UNICESUMAR - CENTRO UNIVERSITÁRIO DE MARINGÁ
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

A EVOLUÇÃO DO DIREITO PENAL FRENTE ÀS NOVAS TECNOLOGIAS:
Um estudo sobre os crimes virtuais de natureza sexual

YONARA DE VASCONCELOS CAMPOS

MARINGÁ – PR
2018

YONARA DE VASCONCELOS CAMPOS

A EVOLUÇÃO DO DIREITO PENAL FRENTE ÀS NOVAS TECNOLOGIAS:

Um estudo sobre os crimes virtuais de natureza sexual

Artigo apresentado ao Curso de Graduação em Direito da UniCesumar – Centro Universitário de Maringá como requisito parcial para a obtenção do título de Bacharela em Direito sob a orientação do Prof. Ricardo da Silveira e Silva

MARINGÁ - PR

2018

YONARA DE VASCONCELOS CAMPOS

A EVOLUÇÃO DO DIREITO PENAL FRENTE ÀS NOVAS TECNOLOGIAS:

Um estudo sobre os crimes virtuais de natureza sexual

Artigo apresentado ao Curso de Graduação em Direito da UniCesumar – Centro Universitário de Maringá como requisito parcial para a obtenção do título de Bacharela em Direito, sob a orientação do Prof. Ricardo da Silveira e Silva

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____

Nome do professor – (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

SUMÁRIO:

A EVOLUÇÃO DO DIREITO PENAL FRENTE ÀS NOVAS TECNOLOGIAS:
Um estudo sobre os crimes virtuais de natureza sexual

YONARA DE VASCONCELOS CAMPOS

RESUMO

O presente estudo objetiva analisar a evolução do Direito Penal, frente às novas tecnologias. Para atingi-lo, explica a revolução tecnológica e seus efeitos positivos e negativos na vida das pessoas; aborda a evolução do direito penal diante das novas tecnologias; e discute alguns crimes virtuais de natureza sexual pouco abordados pelos doutrinadores. Como metodologia, emprega a revisão de literatura em doutrinas e legislações, que ajudem a elucidar o tema delimitado. Foi visto que não obstante a extorsão ser um crime muito antigo, as tecnologias modernas ajudaram a melhorá-lo, o que tornou possível o surgimento de diversos crimes sexuais cometidos pela internet. Criminosos roubam dinheiro de suas vítimas por meio de uma variedade de métodos, mas *hackear* mensagens de texto e *webcams* aumenta sua eficiência implacável para um tipo muito pessoal de crime: a extorsão sexual, que é a ameaça de revelar informações íntimas sobre uma vítima, caso ela não pague o chantagista com dinheiro ou favores sexuais. Do exposto conclui-se que o Direito e, consequentemente, a legislação devem evoluir para acompanhar de perto a dinâmica social, sob pena de se tornar letra morta, sem aplicabilidade aos casos concretos e sem força coercitiva.

Palavras-chave: Tecnologia da Informação. Crimes virtuais. Crimes sexuais.

THE EVOLUTION OF CRIMINAL LAW AGAINST NEW TECHNOLOGIES:
A study on virtual crimes of a sexual nature

YONARA DE VASCONCELOS CAMPOS

ABSTRACT

The present study aims to analyze the evolution of Criminal Law in relation to new technologies. To achieve this, it explains the technological revolution and its positive and negative effects on people's lives; addresses the development of criminal law in relation to new technologies; and discusses some virtual crimes of a sexual nature not addressed by the doctrinators. As methodology, it uses literature review in doctrines and legislation to help elucidate the delimited topic. It has been seen that while extortion is a very old crime, modern technologies have helped to improve it, which has made it possible for a number of sex crimes to be committed through the internet. Criminals steal money from their victims through a variety of methods, but hacking text messages and webcams increases their relentless efficiency for a very personal type of crime: sexual extortion, which is the threat of revealing intimate information about a victim if she does not pay the blackmailer with money or sexual favors. From the foregoing it is concluded that the law and, consequently, the legislation must evolve to

closely monitor the social dynamics, otherwise it will become a dead letter, without applicability to concrete cases and without coercive force

Key-words: Information Technology. Virtual Crimes. Sexual crimes.

1 INTRODUÇÃO

A Internet abriu uma plataforma paralela para comunicações, troca de informações e bens. Embora a dimensão digital possa enriquecer as experiências do homem em muitos níveis diferentes, ela acentua a vulnerabilidade a novas ameaças. Na verdade, como os mercados, os hábitos dos consumidores e as relações interpessoais evoluem dentro de arenas digitais e virtuais, o mesmo acontece com o crime.

O cibercrime é o termo mais comum para se referir à criminalidade organizada na Internet, que visa às atividades ilícitas envolvendo o uso de computadores ou tecnologia da Internet. Embora não sejam tangíveis como ataques físicos, os ataques cibernéticos podem ser tão impactantes e devastadores, como se tivessem sido cometidos fisicamente.

O presente estudo, objetiva analisar a evolução do Direito Penal, frente às novas tecnologias. Para atingi-lo, elegeu-se os seguintes objetivos específicos: explicar a revolução tecnológico e seus efeitos positivos e negativos na vida das pessoas; abordar a evolução do direito penal frente as novas tecnologias; e discutir alguns crimes virtuais de natureza sexual pouco abordados pelos doutrinadores.

O estudo se justifica e se faz relevante tendo em vista que com o advento da internet, os crimes se tornaram cada vez mais complexos e dotados de características inimagináveis quando em 1940 foi promulgado o Código Penal Brasileiro. A acessibilidade e eficiência da Internet e das tecnologias da informação no apoio à infraestrutura das instituições da sociedade também fomentam o desenvolvimento de cibercrimes e comportamentos desviantes, demandando punição exemplar por parte do Estado.

Para a realização dessa pesquisa, como metodologia, optou-se pela revisão de literatura em doutrinas e legislações que abordam o tema em análise.

2 REVOLUÇÃO TECNOLÓGICA

Em 1969, o Departamento de Defesa norte-americano, com o intuito de prevenir falhas de segurança nas comunicações oficiais, desenvolveu o primeiro modelo de rede de computadores que permitia o acesso e a transmissão de dados entre as máquinas que estivessem interligadas, tal sistema foi denominado de Arpanet. Referida rede destinava-se somente aos computadores de sedes militares, centros de tecnologia e universidades que estivessem desenvolvendo algum tipo de projeto ligado às forças armadas. Com o sucesso do sistema, o Governo dos Estados Unidos da América, no início da década de 1970, expandiu a rede para as universidades que se mostraram interessadas em estudar e desenvolver mais ainda essa rede de interligação de computadores[1].

Na década de 1980, com o desenvolvimento das pesquisas universitárias, houve uma cisão no estudo das redes de computadores militares e civis, surgindo, assim, a denominação internet. Mas isso não significou que a população civil já tivesse acesso ao sistema de modo amplo, o que somente veio a ocorrer em 1990, quando o engenheiro Tim Bernes-Lee desenvolveu o que chamou de *World Wide Web*, a rede que possuía sites mais interativos e dinâmicos e de mais fácil acesso[2].

Um pouco antes, no final da década de 1980, as indústrias norte-americana e japonesa também colaboraram para a expansão da rede mundial de computadores, uma vez que investiram na criação, desenvolvimento e produção de computadores e processadores de dados voltados para o consumo da população civil[3].

A partir de 2006, a internet passou a contar com as redes sociais. A primeira delas foi o *Orkut*, muito popular nos Estados Unidos e no Brasil. Logo após, surgiram diversas outras redes sociais, tais como o *Facebook, Instagram* e *Twitter*. Aqui se destaca, de logo, a abrangência e popularidade do *Facebook*, em especial no Brasil. Tal rede social atingiu, em janeiro de 2015, a marca de mais de um bilhão e quatrocentos milhões de usuários em todo o mundo.

1 ERCILILA, Maria; GRAEFF, Antonio. *A internet*. São Paulo: PubliFolha, 2008, p. 26

2 ERCILILA, Maria; GRAEFF, Antonio. *A internet*. São Paulo: PubliFolha, 2008, p. 26

3 TORRES, Gabriel. *Redes de computadores*. 2. ed. revisada e atualizada. Rio de Janeiro: Nova Terra, 2014, p. 228.

A internet tem assumido uma dinâmica cada vez mais interativa entre seus usuários, representada pelo que se chama Internet 2.0, onde a produção de conteúdo não fica monopolizada nos meios de comunicação formais, sendo de forma difusa.

Diversamente do que decorre de seu conceito tradicional, a internet não se trata de uma "rede de computadores", mas uma "rede de pessoas", que se interligam por meio de dispositivos eletrônicos dos mais variados, como computadores pessoais, *notebooks, smartphones, tablets* etc. O expoente dessa nova era das telecomunicações tem sido a rede social eletrônica. No contexto de uma visão mais tecnicista, os experts em tecnologia da informação Canedo, Melo, Albuquerque e Sousa[4] descrevem as atividades praticadas nas redes sociais como:

> Sites de redes sociais (SNS) permitem que os indivíduos apresentam - se com um perfil on-line para estabelecer ou manter vínculos e conexões com outros atores, construindo o que é comumente referido como o seu perfil de rede social. Além disso, as redes sociais permitem o agrupamento de indivíduos em grupos virtuais específicos. A rede social apresenta dois elementos básicos: atores (usuários que podem ser representados por um weblog, um fotolog, etc.) e conexões (relações, que são as interações ou laços sociais). As conexões de uma rede social podem ser percebidas de formas diferentes, sendo formados dinamicamente através da interação social entre os atores. Dessa forma, os atores e suas conexões sociais são semelhantes aos do mundo real, onde um grupo de amigos em um grupo social é composto de pessoas ligadas por amizade (Livre tradução).

Com a era da internet, tem-se no horizonte o surgimento de uma grande "aldeia global", na qual indivíduos de diferentes regiões têm a possibilidade de se conhecer e interagir. A democratização do acesso à tecnologia tem admitido, num mesmo espaço, famosos e anônimos, de modo que estes passaram a ter, igualmente, maiores oportunidades de ver e serem vistos. Este fenômeno tem mudado profundamente a percepção que as pessoas têm de privacidade e o que desejam que seja visto de si[5].

[4] CANEDO, Edna Dias et al. Social Networks: Security and Privacy. *The Fifth International Conference on Forensic Computer Science*, Brasília, v. 1, n. 5, 2010, p.67.

[5] PAESANI, Liliana Minardi. *Direito e Internet***:** Liberdade de Informação, Privacidade e Responsabilidade Civil. 5. ed. São Paulo: Atlas, 2012, p.22.

Em seu livro *O show do eu*, a psicóloga argentina Paula Sibilia[6] retrata o uso da internet como uma espécie de confessionário ou diário virtual, no qual o usuário relata sua vida assumindo um papel tríplice, "é ao mesmo tempo autor, narrador e personagem". Essa autobiografia, no entanto, não reflete, necessariamente, o "eu" verdadeiro, mas uma ficção do ideal que a pessoa tem de si. A personagem é construída a partir de como ela é e de como gostaria de ser vista pelos outros. Diversamente do que costumava ocorrer nos diários tradicionais, que tinham uma dinâmica mais reclusa e secreta (o autor mantinha em sigilo as informações), o "relato de si" atual tem por objetivo a autoafirmação, a ser avaliada e validada pelos demais usuários, estes motivados pela curiosidade acerca da vida cotidiana dos outros[7].

Fatos e situações que, em épocas passadas, restringiam-se ao círculo particular do indivíduo, atualmente são colocados à exposição para um número incalculável de pessoas. Quase tudo é motivo para ser noticiado e registrado, desde tarefas e pensamentos cotidianos até os eventos mais significativos, como formatura, conquista de um novo emprego, nascimento de um filho etc.

A popularização desses diários íntimos contemporâneos, que retratam a vida cotidiana, fez surgir o que a autora chama de "sociedade confidente", que busca, através da repercussão pública, obter reconhecimento e autoafirmação. O anonimato (no sentido de não ser visto) é indesejado, e somente a exibição do "eu" permite a conquista da "existência" e visibilidade. É preciso "aparecer para ser". A experiência da vida real passou a ser informatizada. Assim surge a sociedade do espetáculo, na qual o sujeito é construído a partir de do modelo que cria de si mesmo[8].

Existem diversas redes sociais para públicos e interesses específicos, como o *LinkedIn* (de perfil eminentemente profissional), *Tumblr* (publicação e compartilhamento de conteúdo cultural) *Ask.fm* (site de enquetes e perguntas) e *Par Perfeito* (rede de encontros e relacionamentos amorosos), dentre muitos outros.

6 SIBILIA, Paula. *O show do eu*: a intimidade como espetáculo. Rio de Janeiro: Nova Fronteira, 2008, p.62.

7 SIBILIA, Paula. *O show do eu*: a intimidade como espetáculo. Rio de Janeiro: Nova Fronteira, 2008, p.63.

8 SIBILIA, Paula. *O show do eu*: a intimidade como espetáculo. Rio de Janeiro: Nova Fronteira, 2008, p.63-64.

Desse modo, com a proliferação do uso das redes sociais na internet, tais páginas virtuais passaram a servir de instrumentos de comunicação, manifestação de pensamento, trocas de informações, vídeos e fotos, instrumentos estes que podem ser utilizados tanto para o bem quanto para o mal; para o desenvolvimento social ou para fins criminosos.

Inegável é a crescente adesão de pessoas à utilização da internet e das redes sociais. O barateamento do acesso, por meio da concorrência entre as empresas que prestam serviço de internet, bem como as políticas públicas de expansão da rede mundial de computadores, para municípios interioranos e escolas públicas, que o Governo Federal brasileiro tem executado desde o início dos anos 2000, podem ser apontados como os dois principais fatores de tal crescimento de acesso entre os brasileiros. De outro lado, a própria natureza humana que impõe ao homem a necessidade de se comunicar; a inteligência da espécie determina a curiosidade por aprendizado e; os atrativos comerciais podem ser indicados como motivos ligados a questões pessoais e culturais. Essas características, não somente do povo brasileiro, mas do ser humano em geral, influenciam o crescimento da utilização da internet e de todos os seus atrativos tecnológicos. Nesse contexto, Eric Schmidt e Jared Cohen afirmam:

> Na próxima década, a população virtual mundial será maior do que a da Terra. Quase todas as pessoas estarão representadas de formas múltiplas, criando comunidades vibrantes e ativas de interesses interligados que refletirão e enriquecerão a realidade. Essas conexões vão gerar uma quantidade colossal de dados – uma revolução, como alguns a chamam – e dar poder aos cidadãos de um modo nunca antes imaginado. Entretanto, apesar de tais avanços, existe um grande, porém: o impacto dessa revolução vai privar os cidadãos de grande parte do controle sobre suas informações pessoais no espaço virtual, o que terá consequências significativas no mundo físico. Isso pode até não ser uma verdade absoluta para todos os usuários, mas num nível mais amplo vai afetar e moldar o nosso mundo de forma profunda. O desafio que enfrentamos como indivíduos é determinar que medidas estamos dispostos a tomar para recuperar o controle sobre nossa privacidade e segurança[9].

[9] SCHMIDT, Eric; COHEN, Jared. *A nova era digital:* como será o futuro das pessoas, das nações e dos negócios. Tradução Ana Beatriz Rodrigues e Rogério Durst. Rio de Janeiro: Intrínseca, 2013, p. 26.

Com todas as inovações proporcionadas pela internet, a sociedade atual se tornou mais aberta, transparente e conectada, o que alargou os horizontes do conhecimento humano, dos relacionamentos interpessoais e das comunicações em geral. No entanto, ocorre o que Rodotà[10] chama de sociedade panóptica e midiática, pois o indivíduo é observado continuamente. Ao contrário do que o mesmo identifica como "homem de vidro"[11], cujas informações eram utilizadas para fins políticos, tradicionalmente por regimes nazistas e ditatoriais, atualmente a perspectiva da vigilância se "expande para cada momento da vida e se mostra como um traço próprio das relações de mercado"[12]. A exposição hoje é desejada e estimulada pela interação com outros, especialmente nas redes sociais.

Surge também, conforme já mencionado, o modismo da exibição da vida cotidiana como um espetáculo, o que aumenta os riscos de danos às privacidades decorrentes dessa exposição. Nem sempre o usuário tem a noção exata do que pode ser feito com suas informações divulgadas em ambiente no qual não possui integral controle, ficando, portanto, passível de lesão aos seus direitos.

Um número cada vez maior de pessoas e corporações estão presentes no mundo virtual e, consequentemente, envolvidos no contexto das redes sociais, de modo que a reputação online e a reputação real se confundem. Fertik e Thompson[13] ilustram diversas situações em que as pessoas estão expostas / nos diversos papéis que representam na vida / seja como estudante (cujo perfil pode ser pesquisado por professores, colegas e os pais), como profissional (visto por concorrentes, chefes e subordinados) ou como qualquer pessoa (exposto a ação de bandidos, desafetos etc.).

Assim, a utilização da internet e de suas redes sociais é uma realidade que a história da humanidade registra de modo aparentemente irreversível. A utilização

[10] RODOTÀ, Stéfano. *La vida y lãs reglas*: Entre El derecho y el no derecho. Madrid: Editorial Trotta, 2010, p.88.

[11] Expressão que provém da época do nazismo e alude ao indivíduo destituído de segredos

[12] RODOTÀ, Stéfano. *La vida y lãs reglas*: Entre El derecho y el no derecho. Madrid: Editorial Trotta, 2010, p.113

[13] 3 FERTIK, Michael et THOMPSON, David. *Wild West 2.0*.New York: American Management Association, 2010, p. 22.

desses instrumentos é cada vez maior, e ainda não há outro instrumento que possa sequer se comparar a eles, seja na finalidade, seja na abrangência.

Desse modo, tem-se a necessidade de investigar e pesquisar o modo que esses instrumentos podem ser utilizados, regulados e, se necessário e possível, limitados, no que se refere à utilização para a efetivação de crimes, dentre eles, os crimes sexuais.

3 A EVOLUÇÃO DO DIREITO PENAL FRENTE AS NOVAS TECNOLOGIAS

Não há dúvidas de que a Internet trouxe e traz benefícios a todos que fazem parte da Era da Informação, pois a maioria das tarefas realizadas em ambientes de trabalho e doméstico, exige que se faça uso de tecnologias para agilizar processos que antes eram feitos manualmente. Diante das facilidades, surgem novas práticas ilícitas, que tem como principal instrumento o computador associado à Internet, o que significa que os crimes já existentes estão sendo aperfeiçoados.

Com a era da inclusão digital e com a amplitude da Internet, tomam-se cada vez mais frequentes os casos em que os cidadãos usam da rede mundial de computadores para cometer atos ilícitos.

Segundo Crespo[14], os crimes virtuais "são os crimes praticados com auxílio de modernas tecnologias. Assim, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modi operandi".*

Os crimes cometidos pela *internet* não se restringem a crimes com o intuito de obter dados de maneira escusa, mas também os que têm a finalidade de preparar para outros crimes. De acordo com Crespo:

> [...] podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados) são delitos de risco informático ou próprios, ao passo que aquelas outras condutas que se dirigem contra bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios[15].

Os cibercrimes são, pois, comportamentos humanos lesivos a bens juridicamente tutelados, caracterizados pelo uso ou abuso da tecnologia informática,

14 CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais*. São Paulo: Saraiva, 2011, p.72.

15 CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Saraiva, 2011, p.72.

seja com o emprego de um hardware ou um *software* como instrumento, seja tendo o *hardware* ou o *software* como alvos da ação criminosa. São delitos perpetrados, na maioria das vezes, através da rede mundial de computadores e visam a atingir dados, dispositivos e sistemas informáticos[16].

Os crimes podem ser classificados em próprios, impróprios e mistos conforme será visto a seguir.

Pode-se afirmar que crimes próprios surgiram com a evolução tecnológica, são novas categorias, que facilitadas pela evolução da informática, atingem bens juridicamente protegidos. Dito de outra forma são aqueles crimes praticados com o intuito de obter dados, informações, e também aqueles que afetam o sistema. São exemplos de *cibercrimes* próprios: o acesso indevido ou abusivo a sistemas; a interceptação de dados informáticos (para obtenção, adulteração, deterioração ou destruição de dados); a interferência em sistemas informáticos (na utilização ou no funcionamento, mediante a emissão, instalação, transmissão, cancelamento, deterioração, destruição, alteração e supressão de dados); a instalação de vulnerabilidades; a violação de medidas de segurança dos sistemas; a produção, a oferta, a distribuição, a venda ou difusão de dispositivo ou programa de computador que permitam o acesso, a interceptação, a violação e a interferência em sistemas e dados informáticos[17].

Além destas, algumas condutas passam a merecer cuidados, talvez por meio de mera regulamentação, ainda que não lhes criminalizem, como, por exemplo, o caso da alteração de dados ou programas sem a causação de dano; a utilização não autorizada de programas protegidos; o uso não autorizado de um computador ou rede de computadores[18].

Os cibercrimes impróprios ou impuros são identificados pelos crimes clássicos que passam a ser perpetrados também pela internet, isto é, o computador e a rede são empregados apenas como instrumentos para a execução criminosa. Nesta

16 MORAES, Alexandre Rocha Almeida; SANTORO, Luciano de Freitas. *Direito Penal Avançado*. Curitiba: Juruá Editora, 2015, p.66.

17 MORAES, Alexandre Rocha Almeida; SANTORO, Luciano de Freitas. *Direito Penal Avançado*. Curitiba: Juruá Editora, 2015, p.67.

18 MORAES, Alexandre Rocha Almeida; SANTORO, Luciano de Freitas. *Direito Penal Avançado*. Curitiba: Juruá Editora, 2015, p.67.

categoria estão arroladas: as fraudes (estelionato ou furto mediante fraude), quando o agente utiliza-se de recursos informatizados, criando artifícios para induzir vítimas em erro; as falsificações de documentos, englobando, de acordo com a atual redação do art. 298 do Código Penal, a contrafação de cartões magnéticos; o dano (a dados ou programas ou sistemas informáticos); a espionagem e a sabotagem, além de outros delitos contra a segurança nacional; a reprodução não autorizada de programas ou produtos (com a consequente violação de obras literárias, artísticas ou científicas); a falsificação de produtos informáticos, ou seja, a reprodução de hardwares, de outros produtos e semi-condutores; as ameaças os delitos contra a honra; os delitos de opinião (incitação ao crime, apologia de crime ou criminoso); crimes sexuais, a exemplo do *revenge porn*, estupro virtual e extorsão sexual[19].

Neste caso, o que difere os crimes cometidos pela *internet* dos outros crimes é somente o espaço (ciberespaço), sendo aplicada igualmente a legislação para cada caso, conforme prevê Crespo[20]: "são os crimes praticados com auxílio de modernas tecnologias. Assim, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modi operandi".*

O crime organizado também existe na Internet, há vários criminosos que fazem uso de computadores para agir, invadindo e atacando sistemas. As quadrilhas no meio eletrônico não usam armas e nem ameaçam usuários pessoalmente, a maior arma destes criminosos é o alto conhecimento em informática e outros dispositivos relacionados. As quadrilhas geralmente são departamentalizadas, ou seja, divididas em setores, a citar: o primeiro grupo são os usuários que invadem sistemas, o segundo grupo são pessoas que entram nas empresas para roubar dados e informações importantes, se passando por pessoas que trabalham na empresa alvo, o terceiro setor é formado pelos vendedores de informações importantes, ou seja, de posse das informações, os criminosos conseguem lucrar vendendo dados pessoais (CPF, RG, fotos, vídeos, etc) e informações chaves de empresas[21].

Por fim, tem-se os crimes de informática mistos, que englobam todas aquelas ações em que o agente tem como alvo um bem juridicamente protegido diverso da

19 MORAES, Alexandre Rocha Almeida; SANTORO, Luciano de Freitas. *Direito Penal Avançado*. Curitiba: Juruá Editora, 2015, p.68.

20 CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais*. São Paulo: Saraiva, 2011, p.72.

21 VANCIM, Adriano Roberto; NEVES, Fernando Frachone. *Marco Civil da Internet***.** 2. São Paulo: Editora Mundo Jurídico, 2015, p.53.

informática, porém, o sistema de informática é ferramenta imprescindível para a sua consumação[22].

De acordo com Nakamura e Geus[23] os ataques acontecem no elo mais fraco da corrente, pois de tempos em tempos surgem os crimes da moda. Como resposta o policiamento é incrementado e inibe certo tipo de delito, assim os criminosos praticam um novo tipo de crime e o ciclo continua.

No artigo intitulado *Social Networks: Security and Privacy*[24], quatro experts em segurança da informação apontam os principais ataques verificados nas redes sociais, onde se destacam: furto de senha de acesso (para obtenção de informações sigilosas), uso de falsa identidade (também para o furto de informações, mas por meio de terceiros associados à vítima), abuso de confiança (o infrator ingressa em determinada comunidade virtual frequentada pela vítima, observa seu comportamento e atividades, persuadindo a vítima a fornecer dados), *bullying* e *cyberbullying* (insuiltos que visam a ascensão pessoal do infrator por meio de humilhação e diminuição da vítima perante terceiros), e a prática de *phishing* (o fraudador utiliza as informações coletadas nas redes sociais para, associado a outras ferramentas, como *e-mail* e mensagens instantâneas, por exemplo, instalar um aplicativo tipo *malware*, capaz de capturar e enviar ao infrator todas as informações e atividades da vítima alocadas no computador).

Quanto à motivação dos infratores, a partir das observações feitas no estudo realizado por Fertik e Thompson[25], pode-se classificá-las em quatro categorias principais: pessoal, profissional, política e psicótica.

Em todas elas as vítimas são submetidas a situações de exposição ou ameaça de revelação de fatos por meio de áudios, fotos e/ou vídeos íntimos, bem como a divulgação de informações inverídicas a seu respeito ou de seus familiares;

[22] VANCIM, Adriano Roberto; NEVES, Fernando Frachone. *Marco Civil da Internet***.** 2. São Paulo: Editora Mundo Jurídico, 2015, p.53.

[23] NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. *Segurança de redes em ambientes cooperativos*. São Paulo: Novatec, 2010, p.79.

[24] CANEDO, Edna Dias et al. Social Networks: Security and Privacy. *The Fifth International Conference on Forensic Computer Science*, Brasília, v. 1, n. 5, 2010, p. 69.

[25] THOMPSON, Robert *et al*. *Privacy on Facebook*. 2013. Disponível em: <http://www.amygrude.com/ documents/689.pdf>. Acesso em: 19 set. 2018.

montagens fraudulentas de imagens em situações vexatórias; criação de perfis de usuário falsos; furto de senha e acesso do perfil, dentre outros.

As motivações estritamente pessoais normalmente são resultado de ciúme, inveja, vingança ou puramente a prática de bullying. As vítimas costumam ser pessoas, após o término de um relacionamento amoroso ou por vingança relacionada a um fato ocorrido dentro ou fora da internet.

As situações relatadas acima muitas vezes implicam, além da invasão da privacidade da vítima, em práticas criminais, normalmente ligadas à extorsão, falsa identidade, calúnia, injúria e difamação. A primeira ocorre quando há a ameaça de que determinado conteúdo íntimo, vexatório ou secreto seja divulgado na rede social. No caso da internet, o dano se mostra ainda maior, pois não há como prever o alcance e tempo de permanência do conteúdo ilícito na internet. Com a facilidade de obtenção de imagens e vídeos, esses casos têm se mostrado um dos mais comuns, inclusive alguns deles com grande repercussão nacional.

A falsa identidade costuma ocorrer em duas situações: quando o ofensor tem a intenção de denegrir a imagem de seu desafeto, assumindo uma identidade falsa com as características e fotos da vítima (seja criando um perfil ou furtando a senha) e comportando-se de forma inadequada para diminuí-lo perante terceiros; ou quando cria um perfil falso, mas apenas pelo prazer de agir como se fosse aquela pessoa que admira.

Este último, apesar de violar os direitos de personalidade da vítima, não encontra, no Código Penal Brasileiro (Decreto-Lei nº 2.848/40), tipificação adequada no artigo 307: “Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem”. Vê-se que, sem a vantagem ou dano comprovado, somente uma interpretação extensiva da norma poderia tipificar a conduta na falsa identidade, o que deve ser considerado caso a caso. Esse é mais um dos pontos onde se faz necessária uma reforma do Código Penal, além da já realizada com o advento da Lei nº 12.737/12, que dispõe sobre a tipificação criminal de delitos informáticos, mas nada trata sobre o assunto.

Vê-se, portanto, a variedade de situações que podem comprometer a inviolabilidade da privacidade dos usuários e não usuários de redes sociais, que podem gerar repercussões nas esferas pessoal, profissional e até financeira dessas vítimas.

Passa-se agora à análise de alguns crimes de natureza sexual que ferem o direito à intimidade, cometidos pela internet.

4.1 *Revenge Porn*

O *Revenge Porn* (pornografia da vingança) envolve a distribuição de imagens ou vídeos sexualmente explícitos, sem o consentimento dos indivíduos retratados. Essas imagens são frequentemente usadas como um meio de chantagear os indivíduos a realizar atos sexuais ou continuar um relacionamento - ou apenas como um meio de prejudicar a reputação de uma pessoa e futuros relacionamentos[26].

4.2 Estupro Virtual

O estupro virtual, também conhecido como violação virtual "é o ato em que um agente constrange outra pessoa, mediante uso de violência ou grave ameaça, a praticar com ele ato libidinoso, tudo via internet"[27].

Com isso, segundo Pinheiro, o "estupro virtual" pode ocorrer em diversas situações, a saber: "quando uma pessoa, por meio da internet, WhatsApp, Skype ou mídia social, venha a constranger ou ameaçar a outra a tirar a roupa na frente de um webcam, praticar masturbação ou se fotografar pelada"[28].

Como exemplo cita-se o caso que ocorreu no Estado do Piauí em 10 de agosto de 2017 em que um homem foi preso por estupro após exigir, via internet, que sua ex - companheira lhe remetesse fotos se masturbando, sob a ameaça de vazar suas fotos íntimas na internet em caso de negativa. A vítima cedeu às ameaças do autor a princípio, no entanto, o acusado passou a fazer esse tipo de exigência reiteradamente, levando a vítima a denunciá-lo[29].

[26] PINHEIRO, Patrícia Peck. *Direito Digital***.** 6 ed. São Paulo: Saraiva, 2016, p.87.

[27] PINHEIRO, Patrícia Peck. *Direito Digital***.** 6 ed. São Paulo: Saraiva, 2016, p.87.

[28] PINHEIRO, Patrícia Peck. *Direito Digital***.** 6 ed. São Paulo: Saraiva, 2016, p.88.

[29] DIAS, Leonardo de Sales. Breves comentários sobre o crime de estupro virtual. *Revista Jus Navigandi*, Teresina, ano 23,n. 5453, 6 jun. 2018. Disponível em: <https://jus.com.br/artigos/ 65616>. Acesso em: 24 out. 2018.

Não há dúvida de que a atividade sexual *online* forçada - seja por meio de texto, animação, scripts maliciosos ou outros meios - é real; e é uma experiência traumática que pode fazer com que a vítima tenha sua fé em si mesmo, na comunidade, na plataforma ou até mesmo no próprio sexo, abalada. Assim, requer punição exemplar com vistas a desestimular essa modalidade de crime, que embora não seja novo, somente agora passou a ser alvo de atenção da comunidade jurídica.

4.3 Extorsão sexual

É uma forma de exploração sexual que emprega formas não-físicas de coerção para extorquir favores sexuais da vítima. A extorsão sexual refere-se à ampla categoria de exploração sexual na qual o abuso de poder é o meio de coerção[30].

Mídias sociais e mensagens de texto são muitas vezes a fonte do material sexual e os meios ameaçados de compartilhá-lo com os outros. Um exemplo de extorsão sexual é quando as pessoas são extorquidas com uma imagem nua de si mesmas que compartilharam com o acusado em outras épocas pela Internet. Mais tarde, o acusado passa a coagir o (a) autor (a) a prestar-lhe favores sexuais ou coagem a vítima a posar nua diante um *webcam*, dando origem à produção de material pornográfico[31].

5 CONCLUSÃO

A chantagem é um crime muito antigo e as tecnologias modernas ajudaram a melhorá-lo. Criminosos roubam dinheiro de suas vítimas através de uma variedade de métodos, mas *hackear* mensagens de texto e *webcams* aumenta sua eficiência implacável para um tipo muito pessoal de crime: a extorsão sexual, que é a ameaça de revelar informações íntimas sobre uma vítima caso ela não pague o chantagista com dinheiro ou favores sexuais.

30 PINHEIRO, Patrícia Peck. *Direito Digital***.** 6 ed. São Paulo: Saraiva, 2016, p.90.

31 PINHEIRO, Patrícia Peck. *Direito Digital***.** 6 ed. São Paulo: Saraiva, 2016, p.91.

Nesta era digital, essas informações podem incluir mensagens de texto sexuais (em inglês conhecidas como *sexts*), fotos íntimas e até vídeos. Os criminosos costumam exigir dinheiro ou favores sexuais para não divulgar essas informações, mas às vezes exigem materiais que podem comprometer ainda mais a vítima, deixando-a cada vez mais em suas mãos.

Foi visto nesse estudo que essa conduta já passou a ser punido no Brasil como crime de estupro com base no art. 213 do Código Penal.

Subsumir uma conduta afeta à era digital a uma figura típica no Código Penal é um desafio, principalmente quando se trata de uma ordem jurídica penal fundamentada no princípio da taxatividade.

Assim, nesse estudo, defende-se ser possível a perfeita adequação dos crimes sexuais (*revenge*, estupro virtual e extorsão sexual) à norma contida no art. 213 do Código Penal, ainda que se tenha conhecimento do elevado grau de conservadorismo ainda presente na doutrina pátria.

Nesse contexto, acredita - se não ser necessário criar um novo tipo penal para tipificar as condutas mencionadas nesse estudo, afinal, inserir tipos penais desnecessários no ordenamento jurídico apenas serve para obstar a concretização do Direito Penal.

O Direito e, consequentemente, a legislação devem evoluir para acompanhar de perto a dinâmica social, sob pena de se tornar letra morta, sem aplicabilidade aos casos concretos e sem força coercitiva.

É importante analisar a nova realidade da sociedade na era da internet e a constante busca de evolução que os intérpretes do Direito precisam realizar a fim de que seja possível adequar os fatos hodiernos às antigas leis.

REFERÊNCIAS

CANEDO, Edna Dias et al. Social Networks: Security and Privacy. **The Fifth International Conference on Forensic Computer Science**, Brasília, v. 1, n. 5, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

DIAS, Leonardo de Sales. Breves comentários sobre o crime de estupro virtual. **Revista Jus Navigandi**, Teresina, ano 23, n. 5453, 6 jun. 2018. Disponível em: <https://jus.com.br/artigos/ 65616>. Acesso em: 24 out. 2018.

ERCILILA, Maria; GRAEFF, Antônio. **A internet**. São Paulo: PubliFolha, 2008.

FERTIK, Michael et THOMPSON, David. **Wild West 2.0.** New York: American Management Association, 2010.

MORAES, Alexandre Rocha Almeida; SANTORO, Luciano de Freitas. **Direito Penal Avançado.** Curitiba: Juruá Editora, 2015.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2010.

PAESANI, Liliana Minardi. **Direito e Internet:** Liberdade de Informação, Privacidade e Responsabilidade Civil. 5. ed. São Paulo: Atlas, 2012.

PINHEIRO, Patrícia Peck. **Direito digital.** 6 ed. São Paulo: Saraiva, 2016.

RODOTÀ, Stéfano. **La vida y lãs reglas**: Entre El derecho y el no derecho. Madrid: Editorial Trotta, 2010.

SCHMIDT, Eric; COHEN, Jared. **A nova era digital***:* como será o futuro das pessoas, das nações e dos negócios. Tradução Ana Beatriz Rodrigues e Rogério Durst. Rio de Janeiro: Intrínseca, 2013.

SIBILIA, Paula. **O show do eu:** a intimidade como espetáculo. Rio de Janeiro: Nova Fronteira, 2008.

THOMPSON, Robert et al. **Privacy on Facebook**. 2013. Disponível em: <http://www.amygrude.com/documents/689.pdf>. Acesso em: 19 set. 2018.

TORRES, Gabriel. **Redes de computadores**. 2. ed. revisada e atualizada. Rio de Janeiro: Nova Terra, 2014.

VANCIM, Adriano Roberto; NEVES, Fernando Frachone. **Marco Civil da Internet.** 2. São Paulo: Editora Mundo Jurídico, 2015.