ISSN 2179-0167

REVISTA JurES - v.13, n.24, p. 19-35, dez. 2020

EXTORSÃO VIRTUAL: VELHO CRIME, NOVAS PRÁTICAS

VIRTUAL EXTORTION: OLD CRIME, NEW PRACTICES

Virgínia Luna Smith[1]
Faculdade Estácio de Vitória – FESV, Vitória/ES - Brasil

Janaína Aparecida Soares Gaspar Sanches[2]
Faculdade Estácio de Vitória – FESV, Vitória/ES - Brasil

Roberta de Carvalho Borba[3]
Faculdade Estácio de Vitória – FESV, Vitória/ES - Brasil

Resumo

Com a evolução tecnológica e o desenvolvimento da internet, ligando pessoas, empresas e instituições sem fronteiras, a segurança da informação passou a ser alvo de questionamentos após o surgimento de crimes no âmbito virtual; crimes já existentes no ordenamento jurídico pátrio, porém com novas abordagens no cenário cibernético. A todo o momento, criminosos inovam, criam modalidades, formas e meios com o fim específico de obter vantagens ilícitas. Nesse contexto, o presente estudo objetiva apresentar a extorsão virtual como um ilícito específico que promove a quebra da ordem nesse universo digital. Em seguida, verificou-se sua tipificação criminal e as legislações pertinentes e específicas que possam ser contempladas nesse cenário criminoso. E, por fim, uma breve consideração sobre a atuação das delegacias especializadas em crimes virtuais, avaliando, no seu campo de atuação, a prevenção e repressão desses atos ilícitos, a fim de propor possíveis respostas aos danos patrimoniais nos quais o cidadão brasileiro está submetido.

Palavras-chave: cibercrimes; extorsão; sextorsão; crimes virtuais.

Abstract

With the technological evolution and the development of the internet, connecting people, companies and institutions without borders, information security started to be questioned after the emergence of crimes in the virtual sphere; crimes already existing in the national legal system, but with new approaches in the cyber scenario. At every moment, criminals innovate, create modalities, forms and means with the specific purpose of obtaining illicit advantages. In this context, the present study aims to present virtual extortion as a specific offense that promotes the breaking of order in this digital universe. Then, it was verified its criminal classification and the pertinent and specific legislation that

[1] Doutora em Direito pela Pontifícia Universidade Católica de São Paulo; Professora da Faculdade Estácio de Sá de Vitória-ES. E-mail: smith.virginia@estacio.br

[2] Graduanda em Direito pela Faculdade Estácio de Vitória-ES. E-mail: dejsanches@gmail.com

[3] Mestre em Política Social pela UFES (2011). Especialista em Projetos Sociais (2003) e graduada em Serviço Social, pela UFES (1999). É professora mestre da Sociedade de Ensino Superior Estácio Vitória e Vila Velha/ES e graduanda em Direito pela Faculdade Estácio de Vitória-ES. E-mail: roborba70@gmail.com

can be contemplated in this criminal scenario. And, finally, a brief consideration of the performance of the police stations specialized in virtual crimes, evaluating, in their field of action, the prevention and repression of these illegal acts, in order to propose possible responses to the property damage to which the Brazilian citizen is subjected.

Keywords: cybercrimes; extortion; sextortion; virtual crimes.

1 INTRODUÇÃO

Nesta contemporaneidade, vivemos a era da “sociedade da informação”, onde a tecnologia e o uso da internet evoluem de maneira imensurável, impactando nos padrões de qualidade de vida, aproximando pessoas, influenciando e promovendo avanços sobre o mercado em seus produtos e serviços, o trabalho e tantas outras dimensões da vida em sociedade.

Nesta mesma dinâmica, evidencia-se o aumento acelerado de práticas delituosas e o surgimento de crimes das mais variadas formas, dentre eles, a extorsão no ambiente virtual de informação e comunicação. É imperioso salientar que a extorsão é um delito penal que desde sempre acompanha os processos históricos da civilização. Entretanto, este artigo objetiva refletir sobre as nuances das novas práticas, a extorsão no mundo virtual como um ilícito específico, que promove a quebra da ordem nesse universo digital.

Desafortunadamente, a sociedade brasileira convive com a insegurança no mundo digital e a pouca celeridade da atualização do aparato legal para perseguição de tais crimes. Como desafio, a cibercriminalidade traz à tona, a necessidade de inovações e profundas adaptações dos ordenamentos jurídicos brasileiros, no que tange aos instrumentos e mecanismos adequados de investigação para fazer frente aos novos meios de cometimento de determinados delitos e de inovadoras condutas delituosas que surgem com o mundo cibernético.

Para a realização de tal abordagem, utiliza-se como metodologia a pesquisa bibliográfica de caráter exploratório e descritivo, através de uma revisão literária doutrinária e jurídica, fundamentada em livros, artigos e sites, visando disseminar o conhecimento do público em geral acerca desse crime e a necessidade do ordenamento jurídico e instituições policiais e judiciárias.

Neste artigo, de cunho teórico, almeja-se contribuir para o debate em torno das questões aventadas em cada tópico, sem nenhuma pretensão de preencher as lacunas e desafios inerentes à temática, mas acredita-se que se trata de uma reflexão inicial, sendo somente este nosso intuito.

Primeiramente, o artigo traz uma breve contextualização sobre o Ciberespaço e os Cibercrimes, tratando o universo da web como um imenso território em expansão acelerada e as diversas modalidades tradicionais de crimes que atualmente podem ser praticados web, dentre eles, a “extorsão virtual”, sobre o qual este artigo pretende tratar.

Na sequência, aborda-se a extorsão conforme previsão no código penal brasileiro, bem como as modalidades mais recorrentes do delito de extorsão praticadas no ambiente virtual, como a “sextorsão”, a clonagem de WhatsApp e a invasão de computadores por meio do protocolo RPD.

Em seguida, a abordagem apresenta a atuação das delegacias de crimes informáticos, como jurisdição frente ao enfrentamento às novas modalidades criminosas que desconhecem fronteiras em um mundo politicamente fragmentado e os desafios no combate dessas infrações penais. Posteriormente, adentra-se as considerações finais.

2 O CIBERESPAÇO E OS CIBERCRIMES

Não se pode pretender escrever sobre os crimes cibernéticos, sem ao menos compreender o que o advento da rede mundial de computadores representou e ainda hoje representa, em todos os setores da economia e sociedade mundiais. “Para alguns, seus inventores e primeiros promotores, a rede é um espaço livre de comunicação interativa e comunitário, um instrumento mundial de inteligência coletiva”. (LÉVY, 1999, p. 201).

A definição mais comum para os crimes cibernéticos é:

> (...) aquele no qual um ou mais computador (es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais conduta(s) criminalizada(s), ou são alvo(s) desta(s). O homem interagindo com uma máquina – retroalimentando-a com informações por meio de mensagens – através de uma rede de computadores (cibernética)

> interligados (ciberespaço), agindo conforme uma conduta previamente criminalizada (Crime informático) estereotiparia um modelo de cibercrime" (COLLI, 2010, p. 44).

A expressão *World Wide Web* (WWW) é a sigla para *World Wide Web*, ou *Surface Web*, que significa rede de alcance mundial, em português. O WWW é um sistema em hipermídia, que é a reunião de várias mídias interligadas por sistemas eletrônicos de comunicação e executadas na Internet, onde é possível acessar qualquer site para consulta na Internet. A tradução literal de *World Wide Web* é "teia em todo o mundo" ou "teia do tamanho do mundo", e indica a potencialidade da internet, capaz de conectar o mundo, como se fosse uma teia[4]".

Assim que adentramos no universo da web, ou rede, descobrimos que ele não constitui apenas um imenso território em expansão acelerada, mas que oferece, além de uma infinidade de conteúdo, inúmeros mapas, filtros e seleções para quem pretende explorá-la (LÉVY, 1999).

O termo "*Surface Web*" refere-se à porção aparente, emersa ou superficial da navegação na rede, composta por tudo o que é direcionado por sites de busca como o Google ou o Bing, e, em razão dessa forma de "controle", é acessado livremente.

Há, entretanto, a chamada "*Deep Web*", ou "rede profunda", camada "invisível" dentro da rede superficial, e que possuiria uma área da Internet muito maior do que a área da superfície, formada por incontáveis páginas, blogs, vídeos, fóruns e bancos de dados ocultos do grande público, que reúne milhares de informações com mínima possibilidade de rastreamento e pouca regulamentação.

Esta plataforma fica "escondida", ou seja, não pode ser acessada por meio de pesquisas em buscadores, como o Google ou Bing, e nem digitando um endereço em um navegador comum (Chrome, Firefox, Edge, etc.), afirmando-se, portanto, que estes conteúdos são configurados como privados. Além disso, em alguns casos não é possível identificar o IP do usuário da *Deep Web*, de forma a favorecer o anonimato.

A "privacidade" conferida pela *Deep Web* aos criadores de conteúdo e a quem o acessa é bastante criticada, pois supostamente encorajaria a veiculação de conteúdos de ódio ou que incentivem a prática de crimes. Em geral, esses espaços

[4] Disponível em: < https://www.significados.com.br/www/>. Acesso em 25/10/2020.

na *Deep Web* são conhecidos como *Dark Web* (internet "obscura", em tradução livre), justamente pelo compartilhamento de conteúdo ilegal, como recrutamento, auxílio e compartilhamentos da prática de toda a sorte de crimes[5].

A expansão do espaço físico dentro da rede mundial de computadores, criou o que alguns doutrinadores passaram a denominar de ***"ciberespaço"***, ou seja, o

> "espaço virtual para a comunicação que surge da interconexão das redes de dispositivos digitais interligados no planeta, incluindo seus documentos, programas e dados"[6], e que, portanto não se refere apenas à infraestrutura material da comunicação digital, mas também ao "(...) espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores". (LÉVY, 1999, p. 92).

Esse ambiente virtual de informação e comunicação inegavelmente proporcionou desenvolvimento e mudanças econômicas e sociais, porém, com eles também surgiu a necessidade de proteger novos bens jurídicos, expandindo o Direito Penal para que a tutela estatal seja eficiente.

No ciberespaço, tanto em sua superfície quanto em sua camada profunda e, notadamente na camada obscura, pode-se afirmar que são praticados diversos ilícitos penais, chamados de ***"cibercrimes"***, ou crimes cometidos usando o ambiente digital ou virtual como meio ou elemento.

Ainda que novas figuras típicas penais sejam concebidas a partir das experiências no ciberespaço, pode-se afirmar que qualquer modalidade prevista no Código Penal Brasileiro (Decreto-Lei 2.848/40) e no extenso rol de leis penais extravagantes, criadas à época considerando apenas os limites espaciais físicos, poderão ser praticados também no ambiente virtual, desde que a rede mundial de computadores seja o meio ou instrumento para o seu cometimento.

Dentre as modalidades tradicionais de crimes que atualmente podem ser praticados na *Surface Web*, *Deep Web* ou *Dark Web*, encontra-se a "extorsão virtual", sobre a qual este artigo pretende tratar.

[5] Disponível em: <https://tecnoblog.net/282436/deep-web-e-dark-web-qual-a-diferenca/>. Acesso em 25/10/2020
[6] Disponível em: <https://pt.wikipedia.org/wiki/Ciberespa%C3%A7o>. Acesso em 25/10/2020.

3 O CRIME DE EXTORSÃO PREVISTO NO CÓDIGO PENAL

O uso diversificado da rede mundial de computadores vem abrindo caminhos para a prática de delitos ou para novas formas de cometimentos de crimes já existentes, em casos nem sempre fáceis de serem enquadrados no ordenamento jurídico vigente.

No Brasil, a extorsão foi inserida no Código Penal de 1890, em seu artigo 362, com a seguinte descrição e grafia à época “Sequestrar uma pessoa para obter della, ou de outrem, como preço de sua libertação, dinheiro, cousa ou acto que importe qualquer effeito jurídico: §1° Extorquir de alguém vantagem illicita, pelo temor de grave damno á sua pessoa ou bens; constranger alguém quer por ameaça de publicações infamantes e falsas denuncias, quer simulado ordem de autoridade, ou fingindo-se tal, a mandar depositar, ou pôr á disposição, dinheiro cousa, ou acto que importe effeito jurídico. §2° Obrigar alguém, com violência ou ameaça de grave damno á sua pessoa ou bens, a assignar, escrever ou anniquilar, em prejuízo seu, ou de outrem, um acto que importe effeito jurídico: Pena - prisão cellular por dous a oito annos"[7].

Posteriormente, esse delito foi separado dos outros delitos contra o patrimônio, e encontra-se previsto no art. 158, *caput*, do Código Penal de 1940, conforme disposto: "Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa"[8]. A pena prevista é de reclusão, de 4 (quatro) a 10 (dez) anos, e multa.

Todavia, no ordenamento jurídico brasileiro, verifica-se um esparso grupo de normas que disciplinam e criminalizam essas ações cibernéticas. A Lei n° 12.735/2012, elencando condutas realizadas mediante uso de sistema eletrônico, digital ou similares; a Lei n° 12.737/2012, tipificando criminalmente delitos informáticos e a Lei n° 12.965/2014, estabelecendo princípios, garantias, direitos e

[7] Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1851-1899/d847.htm>. Acesso em 25/10/2020
[8] Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 25/10/2020

deveres para o uso da internet no Brasil – tido como o Marco Civil da Internet. Entretanto, não há uma legislação criminal que trate especificamente da extorsão virtual, devendo o operador do direito, utilizar os tipos existentes no Código Penal e legislações extravagantes.

Bitencourt (2019) assevera que a extorsão é o ato de constranger alguém, mediante violência ou grave ameaça, com o fim de obter vantagem econômica indevida, para si ou para outrem, a fazer, tolerar que se faça ou deixar de fazer alguma coisa. A finalidade do constrangimento, na extorsão, é obter indevida vantagem econômica, para si ou para outrem.

Nesse contexto, o delito exige como elementos essenciais, a coação da vítima e a obrigação de agir ou deixar de agir, de modo a proporcionar o proveito ilícito para o autor do delito. Insere-se na categoria dos delitos com a cooperação da vítima, sendo caracterizada pelo requisito positivo do ato de disposição patrimonial. Por conseguinte, a extorsão pode se concretizar mediante constrangimento físico (violência) ou psicológico (ameaça) e tendo como consequência da conduta, a obtenção de proveito injusto, podendo repercutir em consumação ou tentativa (PRADO, 2019).

O doutrinador Guilherme de Souza Nucci, elenca três estágios para o cometimento da extorsão: “1º) o agente constrange a vítima, valendo-se de violência ou grave ameaça; 2°) a vítima age, por conta disso, fazendo, tolerando que se faça ou deixando de fazer alguma coisa; 3°) o agente obtém a vantagem econômica almejada" (NUCCI, 2019, p.412).

Sob a ótica de Jesus e Estefam (2020, p. 374) "a extorsão atinge a consumação com a conduta típica imediatamente anterior à produção do resultado visado pelo sujeito". A finalidade do sujeito é a obtenção da indevida vantagem econômica. Desse modo, consuma-se o delito com o comportamento positivo ou negativo da vítima, no instante em que ela faz, deixa de fazer ou tolera que se faça alguma coisa. Não há necessidade de que o sujeito obtenha a vantagem indevida.

Além disso, a Súmula 96 do STJ, descreve: "O crime de extorsão consuma-se independentemente da obtenção da vantagem indevida".

A doutrina entende que a extorsão trata-se de um crime comum (aquele que não demanda sujeito ativo qualificado ou especial); formal (configuração com o constrangimento da vítima); comissivo (implicando ação); de dano (consuma-se com a efetiva lesão a um bem jurídico tutelado); unissubjetivo (que pode ser praticado por um só agente); plurissubsistente (em regra, vários atos integram a conduta) e que admite tentativa (NUCCI, 2019).

4 AS MODALIDADES DE EXTORSÃO PRATICADAS NO AMBIENTE VIRTUAL

A tecnologia e a internet proporcionaram vários benefícios para a sociedade. No entanto, os avanços coletivos sem fronteiras, permitem que indivíduos mal intencionados estejam em vários lugares ao mesmo tempo, podendo praticar diversos atos criminosos.

Nesse cenário, temos a figura do criminoso informático que possui inteligência, conhecimento de sistemas e utiliza a tecnologia informatizada com o fim específico de atingir bens jurídicos alheios. Diante disso, podemos diferenciar os criminosos existentes no mundo virtual: *hackers* (invadem sistemas de informação para obtenção de dados ou para testar seus conhecimentos); *crackers* (têm a finalidade de causar prejuízos, trazendo danos as suas vítimas); *lammers* (são iniciantes, usam programas de invasões e de quebra de segurança para atacar pessoas leigas); *phreakers* (especialistas em invasões em sistemas de telefonia); *war drive* (especialistas em invasões de redes sem fio); *carders* (especialistas em fraudes com cartões de créditos) e, por fim, os *gurus* (indivíduos que detêm conhecimentos avançados - telefonia, redes, satélites, etc.).

Nos termos do artigo 158 do código penal brasileiro, a extorsão configura-se quando o agente constrange gravemente a vítima por qualquer meio de comunicação encontrado na internet: redes sociais, programas de mensagens instantâneas e, consequentemente, fazer com que a vítima entregue dinheiro ou qualquer outro bem patrimonial. Entretanto, devido ao modus operandi não estar tipificado em lei, não há uma sanção para o delito praticado por intermédio de sistemas informatizados conectados à internet.

4.1 A “SEXTORSÃO”

O acesso aos dispositivos eletrônicos, tais como: smartphones, computadores e tablets e a praticidade no uso de redes sociais e mensagens instantâneas promoveram o hábito de envios de fotos e vídeos pessoais, levando a conduta de exposição do próprio corpo e podendo gerar graves consequências.

A promotora de justiça Ana Lara Camargo de Castro[9] descreve o termo sextorsão como uma aglutinação da palavra “sexo” com a palavra “extorsão”. Trata-se da situação em que uma relação de poder é utilizada como instrumento para a obtenção de vantagens sexuais.

Sanches (2017) define sextorsão como:

> (...) o agente constrange outra pessoa se valendo de imagens ou vídeos de teor erótico que de alguma forma a envolvam. No caso, emprega-se grave ameaça consistente na promessa de divulgação do material caso a vítima se recuse a atender à exigência. A depender das circunstâncias, vislumbramos três figuras criminosas às quais a conduta pode se subsumir: a) se o agente simplesmente constrange a vítima a não fazer o que a lei permite, ou a fazer o que ela não manda, há constrangimento ilegal; b) se constrange a vítima, com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa, há o crime em estudo; c) se constrange a vítima à prática de atividade sexual, há estupro (SANCHES, 2017, p. 305).

A SaferNet Brasil[10], associação civil de direito privado, com foco na defesa dos Direitos Humanos na internet brasileira, define sextorsão como “ameaça de 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.

O sujeito passivo nessa modalidade criminosa, em sua maioria, são mulheres e adolescentes do sexo feminino. Segundo a associação, 69% das vítimas, no Brasil, são meninas e mulheres e os casos podem começar de diferentes formas: alguém fingindo ter posse de conteúdos íntimos como forma de iniciar conversas e ameaças; desdobramentos de conversas sexuais, experimentações e exposições voluntárias em um suposto relacionamento online; cobranças de valores após

[9] Disponível em: <http://revistaliberdades.org.br/_upload/pdf/26/Liberdades21_Artigo01.pdf>. Acesso em 30/10/2020.

conversa sexual com mútua exposição; invasão de dispositivos para furtar conteúdos íntimos. Quando a foto ou vídeo é compartilhado com o criminoso, as vítimas são ameaçadas a enviarem mais mídias ou para participarem de encontros sexuais reais, em troca de não terem suas imagens íntimas expostas.

Os primeiros casos de grande repercussão no Brasil surgiram no Rio Grande do Sul e Piauí[11], em 2013, no qual o *modus operandi* foi o mesmo, consistente no fato do agressor possuir em seu poder fotos ou vídeos íntimos das vítimas e obrigá-las a fazer algo, sob pena de divulgação desse conteúdo.

No ordenamento jurídico pátrio, a sextorção ainda é uma conduta sem definição concreta, pois associa uma corrupção individual com um abuso, levando a obtenção de resultados sexuais ou patrimoniais.

4.2 A CLONAGEM DE WHATSAPP

A clonagem de números telefônicos e o registro de golpes com o uso do aplicativo de mensagens WhatsApp tem se tornado cada vez mais comum. Nessa modalidade de delito, criminosos clonam o número do telefone da vítima e, em seguida, sequestram a conta de WhatsApp, vindo a se passar pelos proprietários.

Ao invadir uma conta do aplicativo, o falsário acessa históricos de conversas, grupos, contatos, dados pessoais e outras informações que apenas as vítimas conhecem. Assim que parentes e amigos são identificados, golpes mais efetivos são elaborados pelos criminosos.

O Gabinete de Segurança Institucional da Presidência da República, mediante recomendação n° 01/2018 (Golpe de Clonagem de Contas do Aplicativo WhatsApp)[12], do Centro de Tratamento de Incidentes de Redes do Governo – CTIR Gov, determina algumas recomendações de prevenção, dentre elas: manter o aplicativo atualizado; proteger a conta do WhatsApp por meio da verificação em duas etapas; proteger o smartphone com senha; evitar armazenar informações

[11] Disponível em: <http://www.compromissoeatitude.org.br/jovem-comete-suicidio-depois-de-ter-fotos-intimas-vazadas-na-internet-o-globo-20112013/>. Acesso em 30/10/2020.
[12]Disponível em: <https://www.ctir.gov.br/arquivos/alertas/2018/recomendacao_2018_01_whatsapp.pdf>. Acesso em 30/10/2020.

pessoais no cartão de memória; utilizar aplicativos que apagam definitivamente os arquivos excluídos; apagar arquivos pessoais e senhas salvas quando for levar o aparelho para manutenção; não fornecer dados pessoais para confirmação em chamadas telefônicas de números desconhecidos e desconfiar de pedidos de ajuda por meio de aplicativos e redes sociais.

Nesse cenário criminoso é importante destacar que a adoção da criptografia ponta a ponta pelo WhatsApp dificultou ainda mais os procedimentos investigatórios em meios cibernéticos. Tais informações técnicas apuradas no FAQ (*Frequently Asked Questions*) do aplicativo, descrevem que as mensagens só podem ser acessadas pelo emissor e pelo destinatário, os quais possuem a chave especial necessária para destrancá-la, sendo que a cada nova mensagem enviada é atribuído um novo cadeado e uma nova chave, automaticamente[13].

4.3 A INVASÃO DE COMPUTADORES POR MEIO DO PROTOCOLO RPD

A sigla RPD vem do inglês *Remote Desktop Protocol* (Protocolo de Área de Trabalho Remota), desenvolvido pela Microsoft, permite que usuários consigam ter acesso as suas respectivas áreas de trabalhos sem que seja necessário estar fisicamente próximo a seus computadores[14].

A exploração dentro dessa ferramenta se dá devido ao *Terminal Server* e o RDP abrirem a porta 3389, tornando pública a conexão na área de trabalho remota, permitindo o acesso entre dois computadores, através de uma rede local ou da internet[15].

O aspecto mais relevante de uma exploração feita por meio do RPD é o nível de acesso que esse protocolo confere aos criminosos. Um ataque bem sucedido permite que ele acesse o equipamento no nível do sistema operacional, até mesmo como administrador, ampliando os seus acessos e o potencial impacto de suas

[13] Disponível em: <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br>. Acesso em 30/10/2020.
[14] Disponível em: < https://www.welivesecurity.com/br/2020/06/30/o-que-e-um-rdp-e-para-que-serve/>. Acesso em 30/10/2020.
[15] Disponível em: < https://www.welivesecurity.com/br/2020/06/30/o-que-e-um-rdp-e-para-que-serve/>. Acesso em 30/10/2020.

ações, utilizando essas brechas para obter lucros furtando informações e executando vazamentos de dados.

Uma execução comum desse método é por e-mail, onde o remetente transmite uma mensagem afirmando que ele invadiu seu computador e o está operando por meio do protocolo RDP. O remetente diz que um software foi instalado e que seu webcam foi usado para gravar você fazendo algo que talvez você não queira que outras pessoas saibam. O remetente fornece duas opções - envie bitcoin para suprimir o material ou não envie nada e veja o conteúdo enviado para seus contatos de e-mail e pelas suas redes sociais. Os golpistas usam listas de e-mail roubadas e outras informações de usuários vazadas para executar esse esquema em milhares de pessoas em massa[16].

5 A ATUAÇÃO DAS DELEGACIAS DE CRIMES INFORMÁTICOS

A Lei n° 12.735/12 (tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares) dispõe, em seu artigo 4°, que os Órgãos da Polícia Judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado[17].

Em contrapartida, não é possível verificar o atendimento especializado em todos os Estados brasileiros. De acordo com o SaferNet Brasil[18], o país apresenta 17 Delegacias Especializadas entre os 26 Estados e o Distrito Federal.

Apesar de grandes investimentos em sistemas informatizados e segurança da informação, a realidade tecnológica dessas instituições evolui e inova vagarosamente, fazendo com que os órgãos investigativos e judiciários não estejam adequadamente preparados para lidar com as novas modalidades criminosas no ambiente virtual. Desse modo, torna-se difícil o enfrentamento e combate dessas

[16] Disponível em: <https://bitcoin.org/pt_BR/fraudes#distribuicao-gratuita>. Acesso em 31/10/2020.
[17] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em 30/10/2020.
[18] Disponível em: <https://new.safernet.org.br/content/delegacias-cibercrimes>. Acesso em 30/10/2020.

ações delituosas, as quais desconhecem fronteiras, em um mundo politicamente fragmentado.

De acordo com dados da Assembleia Legislativa do Espírito Santo, em 2019, foram registrados 1.922 crimes cibernéticos na Delegacia de Repressão aos Crimes Cibernéticos, representando um "leve" aumento se comparado a 2018, com 1.898 ocorrências[19].

A problemática dos cibercrimes decorre de suas características que dificultam a sua prevenção, investigação, repressão e punição. Apesar da existência de tipificações penais para essas condutas danosas, é importante destacar que isso não é suficiente e não garante um combate eficaz aos crimes virtuais. Dessa forma, torna-se essencial que o Estado possua uma estrutura que possibilite investigações criminais eficazes, fazendo uso de habilidades investigativas associadas a perícia e cooperação internacional.

No cenário virtual criminoso existem diversos tipos de evidências que podem ser utilizadas como elementos probatórios do delito, ou seja, dados armazenados a fim de serem coletados e preservados para análise pericial e podem ser compostos por: documentos, e-mails, softwares maliciosos, fotos, vídeos, evidências de conexões de redes estabelecidas entre computadores ou qualquer outro tipo de dado armazenado em dispositivo físico ou digital. No caso de crimes virtuais, as evidências podem ser coletadas de qualquer dispositivo eletrônico (smartphones, discos rígidos, mídias).

No ordenamento jurídico brasileiro, não há qualquer impedimento para a utilização de provas eletrônicas, conforme descreve o art. 225, do Código Civil, de 2002: "As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão".

A vulnerabilidade e a complexidade na produção de provas exigem a nomeação de técnicos devidamente qualificados em decorrência da minuciosidade

[19] Disponível em: <https://www.al.es.gov.br/Noticia/2020/01/38682/crimes-ciberneticos-aumentam-no-es.html>. Acesso em 30/10/2020.

exigida por este tipo de perícia. Quando feita erroneamente, pode tornar a prova ilícita ou promover sua invalidação.

A investigação de um crime tecnológico busca percorrer o caminho inverso ao tomado pelo criminoso (BARRETO & BRASIL, 2016).

A cooperação direta entre as polícias não necessita de intervenção do Poder Judiciário. Entretanto, um ponto que dificulta o trabalho da investigação é a necessidade de representações judiciais, retardando as investigações.

As redes mais “obscuras” são ambientes muito atraentes aos criminosos, já que a evolução tecnológica propicia soluções que facilitam o cometimento de delitos.

É importante ressaltar que muitos desses ambientes têm por objetivo, não só o cometimento de infrações penais, mas também a troca de ensinamentos sobre a forma de atuação para a obtenção de êxito em suas empreitadas criminosas.

Nas investigações de crimes cometidos na *Dark Web*, é praticamente impossível a identificação por outro meio que não utilize de AI (Inteligência Artificial), visto que essas páginas só podem ser acessadas através de softwares específicos para navegação em ambientes criptografados e anônimos, como o TOR (*The Onion Router*), *Invisible Internet Projetct* (i2p) e *FreeNet*” (SHIMABUKURO & ABREU, 2017).

Assim como a tecnologia sofre constantes evoluções, condutas criminosas no mundo digital se inovam e necessitam ser detectadas e investigadas. Dessa forma, as redes abertas e fechadas devem ser objetos de constante monitoramento e análise, visando resultados eficientes na identificação da materialidade e autoria dessas condutas delitivas.

6 CONSIDERAÇÕES FINAIS

Não resta dúvida que a internet tem uma função extremamente importante para a vida em sociedade, tanto no trabalho, para a economia global, bem como das diversas áreas do cotidiano dos indivíduos e, cada vez mais, reafirma-se como um meio indispensável de acesso a todos.

Não obstante aos benefícios, esse ambiente virtual é cada vez mais, alvo de condutas criminosas por usuários mal intencionados, como por exemplo a extorsão, conforme tratado neste artigo.

Conclui-se que o alto índice de criminalidade cibernética está diretamente relacionado a lentidão legislativa na tratativa do tema, além das lacunas presentes nas leis existentes. Nesse contexto, a dinâmica da era da informação exige uma mudança na forma como o Direito é exercido, surgindo a necessidade de regulação jurídica das novas relações advindas dessa revolução tecnológica, que ainda está em curso, não só no Brasil, mas em nível mundial.

Ainda que o ordenamento jurídico brasileiro tenha apresentado algum avanço nos últimos anos no que concerne à criação de leis que regulem o mundo virtual, como o Marco Civil da Internet, insta ainda, a necessidade de melhor regulamentação e precisão técnica na criação de tipos penais mais específicos quanto aos crimes cibernéticos, evitando a impunidade dos agentes que praticam tais condutas ilícitas pela via da internet.

É neste sentido, que urge a necessidade de investimento e qualificação técnica dos agentes responsáveis pela persecução penal no tocante ao uso ilícito da internet e as ameaças nela existente, uma vez que os mecanismos disponíveis para a prática de crimes na rede, estão em constante atualização.

Importa ainda destacar a necessidade de políticas públicas governamentais para conscientização da sociedade brasileira sobre o bom uso dos serviços virtuais, das ameaças existentes e as maneiras de combater as práticas ilícitas, como a extorsão, alvo desse trabalho.

REFERÊNCIAS

BRASIL. **Código Civil Brasileiro de 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 25 de outubro de 2020.

_____. **Código Penal de 1890**. Disponível em:http://www.planalto.gov.br/ccivil_03/decreto/1851-1899/d847.htm. Acesso em: 25 de outubro de 2020.

_____. **Código Penal de 1940**. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm. Acesso em: 25 de outubro de 2020.

_____. **Lei nº 12.735**, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 25 de outubro de 2020.

_____. **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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 25 de outubro de 2020.

_____. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 de outubro de 2020.

_____. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 de outubro de 2020.

_____. **Recomendação CTIR Gov nº 01/2018**, de 13 de abril de 2018. Golpe de Clonagem de Contas do WhatsApp. Disponível em: <https://www.ctir.gov.br/arquivos/alertas/2018/recomendacao_2018_01_whatsapp.pdf>. Acesso em: 30 de outubro de 2020.

_____. Superior Tribunal de Justiça. **Súmula nº 96**. O crime de extorsão consuma-se independentemente da obtenção da vantagem indevida. Terceira Seção, em 03/03/1994. DJ 10.03.1994, p. 4.021. Disponível em: https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2010_7_capSumula96.pdf. Acesso em: 25 de outubro de 2020.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet.** Ed. Brasport. Rio de Janeiro, 2016.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal:** parte especial 3: crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos. 15. ed. São Paulo: Saraiva Educação, 2019.

COLLI, Maciel. **Cibercrimes.** Limites e perspectivas à investigação policial de crimes cibernéticos. Juruá Editora, 2010.

CUNHA, Rogério Sanches. **Manual de Direito Penal, Parte Especial (Arts. 121 ao 361)**. Volume único. 9ª ed. Revista ampliada e atualizada. Salvador: editora Juspodivm, 2017.

JESUS, Damásio de; ESTEFAM, André Estefam. **Direito Penal**: vol. 2. 36. ed. São Paulo: Saraiva Educação, 2020.

LÉVY, Pierre. **Cibercultura.** Trad. Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

NUCCI, Guilherme de Souza. **Curso de Direito Penal: parte especial**. 3. ed. Rio de Janeiro: Forense, 2019.

PRADO, Luiz Regis. **Tratado de Direito Penal:** parte especial: volume 2. 3. ed. Rio de Janeiro: Forense, 2019.

SHIMABUKURO, Adriana; ABREU, Melissa Garcia Blagitz de. Internet, Deep web e Dark web.In: SILVA, Ângelo Roberto Ilha da et al. (Org.). **Crimes cibernéticos:** racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017.