a falsificações digitais.

⁶ Significa “Distributed Denial of Service” ou “Negação de Serviço Distribuída”. É um tipo de ataque cibernético que visa sobrecarregar um servidor, serviço ou rede com um grande volume de tráfego malicioso proveniente de diversas fontes, tornando-o inacessível para os usuários legítimos.

O art. 171-A do Código Penal – fraude eletrônica, incluído pela Lei Federal nº 14.155/2021, criminaliza em seu preceito primário fraudes patrimoniais cometidas por meio de dispositivos eletrônicos ou redes sociais, como a clonagem de contas de “WhatsApp”, sites falsos, ou manipulação digital com obtenção indevida de valores.

Em que pese não tipique crimes diretamente, a Lei Federal nº 12.965/2014 – Marco Civil da Internet, em seus artigos 11 e 13, § 3º, reforça a responsabilidade penal por infrações penais perpetradas no ambiente digital, servindo de base para a persecução penal de crimes cibernéticos próprios.

Por seu turno, a Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados – LGPD, em seu art. 52, inciso IV, não obstante também possua natureza eminentemente administrativa, a violação intencional de dados pessoais armazenados em sistemas computacionais pode configurar condutas penais quando combinada com os artigos 154-A e 154-B, ambos do Código Penal.

A Lei Federal nº 14.155/2021 – crimes contra o patrimônio com uso de meios eletrônicos, além de ter introduzido o art. 171-A, também alterou os crimes dos arts. 155 e 171 do Código Penal, para prever formas qualificadas por meio da utilização de dispositivos eletrônicos, informáticos ou similares, em conexão com a internet, ampliando as possibilidades de repressão a fraudes digitais.

Portanto, os crimes cibernéticos próprios no Brasil não se restringem à Lei Federal nº 12.737/2012 – lei Carolina Dieckmann, abrangendo outros tipos penais que exigem, como elemento estrutural do tipo penal, o uso de sistemas informáticos ou meios digitais, com destaque especial para os crimes contra o patrimônio e a fé pública cometidos por meio eletrônico, de acordo com as modernizações legislativas promovidas até 2021.

2.1.3 Crime cibernético impróprio

Os crimes cibernéticos impróprios são aqueles em que o agente se vale dos meios eletrônicos para a sua prática. A utilização desses recursos tecnológicos serve apenas como meio de execução para se atingir determinado resultado em delitos reputados como tradicionais. Portanto, os meios digitais são meros instrumentos à prática do crime, e não o objeto material da infração penal.

À vista disso, destaque-se que a infração penal pode ser perpetrada fora do ambiente virtual, sendo o meio informático uma ferramenta de execução, e não a finalidade do crime. Os diversos bens jurídicos violados são todos aqueles previstos na legislação penal pátria.

A “*sextorsão*” pode ser reputada um crime cibernético impróprio, ou seja, o dispositivo informático é o meio empregado para a perpetração de algum crime ou contravenção penal (BARRETO; BRASIL, 2016, p. 18).

A “*sextorsão*”, de acordo com conceito o jurídico-doutrinário apresentado por Rogério Sanches Cunha (2022, p. 594), não é um tipo penal autônomo, mas uma forma de execução de diversos preceitos primários penais considerados tradicionais, mediante utilização de tecnologias digitais.

O meio informático somente opera como instrumento de coação, dominação psicológica e violação a direitos fundamentais, sendo enquadrado como cibernético impróprio. Por isso, a atuação judicial deve, inexoravelmente, perquirir a finalidade do agente e a vulnerabilidade digital da vítima, a fim de subsumir a conduta à norma penal incriminadora que se revele adequada e proporcional com o contexto fático do caso concreto.

3 O APERFEIÇOAMENTO DA “SEXTORSÃO” FINANCEIRA

Considerando o panorama histórico do fenômeno denominado “*sextorsão*” citado na seção 1, aliado aos pertinentes conceito e alusões consignados na seção 2, pode-se afirmar que a conduta ilícita possui aptidão para se subsumir em diversos preceitos primários do Código Penal Brasileiro, dependendo da finalidade pretendida pelo agente.

Nessa linha de intelecção, constata-se que o uso de ferramentas atreladas ao ambiente virtual aumenta a vulnerabilidade da vítima, além de expô-la a riscos de ordem irreversível, considerando a capacidade de propagação das [des]informações que nem sempre serão totalmente acobertadas pelo direito ao esquecimento. Afinal, na era digital, conteúdo publicados, principalmente de natureza sexual, ainda que de forma não consentida, deixam os vestígios que reverberam em todos os contextos sociais das vítimas.

A fim de exemplificar essa inferência, basta reputar os casos de “*sextorsão financeira*” citados neste artigo, cujos desfechos para as vítimas foi o suicídio, diante de tamanho temor quanto às consequências oriundas dessa prática ou da “*revenge porn*” – pornografia de vingança.

A persecução penal, exteriorizada pela jurisprudência pátria, apresenta esse fenômeno denominado “*sextorsão financeira*”, comprovando, mais uma vez que toda história é cíclica, repetindo-se em diferentes épocas, territórios, apenas exurgindo entre personagens distintos.

A “*sextorsão financeira*” prescinde de “*sexting*” ou “*revenge porn*”, ocorrendo, inclusive, por meio de obtenção não consensual de conteúdos de natureza íntima, geralmente de cunho erótico/sexual, que são obtidos no ambiente virtual.

A seguir, apresentar-se-á caso concreto havido em solo pátrio que corrobora essa linha de inteligência, havendo, inclusive, algumas semelhanças com o caso Luis Mijangos, que popularizou sextorsão cibernética, notadamente no ano de 2010, nos Estados Unidos, atraindo a atenção do FBI.

3.1 CASO “GABRIEL PAZZINATTO LIPSKI”

O Ministério Público do Estado de Goiás, no início do ano de 2024, ofereceu denúncia em desfavor de Gabriel Pazzinatto Lipski, programador, imputando-lhe a prática do crime de extorsão, na modalidade de crime continuado, considerando o fato de que nos dias e horários citados na denúncia, enviou mensagens às vítimas em suas caixas de e-mail pessoal, afirmando ter “*hackeado*” e acessado celulares e respectivos computadores, de forma que, por meio dessas invasões, obteve acesso aos conteúdos de natureza íntima delas.

Consta, ainda, que as vítimas foram constrangidas, mediante grave ameaça, a fornecer dinheiro para que as referidas imagens não fossem divulgadas em sites pornográficos, bem como a amigos e familiares das vítimas.

A fim de perquirir eventual impunidade, o acusado apresentou “*link*” para que as vítimas efetuassem pagamento por meio de “*Bitcoin*” – criptomoeda, na tentativa de não ser rastreado.

A seguir, convém destacar afirmações do delegado que atuou no Inquérito Policial (IP) n.º 86/2023, que redundou no indiciamento do acusado, realizadas durante audiência de instrução e julgamento, “*ipsis litteris*”:

[...] que veio um relatório do Ministério da Justiça informando que o mesmo investigado fez várias vítimas no país inteiro e aqui em Goiás foram quinze vítimas; que então eu instaurei o inquérito e dividi por regiões, porque são várias vítimas; que de Aparecida de Goiânia são quatro, três vítimas de Goiânia e outras vítimas do interior; que estou instaurando os inquéritos por serem crimes conexos e com base nos domicílios das vítimas; que diante disso o relatório do Ministério da Justiça comunicou que também tinha uma investigação no Rio Grande do Sul; que pedi o compartilhamento para o delegado do Rio Grande do Sul e o juiz também autorizou o compartilhamento, compartilhou os relatórios que é o mesmo fato; que ele estava fazendo vítimas lá do Rio Grande do Sul que era do Sextouch, que então o Ministério da Justiça fez o rastreio de criptomoedas e as carteiras que guardaram essas criptomoedas e que tudo indicava que era do Gabriel Pazzinato,; que a identificação dele foi por meio do rastreamento das criptomoedas; que eu trabalho na delegacia de crimes cibernéticos; que quem fez o rastreio de criptomoedas foi o Ministério da Justiça, que compartilhou o relatório conosco; que a gente fez a leitura desse relatório e o agente de polícia Melquisedeque, que é técnico nessa área, em rastreio de criptomoedas, fez a tradução desse relatório do Ministério da Justiça para nós; que essa tradução é no sentido de facilitar a linguagem; que ele esclareceu a linguagem, que alguns e-mail's coincidiam, mas ele usava vários, principalmente email's que eram criptografados, “próton” e-mail que é criptografia de ponta a ponta, que a vinculação dele deu tanto pelos IP's que manuseava as carteiras digitais de criptomoedas no Mercado de bitcoins e na Foxpit, quanto também nos endereços de criptomoedas, que a vinculação foi por isso, que os ips que ele manuseava deu os dados cadastrais dele que ele manuseava essa carteira digital e também os rastreios de criptomoedas, que foram utilizadas nessa investigação ferramentas abertas porque o blockchain é público “wallet explorer” e faz a decodificação das transações que são realizadas pelas criptomoedas, por exemplo, se a vítima deposita dinheiro em criptomoedas daí gera uma transação um código criptografado e que por meio desses rastreios você vai sabendo em qual carteira digital que caiu aquela criptomoeda; que qualquer pessoa consegue consultar essa ferramenta, que ela é aberta, que todos os e-mail's foram relacionados a ele por meio do endereço criptoativo, todos criptoativos davam na pessoa do Gabriel, que ele usava protonmail que é a criptografia de ponta a ponta; que não tem como a gente descobrir é igual whatsapp; que todos os endereços criptoativos coincidiam; que ele mandava e eram os mesmos; que a identificação partiu do e-mail do blockchain e lá que eles chegaram ao autor; que não foi pelo e-mail em si porque eles são protonmails; que as vítimas disseram que foram constrangidas, mas que não efetuaram o pagamento; que ele foi o beneficiário direto e no relatório da polícia civil demonstra que ele tem conhecimentos técnicos em informática, e ele estava fazendo estudos de invasão de contas e dispositivos; que eu até coloco no meu relatório que é uma situação específica que ele tá tipo discutindo com outro hacker como que faz essas invasões de contas; que então ele tem esse conhecimento técnico o Gabriel, que foi compartilhada muita informação do Rio Grande do Sul porque se trata da mesma situação fática; que aqui em Goiás ele foi condenado se eu não me engano ele pegou 14 anos ou 12 anos; que ele fornecia o endereço do criptoativo e deu nele; que é crime formal o pagamento é mero exaurimento; que a gente identificou ele pelo endereço

de criptoativo não foi pelo pagamento; que foram mais de mil vítimas, só em Goiás foram mais de quinze e sempre era o mesmo endereço do Gabriel de criptoativos, se ele não poderia tá envolvido diretamente no e-mail da extorsão ele tem participação, e pela decodificação da quantidade de dinheiro que ele recebeu foi uma gama de dinheiro muito alta em pouco período ele estava movimentando mais de 1 milhão de reais; que quando eu olho uma carteira de criptomoeda não consigo identificar quais transações são lícitas ou não; que essa informação que ele tem mais de 1 milhão de reais na conta dele está no relatório compartilhado da polícia do Rio Grande do Sul." [...] (Ação Penal, n.º 5879006-50.2023.8.09.0051, movimentação n.º 64).

O juízo de origem condenou o acusado nas penas do art. 158, "*caput*", c/c art. 71, "*caput*", ambos do Código Penal. Contudo, houve interposição de recurso de apelação, conhecido e parcialmente provido, notadamente para reconhecer a prática do crime na modalidade tentada, reduzindo, conseqüentemente, a pena (TJGO, Apelação Criminal, n.º 5879006-50.2023.8.09.0051, Relator: Dr. Gustavo Dalul Faria - Juiz Substituto em 2º Grau, 4ª Câmara Criminal, julgado em 02/10/2025).

A Turma Julgadora da 4ª Câmara Criminal do Tribunal de Justiça do Estado de Goiás, ao dar parcial provimento ao recurso do apelante, encampou a inteligência da Súmula n.º 96 do Superior Tribunal de Justiça (STJ), a qual dispõe que "o crime de extorsão se consuma independentemente da obtenção da vantagem indevida" (Terceira Seção, julgado em 3/3/1994, DJ de 10/3/1994, p. 4021).

Atualmente, o referido caso concreto conta com a interposição de Recurso Especial, na data de 23 de outubro de 2025.

3. 2 AMBIENTE VIRTUAL: "*LOCUS PERFECTUS*"

O caso a seguir envolve um "*habeas corpus*" (HC) impetrado em favor de uma mulher acusada de integrar uma organização criminosa especializada em "*sextorsão*" financeira, prática consubstanciada na extorsão das vítimas através de ameaças de divulgação de conteúdo íntimo.

A defesa pondera que a acusada não participou diretamente do recebimento dos valores extorquidos e que sua prisão preventiva carece de motivação idônea, destacando ainda a necessidade de cuidados à filha menor.

A defesa alega-se que a ré, ora impetrante, foi usada como "laranja" e que a sua prisão é excessiva, em decorrência da distância da família e a sua primariedade.

Demonstra-se a magnitude da relevância do tema em análise o julgamento do Habeas Corpus n.º 718887 / SC, ao entender que a prisão preventiva decretada tem motivação idônea, mormente pelo motivo transcrito a seguir:

[...] 3. São bastantes os motivos invocados pelo Juízo singular para embasar a prisão da acusada, é integrante de associação criminosa estável e estruturalmente ordenada, com divisão de tarefas, especializada na prática conhecida como "sextorsão". Por meio de conversas enganosas, em redes sociais e aplicativos de mensagens, os investigados constrangiam, em ambiente virtual, vítimas, intimamente expostas, a lhes transferir grande importância em dinheiro, sob a grave ameaça de divulgação de conteúdo de cunho sexual que lhes envolvia. [...] (HC n. 718.887/SC, relator Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 22/3/2022, DJe de 28/3/2022.)

A "sextorsão" financeira tem aptidão para se beneficiar de várias tecnologias, a exemplo de redes sociais, aplicativos de mensagens, jogos "on-line", câmeras em vídeo. Além do mais, não se pode olvidar da sua capacidade de manipulação por meio de inteligências artificiais. Afinal, inúmeros são os casos de manipulação de fotografias e vídeos de pessoas famosas, por exemplo, ampliando a ameaça de exposição e o poder de coação.

Cotejando o caso Luis Mijangos, nos Estados Unidos da América, e o caso Gabriel Pazzinatto Lipski, no Brasil, infere-se que a "sextorsão" financeira apresenta caráter transnacional, ou seja, os sujeitos ativos podem estar em jurisdições distintas da vítima, operando por meio de infraestrutura digital global, dificultando, assim, a persecução penal nacional. Outra similaridade em ambos os casos é o fato de que os réus são "hackers".

Não fosse o suficiente, o ambiente virtual mostra-se, indubitavelmente, como o ambiente perfeito para essa prática ilícita, viabilizando ganhos econômicos que são expressivos. Consequentemente, isso possibilita a estruturação de associações criminosas especializadas em crimes cibernéticos impróprios ["sextorsão" financeira].

À vista disso, ainda que a vítima ajuíze perante o Poder Judiciário eventual ação de desindexação, ação de retirada de conteúdo do ar, ações cíveis e criminais, não se pode negar a capacidade de transacionalidade da conduta, cuja extrapolação

das fronteiras brasileiras pode ensejar consequências irreversíveis à vida da(s) vítima(s) de “sextorsão”. Afinal, nem tudo o que se extirpa da “surface” será, de igual maneira, obliterado da “deep web”⁷.

CONCLUSÃO

Constatou-se, a partir do estudo realizado, que a sextorsão, em especial na sua vertente financeira, constitui fenômeno criminal complexo, que se consolida no ambiente virtual em razão da ampliação das possibilidades de obtenção, armazenamento e difusão de conteúdo íntimo. A internet atua como catalisadora da prática, ao permitir que atos de coação ultrapassem limites territoriais e atinjam vítimas independentemente de vínculos sociais, geográficos ou hierárquicos prévios. Esse cenário revela a crescente atualidade do tema e a necessidade de tratamento jurídico e social adequado.

A análise teórica e jurisprudencial demonstrou que a sextorsão não configura, no ordenamento jurídico brasileiro, um tipo penal autônomo. Ao contrário, corresponde a uma conduta de adequação típica plural, cuja subsunção dependerá da finalidade que impulsiona o agente. Assim, a mesma prática pode configurar constrangimento ilegal, ameaça, extorsão, estupro virtual, assédio sexual ou divulgação não consentida de conteúdo íntimo. Essa característica impõe ao intérprete rigor metodológico para identificar o bem jurídico efetivamente lesionado em cada caso concreto.

Com efeito, evidenciou-se que a sextorsão financeira, quando praticada no ambiente virtual, assume a configuração de crime cibernético impróprio, uma vez que a tecnologia opera como meio de execução, e não como objeto material do delito. O emprego de redes sociais, plataformas de compartilhamento e aplicativos de mensagens facilita o ato de constranger ou ameaçar, ampliando o impacto

⁷ A “deep web” é a parte da internet não indexada por mecanismos de busca, como o “Google”. Ela inclui conteúdo legítimo e comum, como e-mails, extratos bancários online e bases de dados restritas, acessado por meio de login e senha. É diferente da “dark web”, que é uma pequena parcela da “deep web” que exige softwares especiais (como o “Tor”) para ser acessada e é frequentemente associada a atividades ilegais.

psicológico sobre a vítima e dificultando a reação imediata diante da situação de vulnerabilidade emocional.

A investigação empreendida também permitiu constatar que o ambiente digital favorece a consolidação de práticas estruturadas e reiteradas, muitas vezes conduzidas por associações criminosas com divisão de tarefas e rotinas previamente estabelecidas. O caso “*Gabriel Pazzinatto Lipski*”, ocorrido no estado de Goiás, evidencia essa realidade, ao demonstrar que o agente utilizava e-mails criptografados e exigia pagamentos em criptomoedas para dificultar rastreamento e ocultar o produto do crime. Esse exemplo demonstra a sofisticação operacional que a sextorsão pode alcançar.

O “*leading case Luis Mijangos*”, ocorrido nos Estados Unidos e amplamente divulgado pelo FBI, mostra que a sextorsão pode ser praticada mesmo sem prévio compartilhamento voluntário de conteúdo íntimo, quando o agente emprega malware ou outras técnicas de invasão para obter acesso a imagens e conversas privadas. Tal circunstância comprova que a vítima, em muitos casos, sequer tem ciência de que seus dispositivos foram comprometidos, o que amplia o impacto emocional da ameaça de exposição.

O julgamento do Habeas Corpus nº 718887/SC pelo Superior Tribunal de Justiça também merece destaque, pois reconheceu a existência de associação criminosa especializada em sextorsão financeira, reafirmando a gravidade da conduta, sua relevância social e a necessidade de resposta estatal firme. A referência a esse precedente demonstra que o Poder Judiciário já reconhece o caráter organizado e reiterado dessa prática.

A partir dessas constatações, verificou-se que o dano causado à vítima ultrapassa a esfera patrimonial. A ameaça de exposição de conteúdos íntimos, ainda que não concretizada, já é capaz de produzir sofrimento significativo, abalo psicológico, prejuízo à reputação e rupturas familiares e sociais. Em casos extremos, como demonstram os relatos de adolescentes que cometeram suicídio após a

disseminação de imagens íntimas, o dano atinge a esfera mais sensível do direito fundamental à vida.

Além disso, observou-se que o medo da exposição pública, associado ao estigma social, frequentemente impede a denúncia. Depreendeu-se que a vergonha, a culpa internalizada e a sensação de impotência frente ao ambiente digital promovem a subnotificação e dificultam a atuação das instituições encarregadas da persecução penal. Por isso, mecanismos de acolhimento, orientação e proteção à vítima devem ser compreendidos como parte integrante da resposta estatal.

Constatou-se que a investigação criminal enfrenta obstáculos relevantes decorrentes da volatilidade do ambiente digital. A utilização de criptomoedas, redes privadas virtuais e e-mails criptografados permite ao agente diluir os rastros de identificação, tornando indispensável o desenvolvimento de métodos tecnológicos de rastreamento, assim como a cooperação internacional entre órgãos de investigação e inteligência.

Outro aspecto digno de ênfase é a ausência de um tipo penal específico que descreva a sextorsão de forma clara e autônoma. Embora o ordenamento jurídico brasileiro disponha de instrumentos adequados para a punição da conduta citada, a multiplicidade de enquadramentos possíveis dificulta a uniformidade interpretativa e pode gerar disparidade de soluções entre diferentes decisões judiciais. Esse cenário indica a necessidade de reflexão legislativa.

Demonstrou-se que a ausência de legislação específica não inviabiliza a responsabilização. O caso “*Gabriel Pazzinatto Lipski*” reafirma esse entendimento, na medida em que o Tribunal de Justiça do Estado de Goiás (TJGO) reconheceu a possibilidade de enquadramento da conduta no crime de extorsão, ainda que sem pagamento, em conformidade com a Súmula n.º 96 do Superior Tribunal de Justiça (STJ), segundo a qual o crime de extorsão se consuma independentemente da obtenção da vantagem indevida.

Permanece atual a necessidade de aperfeiçoamento normativo. A criação de um tipo penal específico contribuiria para reduzir a insegurança jurídica, uniformizar a atuação dos órgãos de investigação e fortalecer a proteção das vítimas, além de facilitar a produção de estatísticas criminais confiáveis, condição essencial para a formulação de políticas públicas eficazes.

Observou-se, também, que a política de enfrentamento da sextorsão não pode limitar-se à esfera repressiva. O fortalecimento de mecanismos educativos e preventivos é essencial para minimizar a incidência da conduta. Nesse sentido, programas de educação digital nas escolas, campanhas de conscientização sobre compartilhamento de conteúdo íntimo e formação de profissionais para atuar no acolhimento às vítimas são mecanismos indispensáveis.

A educação digital deve abranger, ainda, a orientação sobre práticas de segurança informacional, como o uso de autenticação de dois fatores, senhas reforçadas, verificação da origem de contatos virtuais e compreensão sobre riscos associados ao envio de imagens íntimas. Tais medidas não eliminam o risco, mas reduzem sua probabilidade, especialmente entre adolescentes, que constituem grupo de elevada vulnerabilidade.

Outro ponto relevante é o crescimento do uso de inteligência artificial para a criação de imagens sintéticas de cunho sexual, conhecidas como *“deepfakes”*. A manipulação de fotografias disponíveis em redes sociais para gerar conteúdo falso, mas visualmente convincente, amplia o poder de coerção da sextorsão, uma vez que retira da vítima a capacidade de se defender mediante o argumento da inexistência do ato retratado.

Esse avanço tecnológico indica que a sextorsão financeira tende a ampliar sua sofisticação e alcance nos próximos anos. A resposta estatal, portanto, deve acompanhar a evolução tecnológica, investindo em laboratórios forenses digitais, protocolos de rastreamento de transações em *“blockchain”* e capacitação contínua de agentes públicos e operadores do direito.

Ademais, políticas públicas de apoio psicossocial tornam-se imprescindíveis. A vítima da sextorsão não necessita apenas de amparo jurídico, mas também de suporte emocional estruturado, capaz de auxiliar na reconstrução de sua autoestima, de suas relações sociais e no enfrentamento dos efeitos duradouros da violência emocional e psicológica sofrida.

Nesse sentido, recomenda-se a integração entre Ministério Público, Poder Judiciário, Defensoria Pública, instituições de saúde mental e organizações da sociedade civil, de modo a construir rede de proteção contínua que ultrapasse o momento da denúncia e acompanhe a vítima em seu processo de superação.

Também se verificou a necessidade de fortalecimento de mecanismos de cooperação internacional. Considerando que os servidores, contas, perfis e fluxos financeiros podem se localizar em diferentes países, a articulação entre Estados é indispensável para prevenir que barreiras territoriais se convertam em refúgios para criminosos digitais.

A análise dos casos concretos demonstra, portanto, que a sextorsão financeira possui caráter transnacional, reiterado e lucrativo, constituindo prática que alimenta economias ilícitas e organizações criminosas estáveis. Seu enfrentamento exige visão sistêmica, interdisciplinar e coordenada.

A partir de todos os aspectos apresentados, conclui-se que a sextorsão financeira é fenômeno que ultrapassa a perspectiva penal estrita. Exige respostas que dialoguem com direitos fundamentais, saúde pública, políticas educacionais e desenvolvimento tecnológico. A proteção da dignidade da vítima deve ser o eixo orientador de toda ação institucional.

A sextorsão financeira representa uma das expressões contemporâneas mais sensíveis de violação da dignidade humana no ambiente virtual, pois converte a intimidade em instrumento de lucro, coerção e destruição emocional. Sua evolução acompanha o progresso tecnológico, e sua contenção dependerá da mesma capacidade de atualização e resposta.

Espera-se que estudos futuros aprofundem a análise do papel das inteligências artificiais na produção e detecção de conteúdos íntimos manipulados, a eficácia de ferramentas de rastreamento de transações digitais e o impacto de políticas de educação preventiva em ambientes escolares e digitais.

Assim, reforça-se que o enfrentamento da sextorsão financeira deve ser contínuo, interdisciplinar e estruturado, articulando repressão penal, prevenção educativa, proteção emocional e cooperação internacional. Somente uma resposta conjunta e coordenada poderá assegurar proteção efetiva à dignidade, à intimidade e à vida das vítimas.

Conclui-se, portanto, que a sextorsão financeira exige do Estado e da sociedade atuação constante, dinâmica e comprometida com a defesa dos direitos fundamentais, a prevenção da violência digital e a promoção de ambientes virtuais éticos e seguros.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Manual de investigação cibernética à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016.

BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 2 maio 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: seção 1, Brasília, DF, 31 dez. 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 31 abr. 2025.

BRASIL. Decreto-Lei nº 4.657, de 4 de setembro de 1942. Lei de Introdução às Normas do Direito Brasileiro. Diário Oficial da União: seção 1, Brasília, DF, 5 set. 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em: 2 maio 2025

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União: seção 1,

Brasília, DF, 3 dez. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 22 maio 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 maio 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 22 maio 2025.

BRASIL. Lei nº 13.869, de 5 de setembro de 2019. Dispõe sobre os crimes de abuso de autoridade. Diário Oficial da União: seção 1, ed. extra, Brasília, DF, 5 set. 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13869.htm>. Acesso em: 31 abr. 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato. Diário Oficial da União: seção 1, Brasília, DF, 28 maio 2021. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>. Acesso em: 22 maio 2025.

BRASIL. Superior Tribunal de Justiça (Sexta Turma). Habeas Corpus n.º 718.887/SC. Relator: Ministro Rogério Schietti Cruz. Julgado em 22 mar. 2022. DJe 28 mar. 2022. Disponível em: <<https://www.jusbrasil.com.br/jurisprudencia/stj/1466719279>>. Acesso em 23 out. 2025.

BRASIL. Superior Tribunal de Justiça. Súmula n. 96: O crime de extorsão consuma-se independentemente da obtenção da vantagem indevida. Terceira Seção, julgado em 3 mar. 1994. Diário da Justiça, Brasília, DF, 10 mar. 1994, p. 4021. Disponível em: <https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2010_7_capSumula96.pdf>. Acesso em: 24 out. 2025.

CAPEZ, Fernando. Curso de direito penal: parte geral (arts. 1º a 120). 19. ed. v. 1. São Paulo: Saraiva, 2015.

CUNHA, Rogério Sanches. Bate-papo: qual crime pratica quem comete sextorsão? Youtube, 25 jan. 2017. Disponível em: <<https://www.youtube.com/watch?v=RPxHYKQC0bs>>. Acesso em: 21 abr. 2025.

CUNHA, Rogério Sanches. Direito penal: parte especial: arts. 121 a 234-C do Código Penal. 17. ed. rev., ampl. e atual. de acordo com a Lei nº 14.155/2021. Salvador: JusPodivm, 2022. p. 594.

CUNHA, Rogério Sanches. Manual de direito penal: parte especial (arts. 121 ao 361). 9. ed. Salvador: JusPodivm, 2017.

FAGANELLO, Priscila Liane Fett. Operações de manutenção da paz da ONU. Brasília: Fundação Alexandre de Gusmão, 2014. Disponível em: <<https://funag.gov.br/loja/download/1078-operacoes-de-manutencao-de-paz.pdf>>. Acesso em: 23 abr. 2025.

FERNANDEZ, Jorge Flores. Sexting, Sextorsão e Grooming. In:_____. Vivendo esse mundo digital: impactos na saúde, na educação e nos comportamentos sexuais. Porto Alegre: Artmed, 2013.

GIUSTI, Maria Beatriz; TORRES, Vitória. Especialistas alertam para os perigos do vício em pornografia digital. Correio Braziliense. Disponível em: <<https://www.correiobraziliense.com.br/brasil/2024/10/6975633-especialistas-alertam-para-os-perigos-do-vicio-em-pornografia-digital.html>>. Acesso em: 18 maio. 2025.

GOIÁS. Tribunal de Justiça do Estado de Goiás (4ª Câmara Criminal). Apelação Criminal n. 5879006-50.2023.8.09.0051. Relator: Dr. Gustavo Dalul Faria (Juiz Substituto em 2º Grau). Julgado em 02 out. 2025. Disponível em: <<https://projudi.tjgo.jus.br/ConsultaJurisprudencia>>. Acesso em: 23 out. 2025.

ILHA, Flávio. Jovem comete suicídio depois de ter fotos íntimas vazadas na internet. O Globo. Disponível em: <<https://oglobo.globo.com/politica/jovem-comete-suicidio-depois-de-ter-fotos-intimas-vazadas-na-internet-10831415>>. Acesso em: 19 maio. 2025.

ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo, ADPESP Cultural, 2007.

INTERNATIONAL ASSOCIATION OF WOMEN JUDGES (IAWJ). Naming, Shaming, and Ending Sextortion. Washington, DC: IAWJ, 2012. Disponível em: <https://www.unodc.org/res/ji/import/guide/naming_shaming_ending_sexortion/naming_shaming_ending_sexortion.pdf>. Acesso em: 31 abr. 2025.

SAFERNET BRASIL. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. SaferNet Brasil, [s.d.]. Disponível em: <<https://indicadores.safernet.org.br/indicadores.html>>. Acesso em: 19 maio 2025.

CORREIO BRAZILIENSE. Especialistas alertam para os perigos do vício em pornografia digital. Correio Braziliense, Brasília, 29 out. 2024. Disponível em: <<https://www.correiobraziliense.com.br/brasil/2024/10/6975633-especialistas-alertam-para-os-perigos-do-vicio-em-pornografia-digital.html>>. Acesso em: 18 maio 2025.

SAFERNET BRASIL. O que é sextorsão? SaferNet Brasil, [s.d.]. Disponível em: <<https://new.safernet.org.br/content/o-que-%C3%A9-sextors%C3%A3o>>. Acesso em: 21 abr. 2025.

SOPRANI, Carolina. Abuso e exploração sexual nas operações de paz da ONU. Série Conflitos Internacionais, Marília: Observatório de Conflitos Internacionais, UNESP, v. 5, n. 6, dez. 2018. Disponível em: <<https://www.marilia.unesp.br/Home/Extensao/observatoriodeconflitosinternacionais/v.-5-n.-6-dez.-2018---abuso-e-exploracao-sexual-nas-operacoes-de-paz-da-onu.pdf>>. Acesso em: 23 abr. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Special Measures for Protection from Sexual Exploitation and Sexual Abuse. ST/SGB/2003/13. Nova York: ONU, 2003. Disponível em: <<https://docs.un.org/en/st/SGB/2003/13>>. Acesso em: 28 abr. 2025.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo de. 1. Sextorsão. In: SILVA, João da. A responsabilidade tributária dos sócios e administradores nas empresas limitadas. Revista Tributária e de Finanças Públicas, São Paulo: Revista dos Tribunais, n. 959, fev. 2006. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.959.02.PDF>. Acesso em: 31 abr. 2025.