UNIVERSIDADE PAULISTA

CURSO DE DIREITO

MAYARA DA SILVA SANTOS

CAMINHOS PARA COMBATER O CRIME DE EXTORSÃO VIRTUAL NA CONTEMPORANEIDADE

SANTOS/SP

2025

MAYARA DA SILVA SANTOS

CAMINHOS PARA COMBATER O CRIME DE EXTORSÃO VIRTUAL NA CONTEMPORANEIDADE

Trabalho de conclusão curso para obtenção do título de Graduação em Direito apresentado à Universidade Paulista – UNIP.

Orientador: Prof. Anderson Real Soares

SANTOS/SP

2025

MAYARA DA SILVA SANTOS

CAMINHOS PARA COMBATER O CRIME DE EXTORSÃO VIRTUAL NA CONTEMPORANEIDADE

Banca Examinadora

_____

Prof. Anderson Real Soares

Universidade Paulista - UNIP

_____

Professor Convidado

Universidade Paulista - UNIP

Aprovado em: ____ / ____ / ____

Dedico esse trabalho em primeiro lugar a Jesus, pois foi quem me sustentou no decorrer dessa jornada de cinco anos de curso, segundamente aos meus familiares pelo apoio que me foi fornecido e por acreditarem em mim.

“Posso não concordar com uma única palavra do que dizes, mas defenderei até a morte o direito de dizê-la”, Voltaire 1700.

RESUMO

Com o rápido desenvolvimento das tecnologias digitais, os delitos ocorridos no espaço virtual têm se tornado cada vez mais frequentes, gerando preocupações significativas para a sociedade. Neste contexto, o crime de extorsão virtual se destaca pela seriedade de suas repercussões e pela dificuldade de sua prevenção. O presente estudo tem como principal meta examinar a prática da extorsão virtual no mundo atual, analisando seus efeitos tanto nas organizações quanto na população em geral. A pesquisa também pretende refletir sobre as dificuldades encontradas no enfrentamento desse crime e propor soluções viáveis para a sua redução, levando em consideração os fatores legais, sociais e tecnológicos em jogo.

Palavras-chave: Extorsão virtual; Criminalidade cibernética; Prevenção; Direito digital.

ABSTRACT

With the rapid development of digital technologies, crimes committed in virtual spaces have become increasingly frequent, generating significant concerns for society. In this context, the crime of virtual extortion stands out due to the severity of its repercussions and the difficulty of its prevention. The main objective of this study is to examine the practice of virtual extortion in today's world, analyzing its effects on both organizations and the general population. The research also aims to reflect on the difficulties faced in combating this crime and propose viable solutions for its reduction, taking into account the legal, social and technological factors involved.

Keywords: Virtual extortion; Cybercrime; Prevention; Digital law.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
URSS	União-Soviética
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
VPNs	Redes Privadas Virtuais
CIBERLAB	Laboratório de Operações Cibernéticas

SUMÁRIO

INTRODUÇÃO 10

1. A INTERNET 12

1.1 A criação da internet 12

1.2 A importância e necessidade atual da internet 13

1.3 A evolução contínua da internet 14

2. O USO DA INTERNET COMO INSTRUMENTO DE CRIME 16

2.1 Extorsão virtual 16

2.2 Tipos de extorsão na internet 17

2.3 Análise de casos reais 19

3. A LEGISLAÇÃO ATUAL 21

3.1 Lei nº 12.965/2014 – Marco Civil da Internet 21

3.2 Lei nº 12.737/2012 – Lei Carolina Dieckmann 22

3.3 Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) 23

4. MEIOS DE MITIGAÇÃO E COMBATE 25

4.1 A necessidade de atualização contínua das tecnologias de segurança 25

4.2 Sistemas governamentais de proteção digital 26

4.3 Educação digital e conscientização pública 28

CONSIDERAÇÕES FINAIS 30

BIBLIOGRAFIA 31

INTRODUÇÃO

É notório que, atualmente a internet é um dos mais importantes meios de pesquisa, por possibilitar um rápido acesso a diversas informações, ela facilita o dia a dia dos indivíduos, se tornando imprescindível no trabalho, nos estudos e até mesmo em alguns hobbies, em razão disso ela se tornou algo fundamental para o avanço tecnológico.

Entretanto pode ser usada para cometer ilícitos penais, tais como o uso não autorizado da imagem pessoal, "*deep fakes*", nas quais são feitas imagens falsas por meio de inteligência artificial para extorsão, pornografia, chantagem e transações bancárias.

> Segundo Chaves (apud SILVA, 2003, p.19), Cibernética é a "ciência geral dos sistemas informantes e, em particular, dos sistemas de informação". Assim, por meio do conceito analítico de crime, pode-se chegar à conclusão de que "crimes cibernéticos" são todas as condutas "típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática" (SCHMIDT, 2014, [n.p.])

No amplo contexto dos delitos cibernéticos, sobressai a extorsão virtual, uma prática que se torna cada vez mais comum e elaborada. Esta abordagem consiste em forçar indivíduos a cederem benefícios financeiros, morais ou sexuais, por meio de ameaças, chantagens ou revelação de informações confidenciais. A expansão dessa forma de crime vai de par com o progresso tecnológico e a crescente integração da tecnologia na vida diária, sendo um dos principais desafios para a segurança pública no século XXI.

Em razão disso, esse trabalho tem como objetivo analisar quais são os principais crimes cibernéticos praticados atualmente no Brasil, bem como, mostrar quais as ferramentas escolhidas para tal prática, identificar as principais vítimas e estudar medidas de prevenção e mitigação desses crimes.

Além disso, o objetivo é analisar as dificuldades jurídicas que existem ao lidar com a extorsão virtual, como as autoridades policiais especializadas atuam nesse contexto, e a importância de investir na educação digital e na conscientização das pessoas. Também será discutido como a tecnologia pode ajudar na segurança cibernética. No final, espera-se apresentar ideias e sugestões que possam fortalecer

a proteção dos direitos fundamentais no ambiente online e melhorar a forma de enfrentar as ameaças digitais de maneira mais eficaz.

1. A INTERNET

1.1 A criação da internet

Segundo TANENBAUM (2011, p. 17) “A internet é um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns. É um sistema incomum no sentido de não ter sido planejado nem ser controlado por uma única organização.”

Tendo em vista a citação acima, pode-se analisar que esse conjunto de redes, originou-se durante a década de 1960, no decorrer da Guerra fria, onde ocorreu um confronto de opiniões políticas e ideológicas, tendo como protagonistas os Estados Unidos e a antiga União-Soviética (URSS), essa guerra teve um grande marco histórico, devido à ausência do uso de armas, além disso foi a responsável por dividir o mundo em dois grandes blocos econômicos, um atrelado ao comunismo e outro ao capitalismo.

A princípio esse ciberespaço era denominado como "*Arpanet*" e se tratava de uma rede de buscas, usada por militares e pesquisadores, até o momento ela tinha como objetivo possibilitar que houvesse comunicações entre os centros de produção e os centros militares, pois essa comunicação ocorria por meio de uma rede de telefonia pública, o que gerava grande vulnerabilidade nesse sistema, além disso o departamento de defesa dos Estados Unidos desejava a implementação de uma rede de controle e comandos que tivesse a capacidade de resistir a guerras nucleares, então após a antiga união soviética criar um satélite artificial denominado de Sputnik, os Estados Unidos criou em reposta a isso, o que chamamos atualmente de internet.

Entretanto, essa criação permaneceu como algo de uso exclusivo de militares e pesquisadores durante alguns anos, e foi apenas em 1980 que a internet foi expandida para a população, sendo vista como algo muito positivo, pois os indivíduos começaram a receber informações por meio de jornais online e a trocar mensagens por e-mail. E no ano de 1997 foi criado o google, maior instrumento de pesquisas na internet, que se tornou popular rapidamente, devido a sua rapidez e precisão.

> “Estima-se que em 2007 o Google processou mais de 37 bilhões de buscas por mês, seguido por 8,5 bilhões processados pelo Yahoo! E 2,2 bilhões pela Microsoft. A maioria das pessoas procura informações na internet e, com frequência, o faz muitas vezes ao dia.” (LOWE, 2010, p. 41)

Porém o Brasil só teve acesso ao mundo virtual em 1988 pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), para o uso de pesquisas acadêmicas e foi liberado a sociedade posteriormente em 1995 e assim como em seu país de origem, a internet teve um grande sucesso entre a população.

Conforme o levantamento de dados feito pelo Instituto Brasileiro de Geografia e Estatística (IBGE) em 2023, cerca de 72,5 milhões de domicílios possuem acesso a rede, no Brasil, sendo aproximadamente 94,1% na região urbana e 81,0% na região rural.

1.2 A importância e necessidade atual da internet

É de conhecimento geral que, a internet é um dos mais populares instrumentos de pesquisa da atualidade em razão de sua celeridade de informações, o que a torna algo indispensável na contemporaneidade, ela possibilita acesso a estudos, informações rápidas, comunicações e até mesmo lazer.

Pode-se analisar como exemplo o início da pandemia ocasionada pelo corona vírus, em que por se tratar de uma doença recém descoberta, ainda não tínhamos noção dos impactos da doença no organismo das pessoas e não era possível a criação de uma vacina na época, portanto a população estava impedida de se locomover, devido ao grande risco de contaminação. As escolas e todos os estabelecimentos não considerados essenciais foram obrigados a fechar, porém foi possível proporcionar o seguimento dessas atividades no ambiente virtual, crianças e adultos foram capazes de continuar estudando para não perder o seu ano letivo e várias empresas a trabalhar de maneira remota.

> “A simplificação do acesso aos computadores e a redução dos preços de software e hardware tornou a Internet um instrumento tecnológico cada vez mais popular. Mas o uso que tem sido feito da rede mundial suscita uma pluralidade de questões do ponto de vista da ética e também do Direito Penal. Se de um lado o advento dessas novas tecnologias pode propiciar incalculáveis benefícios à humanidade, por outro, tem propagado e vem

> propagando estímulos e influxos negativos, contribuindo para a decadência moral, para a violência, e principalmente, para a elevação dos índices de criminalidade, podendo se transformar num retrocesso da sociedade, visto que o mundo virtual vem causando uma série de transtornos no mundo real. Por ser um instrumento de comunicação sem fronteiras, a divulgação de informações imorais e ilegais também se tornaram práticas corriqueiras e a cada nova criação ou avanço tecnológico na área de informática também avançam os crimes de informática e pela informática (BARROS, 2002).(Apud Nina, Vinicius José da Silva, Walter José Gomes, and Domingo Marcolino Braile. "A importância da internet para as sociedades médicas." *Brazilian Journal of Cardiovascular Surgery* 26 (2011): vi-vii.)”

Fábio de Oliveira expôs em sua tese a maneira como a internet é eficaz na difusão de conhecimentos sobre a saúde, destacando o fato de o Brasil ser o quinto país no mundo a se informar sobre isso de forma online**.**

1.3 A Evolução Contínua da Internet

Posteriormente ao surgimento da Web 1.0, que era baseada em conteúdos estáticos e no consumo passivo, vieram a Web 2.0, marcada pela participação ativa dos usuários, e agora a Web 3.0, que traz conceitos de descentralização, blockchain, inteligência artificial e realidades imersivas.

Essas mudanças afetam de maneira direta as fundações sociais, políticas e legais. A Web 3.0, por sua vez, provoca debates acerca da posse digital, dos contratos inteligentes e da urgência de estabelecer regulamentações adequadas.

Além disso, assuntos como segurança digital, proteção de informações, liberdade de fala e luta contra a desinformação passaram a ser fundamentais nas conversas ao redor do mundo. Entidades internacionais, governos e empresas do setor privado estão sempre revisando regulamentos e diretrizes para enfrentar os desafios e aproveitar as oportunidades apresentadas por uma internet que se torna cada vez mais intrincada.

Assim, compreender o desenvolvimento da internet é fundamental não apenas para valorizar seu passado, mas também para se preparar para os desafios éticos, financeiros e legais que poderão aparecer no futuro. Aquilo que se iniciou

como uma iniciativa militar agora conecta bilhões de indivíduos e se consolidou como um elemento crucial para o funcionamento das sociedades atuais.

2. O USO DA INTERNET COMO INSTUMENTO DE CRIME

2.1 Extorsão virtual

O crime de extorsão, com previsão no artigo 158 do Código Penal Brasileiro, trata-se do ato de obter vantagens econômicas ou não sobre um indivíduo mediante coação. De acordo com Fernando Capez, a principal característica desse crime é que a pessoa força a vítima a fazer, não fazer ou tolerar que algo seja feito, usando violência ou uma ameaça séria, em resumo, trata-se de uma variação do crime de constrangimento ilegal, mas com uma particularidade: o criminoso tem como objetivo obter alguma vantagem econômica. CAPEZ, Fernando; op.cit. p. 455.

> “Os crimes virtuais utilizam a mesma metodologia de crimes utilizados em crimes já conhecidos. A técnica empregada que difere um pouco dos delitos presentes em nosso ordenamento jurídico penal, mas o fim que se pretende é o mesmo da conduta já tipificada. (de Oliveira, Luiz Gustavo Caratti, e Marília Gabriela Silva Dani. "Os crimes virtuais e a impunidade real”, 2011).”

Em uma breve análise da citação acima pode-se definir a extorsão virtual como a mesma conduta, porém realizada através da internet que é um ambiente em que os criminosos se sentem mais seguros em praticar delitos do que pessoalmente, em razão de terem uma sensação de ‘segurança’, devido a dificuldade em que há em rastreá-los ou até mesmo em descobrir quem é o responsável pelo crime.

O ambiente virtual dá aos criminosos uma sensação de anonimato e impunidade, tornando-os mais audaciosos. O uso de redes privadas virtuais (VPNs), e-mails temporários, perfis falsos e criptografia avançada dificulta a identificação dos responsáveis. Isso cria sérios obstáculos à persecução penal, exigindo do Estado e das instituições jurídicas constante atualização técnica e legislativa.

> “A desterritorialidade, o anonimato, a mínima chance de cair nas malhas do controle formal, a falta de aparelhamento da polícia e os impedimentos tecnológicos aliados aos altíssimos lucros obtidos promove um crescimento exponencial deste tipo de criminalidade, fazendo valer o risco por parte do criminoso.” (MOURA, 2021, p. 123*)*

Ademais, observa-se que algumas vítimas, por vergonha ou medo de exposição, deixam de denunciar os casos de extorsão virtual, o que contribui para a subnotificação e perpetuação desse tipo de crime. Essa realidade revela a

importância de campanhas educativas sobre segurança digital, bem como o fortalecimento de canais seguros e acolhedores para denúncias, como as delegacias especializadas em crimes cibernéticos.

> “Os primeiros delitos cibernéticos de informática iniciaram-se na década de 70, sendo executados, em sua grande maioria por pessoas especializadas no ramo informático com o objetivo principal de adentrar ao sistema de segurança das grandes empresas tendo como maior foco as denominadas como instituições financeiras. O perfil atual dos criminosos que atuam nessa área foi alterado, já que nos dias atuais qualquer pessoa que tenha um conhecimento, porém não tão aprofundado basta ter acesso a rede mundial de computadores para que consiga lograr êxito na execução de um crime virtual. (CARVALHO,2020, p.9).”

Essa espécie de crime, portanto, é uma realidade crescente, que afeta desde cidadãos comuns até empresas e figuras públicas, gerando prejuízos materiais, psicológicos e sociais. Seu combate exige uma atuação coordenada entre sociedade, autoridades públicas, setor privado e o sistema de justiça.

2.2 Tipos de extorsão na internet

Embora se trate do mesmo crime, existem algumas variações na forma em que ele é praticado, entre elas está a sextorsão, nesse método a extorsão é feita com base em ameaças relacionadas a conteúdos de cunho sexual envolvendo a vítima, que geralmente são fotos, vídeos ou até mesmo mensagens, em alguns casos isso é disponibilizado pela própria vitima que acredita estar compartilhando isso com alguém de confiança, já em outras situações o individuo tem a sua privacidade invadida por hackers ou por alguém que teve acesso aos seus dispositivos eletrônicos, além da coação para obtenção de dinheiro, há casos em que o criminoso obriga a pessoa a produzir mais imagens suas ou até mesmo a praticar atos libidinosos, mediante a ameaça de ser exposta.

Ademais existe o golpe por meio de *ransomware*, que trata-se de um *softwer*, que ao ser instalado bloqueia o acesso a arquivos e sistemas de um individuo ou até mesmo de uma empresa, entretanto há algumas modalidades em meio a esse método, sendo o *Leakware* ou *doxware* em que os dados são roubados e posteriormente os hackers exigem dinheiro em troca da recuperação do acesso e

para não vazarem alguns dados confidenciais, já no *Wipers*, ou *ransomware* destrutivo, em que ameaçam destruir os dados caso não obtenha as vantagens financeiras exigidas e o *Scareware* em que a quadrilha ou individuo tenta receber o resgate assustando o proprietário dos dados.

Conforme dados apurados por uma empresa Russa de cibersegurança chamada Kaspersky, foi revelado que aproximadamente 88% das empresas que já foram atacadas por meio de *ransomware*, escolheriam por fazer o pagamento do resgate caso sofressem ataques novamente, embora os especialistas indiquem que pagar aos criminosos não seja uma boa opção, pois não há nenhuma garantia de que os dados que foram encriptados, serão restituídos, o que pode resultar em novas ameaças.

Outra técnica feita para extorquir é a clonagem de contas em redes sociais ou aplicativos de mensagem, após acessarem o perfil, geralmente por meio de golpes de engenharia social, o infrator envia mensagens pedindo transferências bancárias ou PIX aos familiares e indivíduos próximas da pessoa que foi lesada, se passando por ela, apesar de se obter valores baixos, esse método tem uma grande frequência.

Em razão da evolução da inteligência artificial, foram criadas as “*deep fakes*”, em que são feitos vídeos ou fotos falsas usando o rosto e a imagem de uma pessoa, para a criação de conteúdos sexuais ou declarações enganosas e comprometedoras que ocasionam danos a reputação.

Os golpes sentimentais ou romance *scams***,** são aqueles em que o golpista se a aproveita da fragilidade emocional da vitima forjando um envolvimento amoroso, usando da confiança conquistada para consegui dinheiro, geralmente eles dizem estar passando por dificuldades financeiras e pedem ajuda, fazendo com que a pessoa transfira valores ao longo do tempo, na maioria dos casos sem perceber o perigo.

Esse tipo de fraude emocional costuma atingir principalmente pessoas mais vulneráveis, que vivem sozinhas ou que são leigas no ambiente virtual, o que torna essa prática é bastante comum em redes sociais e aplicativos de relacionamento.

A variedade de formas de extorsão na internet expõe o quão complexo e dinâmico é o ambiente digital, além de revelar a criatividade e a capacidade de adaptação dos criminosos às novas tecnologias.

2.3 Análise de casos reais

Ter uma análise de casos reais de na modalidade virtual desse delito, é de suma importância para o entendimento da complexidade a seriedade dele, além de destacar os desafios enfrentados por autoridades e vítimas na investigação e na responsabilização dos culpados, em razão disso, pode-se verificar um exemplo marcante é o ataque de *ransomware* que ocorreu em maio de 2021, envolvendo o frigorifico JBS em que as suas filiais nos Estados Unidos, no Canadá e na Austrália tiveram suas operações interrompidas durante um curto período de tempo, porém só foram reestabelecidas mediante ao pagamento de uma quantia no valor equivalente a US$ 11 milhões, realizado por meio de bitcoins, de acordo com o CEO da empresa a decisão de ceder as exigências dos criminosos, foi feita após a consulta de alguns especialistas em segurança digital, visando minimizar os impactos causados a empresas, restaurantes, fazendeiros e lojas que se abastecem pela companhia, apesar de os servidores de backup não terem sido comprometidos, o ataque teve muita repercussão devido ao valor do resgate ter sido um dois maiores a serem feitos com criptomoeda da história.

Outra situação de grande impacto foi a que ocorreu com a rede de lojas femininas Marisa em 2024, que sofreu uma invasão cibernética que gerou a exposição de alguns dados confidenciais, o ocorrido se destaca por ter sido feito por um grupo de hackers denominado de “Medusa”, que se diferencia de outros infratores por se manterem visíveis na internet, usando não só a dark web que é um local não regulamento conhecido por facilitar os crimes virtuais e ajudar na preservação do anonimato, como também a superfície da web, que é a rede tradicionalmente usada por todos. Os responsáveis pela empesa, suspenderam temporariamente os seus sistemas como uma medida de prevenção, o que limitou as consequências do ataque, entretanto o atentado criou um alarde em razão da falta de temor da quadrilha em ser descoberta.

Ademais em fevereiro de 2025, foi iniciada uma investigação pela policia civil do Estado de São Paulo, para efetuar o combate de uma quadrilha de criminosos suspeita de efetuar romance *scams* (golpes sentimentais), foi dada a operação conjunta o nome de “*Fictus Puella*”, foi necessário que a ação ocorresse em concomitância em três estados, no qual a coordenação foi feita pela diretoria de operações integradas e de inteligência (DIOPI/SENASP/MJSP), por meio do

Laboratório de Operações Cibernéticas – CIBERLAB, ocorreu o apreendimento de computadores, celulares e outros dispositivos eletrônicos o que facilitou a identificação dos participantes, o grupo abordava suas vítimas por meio de aplicativos de namoro e redes sociais, eram criados falsos perfis femininos com o objetivo de conseguir imagens intimas de homens, posteriormente os malfeitores fingiam serem policiais ou advogados para exigir vantagens financeiras em troca da não exposição das imagens. Em decorrência disso, um colaborador de um bando em Cruzeiro, acabou ceifando a sua própria vida ao não suportar a coação e pressão psicológica direcionada a ele.

Os valores acumulados por eles, eram compartilhados entre o grupo criminoso, que conseguia apagar os rastros com lavagem de dinheiro, as investigações ainda estão sendo feitas e em caso de condenação, os envolvidos podem ser submetidos a mais de 20 anos de reclusão pelos crimes de extorsão qualificada devido ao resultado de morte, associação criminosa e lavagem de dinheiro.

Além disso em 2012, imagens íntimas da atriz Carolina Dieckmann foram expostas na internet. Os criminosos exigiram dinheiro para não divulgar as fotos, configurando uma evidente tentativa de extorsão virtual. O impacto desse caso foi tão grande que levou à aprovação da Lei Carolina Dieckmann (Lei nº 12.737/2012), que tipificou crimes informáticos no Brasil e ampliou o debate público sobre privacidade e segurança digital.

Ao observar esses casos, pode-se notar os impactos e consequências ocasionadas pelo uso da internet como ferramenta de crime, que vão desde prejuízos financeiros e psicológicos até resultados mais graves como morte.

> “As pesquisas acadêmicas rigorosas parecem indicar que, em certas condições, o uso da Internet aumenta as chances de solidão, sensações de alienação ou até mesmo depressão” (CASTELLS, 2006, p. 443).

3. A LEGISLAÇÃO ATUAL

3.1 Lei nº 12.965/2014 – Marco Civil da Internet

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, é considerada um avanço importante na regulamentação do uso da internet no Brasil, pois com o seu advento foram estabelecidos direitos, deveres e princípios para usuários, provedores de serviços e autoridades públicas. Apesar de não ser uma legislação penal, o Marco Civil fornece fundamentos jurídicos relevantes para combater crimes virtuais, como casos de extorsão digital.

Entre os princípios e garantias destacados no artigo 3º do Marco Civil, estão: a proteção da privacidade, proteção dos dados pessoais, a preservação da neutralidade da rede, a responsabilização dos envolvidos de acordo com suas ações. Esses princípios ajudam a orientar ações contra abusos na internet, garantindo que a liberdade de expressão seja exercida de forma responsável, sem que isso sirva de justificativa para a prática de crimes.

Além disso, um dos dispositivos mais relevantes no combate à extorsão virtual está no artigo 19 da lei, que trata da responsabilidade dos provedores de aplicações da internet (como redes sociais, sites e plataformas de mensagens). Conforme o dispositivo:

> “O provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço, tornar indisponível o conteúdo apontado como infringente.”

Esse artigo é fundamental em casos de chantagem online ou ameaça de exposição, pois possibilita que vítimas solicitem judicialmente a remoção de conteúdo ameaçador ou ofensivo.

O Marco Civil da Internet também estabelece que as empresas devem guardar registros de conexão e de acesso a aplicações por um período determinado. Isso permite que as autoridades tenham acesso a esses dados, desde que haja uma decisão judicial, ajudando a identificar os responsáveis por crimes online, de acordo com os artigos de 13 a 15.

Outro ponto importante é a proteção do sigilo das comunicações, que busca resguardar os dados do usuário contra acessos não autorizados (art. 7º, III e VII). Mas essa proteção não é total: o próprio Marco Civil permite que informações sejam fornecidas mediante autorização judicial, o que é fundamental em investigações de crimes como extorsão.

Outrossim, o artigo 15 obriga os provedores de internet a manterem registros de acesso por pelo menos seis meses. Essa medida pode ajudar na investigação e rastreamento de criminosos, especialmente em casos em que a vítima recebe ameaças por perfis falsos ou anônimos.

3.2 Lei nº 12.737/2012 – Lei Carolina Dieckmann

A lei Carolina Dieckman (Lei nº 12.737/2012), já citada anteriormente, representa um marco significativo no combate aos crimes cibernéticos no Brasil, especialmente a extorsão virtual. Ela foi sancionada em 30 de novembro de 2012 e entrou em vigor em abril de 2013, após um caso notório envolvendo a atriz Carolina Dieckmann, cujas fotos íntimas foram disponibilizadas online, após uma invasão ao seu e-mail. Na ocasião, os criminosos exigiram dinheiro da vítima em troca da não divulgação das imagens, caracterizando uma tentativa de extorsão virtual.

Antes da implementação dessa legislação, o sistema jurídico brasileiro carecia de ferramentas específicas para lidar com crimes eletrônicos, o que dificultava a classificação, investigação e punição dos responsáveis. Essa lei trouxe mudanças ao Código Penal, com destaque para o artigo 154-A, que criminaliza a invasão de dispositivos informáticos, como computadores e celulares, sem autorização do proprietário, com o intuito de obter, adulterar ou destruir dados. O artigo 154-A do Código Penal estabelece: Invadir dispositivo informático alheio, violando indevidamente mecanismos de segurança, para obter, adulterar ou destruir dados sem autorização do titular ou instalar vulnerabilidades visando vantagem ilícita: pena de detenção de 3 meses a 1 ano e multa.

A pena pode aumentar se houver divulgação ou comercialização dos dados ou se a infração causar danos econômicos à vítima. Isso é crucial para casos de sextorsão ou chantagens digitais, onde dados íntimos são usados para coagir. Assim, a Lei Carolina Dieckmann é fundamental na prevenção e repressão da

extorsão virtual, responsabilizando os autores de invasões digitais que exploram emocional e financeiramente suas vítimas.

3.3 Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi criada para acompanhar o crescimento da digitalização na nossa rotina e o aumento na coleta e compartilhamento de informações pessoais por empresas e órgãos públicos. No caso de crimes como a extorsão virtual, ela tem suma importância pois muitos desses delitos dependem do acesso, uso ou vazamento indevido de dados sensíveis para ameaçar ou chantagear as vítimas. Por isso, fortalecer as regras de proteção de dados ajuda tanto na prevenção quanto na repressão desses crimes, dificultando a ação dos criminosos e estabelecendo responsabilidades para quem, por negligência ou má intenção, facilita o acesso às informações pessoais.

Além de ser responsável pela regulamentação de tratamento de dados pessoais, abrangendo desde a coleta até a eliminação, aplicando-se a indivíduos ou entidades, públicas ou privadas, que realizem operações de tratamento de dados no território brasileiro ou envolvendo pessoas localizadas no Brasil. De acordo com o artigo 2º, os princípios da lei são: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, informação e comunicação; e a proteção da intimidade, honra e imagem. A LGPD oferece proteção especial aos chamados dados pessoais sensíveis, definidos no artigo 5º, II, como aqueles relacionados à origem racial ou étnica, crenças religiosas, opiniões políticas, dados genéticos ou biométricos, além de informações sobre saúde ou vida sexual, tais dados são frequentemente usados como principais meios de ameaça, em casos de sextorsão ou na chantagem referente a divulgação de histórico de navegação ou conversas privadas.

Outrossim, instituiu a Autoridade Nacional de Proteção de Dados (ANPD), como o órgão encarregado de supervisionar e aplicar a legislação, além de fomentar a conscientização sobre a relevância da proteção de dados. A atuação da ANPD é fundamental para definir diretrizes de boas práticas e governança, estimulando organizações a implementarem medidas preventivas contra o uso inadequado de informações pessoais. A ANPD também tem a competência de exigir a notificação

obrigatória de incidentes de segurança, possibilitando respostas rápidas por parte das vítimas e das autoridades, reduzindo os impactos de eventuais delitos digitais.

4. MEIOS DE MITIGAÇÃO E COMBATE

4.1 A necessidade de atualização contínua das tecnologias de segurança

A mitigação de chantagem digital requer, além de leis apropriadas, o uso firme e planejado de técnicas de proteção de dados, atualmente várias ferramentas têm sido criadas com o objetivo de evitar, achar e enfraquecer investidas online. Entre as mais usadas estão: programas antivírus, barreiras de proteção, verificação de múltiplos fatores, codificação completa, estruturas de cópia de segurança automática e capacidade intelectual simulada aplicada à proteção digital.

Tais técnicas já mostraram força na proteção de informações e na diminuição de pontos fracos, contudo, a capacidade de ação desses métodos depende de sua melhora constante, da prática em grande quantidade e da união entre áreas diferentes. Por exemplo, estruturas de descoberta de perigos com uso de aprendizado automático podem perceber jeitos raros de chegar a redes, mas têm limites se não estiverem ligadas a bases de dados melhoradas com perigos mundiais.

Em relação à entrada, há tanto soluções sem custo quanto pagas. Ferramentas como antivírus sem custo (ex: Avast, AVG), redes privadas virtuais básicas, verificadores móveis (ex: Google *Authenticator*, Microsoft *Authenticator*) e depósito na nuvem com cópia de segurança limitada são bem fáceis de achar sem custos. Entretanto, versões mais fortes e totais — com acompanhamento no tempo certo, ajuda técnica especializada e proteção contra programas de resgate — geralmente são propostas em planos pagos, o que pode diminuir a entrada de firmas pequenas e pessoas normais.

Para fazer essas técnicas mais eficazes, é preciso que o governo impulsione sua divulgação por meio de planos de incentivo, acordos com o campo privado e ações de ensino. Além disso, é importante que o próprio governo coloque dinheiro em estruturas próprias de proteção digital, de forma sem custo, e deixe disponível ajuda técnica à gente fraca a investidas online.

Sendo assim, a proteção digital não deve ser vista como uma vantagem só de empresas grandes ou peritos em tecnologia da informação. A mudança para que

todos entrem nas técnicas de proteção é um passo importante para evitar a chantagem digital, ainda mais na frente do aumento de golpes baseados em jeito social, captura de dados e saídas de informações delicadas.

4.2 Sistemas Governamentais de Proteção Digital

A segurança é um dos direitos fundamentais estabelecidos pela constituição federal brasileira, em razão disso a proteção da comunidade contra delitos digitais, não deve ser responsabilidade única do cidadão. O governo deve assumir um papel fundamental na antecipação, vigilância e repressão a essas atividades ilegais, por meio da criação e aprimoramento de sistemas estatais de segurança digital. Uma das iniciativas mais significativas existentes no Brasil é o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), que é responsável pela vigilância de ameaças, pela geração de alertas de segurança e pela coordenação de respostas a incidentes cibernéticos na esfera da administração federal.

> “Em segurança, a informação um ativo importante na sociedade contemporânea, estas precisam ser protegidas contra as ameaças que podem pôr em risco sua adulteração, divulgação não autorizada e até mesmo perda (MINATEL; MALAGOLLI, 2019).”

Entretanto, o impacto dessa iniciativa ainda é restrito, não abrangendo diretamente a proteção de cidadãos individuais e pequenas empresas, para que esse sistema seja mais eficiente, é vital que ele seja ampliado e integrado às políticas públicas em níveis municipal e estadual, criando uma rede de defesa digital descentralizada.

Outra alternativa viável é a criação de plataformas públicas gratuitas focadas em educação sobre segurança digital, identificação de ataques e assistência técnica. Esses sistemas poderiam atuar como centros de denúncia e aconselhamento, semelhantes ao Disque 100 ou 180, mas voltados especificamente para crimes virtuais. Além disso, essas plataformas poderiam fornecer serviços básicos de proteção, como antivírus de domínio público, sistemas para checar vulnerabilidades em redes domésticas e notificações de riscos online.

Adicionalmente, o governo pode incentivar a segurança digital através de colaborações entre o setor público e o privado, estabelecendo acordos com empresas especializadas para disponibilizar tecnologias avançadas à população de forma acessível ou gratuita. Um exemplo disso seria a disponibilização de licenças subsidiadas para softwares de proteção digital a alunos, servidores públicos, profissionais autônomos e microempresários, que frequentemente não têm acesso a soluções robustas devido aos custos envolvidos.

No aspecto regulatório, é imprescindível que o governo crie políticas públicas claras e eficientes voltadas para a governança digital, a proteção de dados pessoais e a resposta imediata a incidentes de segurança. A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e a Lei nº 12.965/2014 (Marco Civil da Internet) já proporcionam bases jurídicas importantes, mas a execução eficaz depende da implementação de infraestruturas técnicas que garantam a segurança das informações que transitam no ambiente digital.

Um progresso adicional seria a criação de uma plataforma nacional integrada de rastreamento de delitos cibernéticos, interligada a delegacias especializadas e órgãos de polícia, acelerando investigações e promovendo a cooperação entre entidades de diferentes estados. Isso não apenas reforçaria a capacidade de resposta, mas também aumentaria a confiança da população nas ações do governo em relação a crimes que, frequentemente, são ignorados ou subnotificados.

Finalmente, é fundamental que o governo brasileiro dedique esforços à cooperação internacional, conectando-se com outras nações e organismos multilaterais para abordar a essência transnacional dos crimes cibernéticos. O intercâmbio de informações, metodologias de investigação e tecnologias de proteção se torna cada vez mais imprescindível devido à atuação de criminosos que atuam além das fronteiras.

Em resumo, os sistemas de segurança digital do governo precisam se transformar em um formato mais inclusivo, acessível, claro e tecnológico, de acordo com as demandas da sociedade digital atual. Proteger a dignidade, a privacidade e a segurança dos cidadãos no ambiente online é uma responsabilidade do governo e um elemento crucial do Estado Democrático de Direito na era digital.

4.3 Educação Digital e Conscientização Pública

Alguns ataques virtuais, incluindo aqueles que resultam em extorsão, ocorre por meio da chamada engenharia social, técnica que explora vulnerabilidades humanas, como o desconhecimento, a confiança ou o medo. Criminosos induzem as vítimas a fornecerem dados sensíveis, acessarem links maliciosos ou realizarem pagamentos indevidos. Nesses casos, a melhor defesa não é técnica, mas educacional.

> “Engenharia Social pode ser definida como conjunto de métodos e técnicas com o objetivo de obter informações sigilosas através de técnicas investigativas, psicológicas e de enganação, para isso os indivíduos manipulam pessoas para obter informações confidenciais ou persuadi-las a realizar ações que beneficiem os manipuladores. Essa prática se baseia na exploração da confiança e na habilidade de comunicação dos engenheiros sociais, usam truques psicológicos para enganar as pessoas, aproveitando sua tendência natural de confiar umas nas outras (MINATEL; MALAGOLLI, 2019)”.

Nesse contexto, a alfabetização digital deve ser promovida desde a educação básica, integrando noções de segurança da informação, privacidade e ética digital ao currículo escolar. Além disso, é necessário investir em programas contínuos de capacitação voltados para diferentes faixas etárias e públicos, especialmente idosos, jovens e microempreendedores — que são alvos frequentes de fraudes e extorsões online.

Campanhas públicas de conscientização, com linguagem acessível e ampla divulgação, são também estratégias eficazes. Órgãos como o Ministério da Justiça, a Polícia Federal e a Autoridade Nacional de Proteção de Dados (ANPD) podem liderar iniciativas educativas nacionais, com orientações práticas sobre proteção de senhas, identificação de golpes, configuração de privacidade e cuidados com redes públicas de internet.

A disseminação de boas práticas de segurança digital deve ser incentivada não apenas em escolas e repartições públicas, mas também por meio da mídia, redes sociais, aplicativos governamentais e plataformas digitais de uso cotidiano. A criação de um portal oficial de orientação e prevenção contra crimes cibernéticos, mantido pelo governo, poderia reunir cartilhas, vídeos tutoriais e canais de denúncia, tornando o conhecimento acessível a toda a população.

Além disso, a formação continuada de profissionais do Direito, da Segurança Pública e da Educação é essencial para que esses agentes atuem como multiplicadores da conscientização digital e estejam preparados para lidar com as complexidades dos crimes virtuais.

Portanto, promover a educação digital é investir em prevenção eficaz, inclusão social e cidadania digital. A conscientização pública não é apenas uma medida de segurança, mas um direito coletivo e um dever do Estado na era da informação. Somente com uma sociedade informada e consciente será possível reduzir significativamente a incidência de crimes de extorsão virtual e outros delitos cibernéticos.

CONSIDERAÇÕES FINAIS

Nesse cenário, é notório que, a internet gera diversas vantagens e conveniências as organizações e a sociedade, devido a possibilitar um célere acesso a diversas informações, por outro lado pode ser usada como um instrumento facilitador de crimes, por gerar comodidade e uma sensação de anonimato e impunidade aos criminosos.

Diante da problemática exposta sobre os caminhos para o combate a extorsão virtual na contemporaneidade, nota-se que apesar do avanço em relação ao combate de crimes realizados por meio de internet, como a extorsão virtual, tais como as leis citadas, LGPD, Carolina Dieckman e o Marco histórico, os delitos ainda não foram minimizados.

Em razão disso, torna-se necessário a implementação de sistemas de sistemas governamentais de proteção digital, para uma democratização ao acesso desses *softwers*, a atualização contínua das tecnologias de segurança para garantir a sua eficácia e a educação digital e conscientização pública, para evitar que as pessoas sejam lesadas por meio de extorsão virtual.

BIBLIOGRAFIA

BARROS, E. C. *Crimes digitais: teoria e prática*. São Paulo: Editora Atlas, 2002.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União: seção 1, Brasília, DF, 03 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

CAPEZ, Fernando. *Curso de direito penal: parte especial*. 15. ed. São Paulo: Saraiva, 2010.

CARVALHO, A. R. de. *Crimes virtuais: teoria, prática e legislação aplicada*. São Paulo: Revista dos Tribunais, 2020.

CASTELLS, Manuel. *A sociedade em rede*. 9. ed. São Paulo: Paz e Terra, 2006.

CHAVES, José. Apud SILVA, José Afonso da. *Curso de direito constitucional positivo*. 25. ed. São Paulo: Malheiros, 2003.

DE OLIVEIRA, Luiz Gustavo Caratti; DANI, Marília Gabriela Silva. *Os crimes virtuais e a impunidade real*. Revista Eletrônica de Direito Penal, 2011.

LOWE, Henry. *Internet e Sociedade*. Porto Alegre: Bookman, 2010.

MINATEL, Sebastião L.; MALAGOLLI, Gabriel M. *Segurança da informação: aspectos teóricos e práticos*. São Paulo: Érica, 2019.

NINA, Vinicius José da Silva; GOMES, Walter José; BRAILE, Domingo Marcolino. A importância da internet para as sociedades médicas. *Brazilian Journal of Cardiovascular Surgery*, v. 26, p. vi–vii, 2011.

SCHMIDT, Alan. *Crimes digitais: a evolução da cibercriminalidade*. Curitiba: Juruá, 2014.

TANENBAUM, Andrew S. *Redes de computadores*. 5. ed. São Paulo: Pearson, 2011.

CNN BRASIL. Após ataque, 90% das empresas vítimas de ransomware pagariam resgate, diz relatório. 2024. Disponível em: https://www.cnnbrasil.com.br/tecnologia/apos-ataque-90-das-empresas-vitimas-de-ransomware-pagariam-resgate-diz-relatorio/. Acesso em: 15 mar. 2025.

G1. JBS diz que pagou US$ 11 milhões em resposta a ataque hacker. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 25 mar. 2025.

G1. Lojas Marisa sofre ataque cibernético e avalia extensão do incidente. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/11/05/lojas-marisa-sofre-ataque-cibernetico-e-avalia-extensao-do-incidente.ghtml. Acesso em: 30 mar. 2025.

INTRANET TRT8. Extorsão digital: entenda o que é e como se proteger. Disponível em: https://intranet.trt8.jus.br/noticia/extorsao-digital-entenda-o-que-e-e-como-se-proteger. Acesso em: 07 abr. 2025.

BRASIL ESCOLA. Internet. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em: 11 mai. 2025.