Revista Brasileira de Estudos Jurídicos
Centro Universitário FIPMoc
ISSN: 1809-7278 / 2358-9744

CRIMES CIBERNÉTICOS CONTRA MULHERES E O ORDENAMENTO JURÍDICO

Cinthia Danielle Pereira Rosa[1]
Dirceu Lopes Fonseca[2]
Enzo Alcântara Silva[3]
Geane Cássia Alves Sena[4]
Samuel Antônio Lima de Castilho[5]

RESUMO

O presente trabalho de conclusão de curso expõe as fragilidades do ambiente virtual (em particular para mulheres), maiores vítimas de crimes cibernéticos virtuais, uma vez que ainda não foram regulamentadas as leis para tais crimes. Tem- se por objetivo a análise dos crimes cibernéticos, como devem as pessoas ser protegidas deles, mesmo com as parcas leis que no momento podem socorrê-las, até que sejam amplamente estudados, definidos e regulamentados por lei. Esta monografia foi elaborada através da análise de posicionamentos doutrinários, leis antigas e atuais, com base em referências bibliográficas e uma abordagem dedutiva. Após a realização deste trabalho, conclui-se que a legislação da República Federativa do Brasil iniciou o processo de regulamentação do meio digital, entretanto ainda há um longo caminho a ser percorrido para a tipificação dos crimes virtuais, ora conhecidos, sendo certo que a regulamentação deverá ter em conta o pressuposto de que o estudo constante e dinâmico é a meta, por assim ser essa a forma de relação social.

[1]Graduanda em Direito. Acadêmica no Centro Universitário FIPMoc-UNIFIPMoc. ORCID: https://orcid.org/0009-0002-9294-3198. E-mail: cinthiahair89@gmail.com.
[2]Graduando em Direito. Acadêmico no Centro Universitário FIPMoc-UNIFIPMoc. ORCID: https://orcid.org/0009-0004-0684-7680. E-mail: dirceulopfon@gmail.com.
[3]Graduando em Direito. Acadêmico no Centro Universitário FIPMoc-UNIFIPMoc. ORCID: https://orcid.org/0009-0005-4521-8307. E-mail: enzoalcantara21@hotmail.com.
[4]Doutora em Linguística. Docente no Centro Universitário FIPMoc-UNIFIPMoc. ORCID: https://orcid.org/0000-0001-8122-0731. E-mail: geaneasena@gmail.com.
[5]Graduando em Direito. Acadêmico no Centro Universitário FIPMoc-UNIFIPMoc. ORCID: https://orcid.org/0009-0003-0751-4063. E-mail: samuelantoniocastilho@gmail.com.

CC BY NC ND

Palavras-chave: Meio Virtual. Cibercrimes contra mulheres. Legislação dos crimes virtuais.

CYBER CRIMES AGAINST WOMEN AND THE LEGAL ORDER

ABSTRACT

This undergraduate thesis exposes the weaknesses of the virtual environment (in particular for women), the biggest victims of virtual cybercrimes, since the laws for such crimes have not yet been regulated. The objective is to analyze the cybercrimes, how people should be protected from them, even with the few laws that can currently help them, until they are widely studied, defined and regulated by law. This monograph was prepared through the analysis of doctrinal positions, old and current laws, based on bibliographic references and a deductive approach. After structuring this work, in three sections, it is concluded that the legislation of the Federative Republic of Brazil has started the process of regulating the digital environment, however there is still a long way to go to classify virtual crimes, now known, being It is certain that regulation must always take into account the assumption that constant and dynamic study is the goal, as this is the form of social relationship.

Keywords: Virtual Environment. Cybercrimes against women. Legislation of virtual crimes.

CIBER DELITOS CONTRA LAS MUJERES Y ORDEN JURÍDICO

RESUMEN

El presente trabajo de conclusión de curso expone las fragilidades del entorno virtual (en particular para las mujeres), principales víctimas de los delitos cibernéticos, dado que aún no se han regulado las leyes para tales crímenes. Se tiene como objetivo el análisis de los delitos cibernéticos, cómo deben las personas ser protegidas de ellos, incluso con las escasas leyes que en este momento pueden socorrerlas, hasta que sean ampliamente estudiados, definidos y regulados por ley. Esta monografía fue elaborada a través del análisis de posicionamientos doctrinales, leyes antiguas y actuales, con base en referencias bibliográficas y un enfoque deductivo. Tras la realización de este trabajo, se concluye que la legislación de la República Federativa de Brasil ha iniciado el proceso de regulación del medio digital; sin embargo, aún queda un largo camino por recorrer para la tipificación de los delitos virtuales, ahora conocidos. Es cierto que la regulación deberá tener en cuenta el supuesto de que el estudio constante y dinámico es la meta, ya que esta es la forma de relación social.

Palabras clave: Entorno Virtual. Cibercrímenes contra las mujeres. Legislación sobre delitos virtuales.

CC BY NC ND

INTRODUÇÃO

O presente artigo visa analisar a prática de crimes cibernéticos pelo prisma do combate à descriminação da população feminina brasileira, abordando as atitudes jurídicas que estão sendo tomadas pelo Estado para punir tais transgressões, o que será contextualizado do surgimento à evolução da internet atual, demonstrando como essa ferramenta de comunicação de dados tornou-se instrumento facilitador de contravenções penais cibernéticas.

A análise da prática de crimes cibernéticos será feita tendo como ponto de partida a Guerra Fria (durante as décadas de 1950 a 1990), período de intensa rivalidade entre os Estados Unidos da América (EUA) e a União das Repúblicas Socialistas Soviéticas (URSS) por disputa de supremacia ideológica e tecnológica, resultando em avanços significativos em várias áreas científicas.

A seguir, pretende-se explicar de maneira didática o panorama abrangente da legislação brasileira relacionada aos crimes cibernéticos, abordando a origem das leis que regulam o meio penal cibernético atualmente. Inicialmente, serão discutidas a Leis nº 12.735 (conhecida como Lei Azeredo) e a Lei nº 12.737 (conhecida como Lei Carolina Dieckmann), ambas promulgadas em 2012. Em seguida, será demonstrado o amadurecimento do Código Penal na temática virtual ao longo dos anos, tendo como fator de destaque seu aperfeiçoamento por meio da Lei nº 13.772/18 (conhecida como Lei Rose Leonel). Por fim, será abordado o papel desempenhado pelo Decreto nº 11.491/2023 e suas implicações para cooperação internacional na regulamentação das penalidades de crimes virtuais.

A divisão deste trabalho compreenderá três seções principais, sendo a primeira seção dedicada à contextualização histórica da origem da internet, passando pelo desenvolvimento de tecnologias de comunicação de dados no território brasileiro, levando-se em conta a comercialização de dados tecnológicos fora do meio acadêmico e análise dos métodos utilizados por crackers para cometer contravenções.

A segunda seção abordará as Leis nº 12.735/12, nº 12.737/12 e nº 13.772/18, focando nos crimes cometidos contra as mulheres, abordando as primeiras tentativas de regulamentação do meio virtual e a inclusão recente do direito digital

CC BY NC ND

no Código Penal, tipificado como crimes cibernéticos.

Por fim, a terceira seção discutirá o papel do Decreto nº 11.491 de 12 de abril de 2023 e sua importância no combate dos crimes cibernéticos contra as mulheres brasileiras.

A HISTÓRIA DA INTERNET

A Era Digital transformou a forma como as pessoas utilizam a internet, tornando- a parte fundamental da vida cotidiana. Essa mudança ocorreu de maneira gradual e exponencial, estabelecendo uma nova norma global de conexão entre pessoas e com compartilhamento do conhecimento, muitas vezes restrito a uma pequena parcela da população, no ambiente virtual. A origem da rede mundial de computadores remonta à década de 1957, durante o período da Guerra Fria, quando os Estados Unidos e a União Soviética competiam em várias frentes, incluindo a tecnológica, e, em meio a esse contexto, surgiu a necessidade de criar um sistema digital para proteger informações governamentais críticas.

O primeiro passo em direção à criação de uma rede mundial de computadores ocorreu em 1958, com o estabelecimento da Agência de Projetos de Pesquisa Avançada de Defesa dos Estados Unidos (DARPA), focada em pesquisa e desenvolvimento de tecnologias de defesa militar (Leiner *et al*.,1997). Depois, em 1962, o cientista da computação Joseph Licklider, do Instituto de Tecnologia de Massachusetts (MIT), juntou-se à DARPA para articular a ideia de uma “rede galáctica” de computadores para comunicação de informações acessíveis a todos.

Ainda no ano de 1962, os cientistas da computação Paul Baran, Donald Davies, Lawrence Roberts e Roger Scantlebury, propuseram um sistema descentralizado de comunicação de pacotes, chamado ARPANET, que daria garantia da continuidade da comunicação mesmo ainda que uma máquina fosse comprometida (Leiner *et al*.,1997).

Em 1965, foi estabelecida a Rede de Longa Distância (WAN), permitindo a conexão de dois computadores por meio de linhas telefônicas, ainda que com baixa velocidade de transmissão, marcando um avanço na comunicação de dados. Com a criação da ARPANET entre 1966 e 1969, utilizou-se Interfaces de Processamento de

Mensagens (IMPs) para interconectar institutos de pesquisa nos Estados Unidos. A ARPANET, que tinha como objetivo inicial proteger informações sigilosas durante o período instável da guerra fria, teve seus propósitos modificados com os avanços tecnológicos e necessidades de encurtar distâncias entre institutos de tecnologia (Abbate, 1999).

Em 1971, os Protocolos de Controle de Rede (NCP) foram introduzidos, permitindo o envio e recebimento de arquivos, bem como o controle remoto de computadores. Nesse mesmo ano, Ray Tomlinson criou o *e-mail* para facilitar a troca de mensagens na ARPANE. Em 1973, a primeira conexão internacional de redes foi estabelecida, ligando a ARPANET aos sistemas da Noruega e da Inglaterra, um marco crucial para o desenvolvimento de uma rede global de comunicações (Leiner *et al*.,1997). Tais avanços tecnológicos foram fundamentais para a evolução da comunicação digital e estabeleceram as bases para a criação da internet, como a conhecemos hoje.

A fase final da criação da internet ocorreu entre os anos de 1987 e 1991, trazendo protocolos importantes como o FTP para transferência de dados, o DNS para traduzir domínios em endereços de IP, o HTTP para transferência de hipertexto, URL para identificar fontes de páginas e o HTML para a apresentação de protocolos. A combinação desses protocolos foi essencial para a criação de uma rede interconectada de envio e recebimento de dados que revolucionou a comunicação global (Dodge; Kitchin, 2001).

No ano de 1988, a rede mundial de computadores chega ao território brasileiro, sendo esse o início de uma nova era na comunicação e na interconexão digital do país, trazendo consigo mudanças significativas na forma como as pessoas se comunicavam e acessavam informações (Castells, 2013).

A internet fez sua estreia no Brasil como uma ferramenta voltada principalmente para conectar centros acadêmicos de pesquisa com o objetivo de compartilhar informações, dados e recursos de forma mais eficiente. A conexão entre centros de pesquisa foi muito importante para o avanço da colaboração científica e tecnológica no país, permitindo a troca de conhecimento e a realização de projetos, em conjunto com instituições estrangeiras (Castells, 2013).

No ano seguinte, em 1989, o governo brasileiro custeou, por meio do

CC BY NC ND

Conselho Nacional de Desenvolvimento Científico e Tecnológico, a estrutura originária de tráfego de dados do Brasil (Lins, 2013). Isso se configurou como um marco da internet no território brasileiro, com foco inicial em atividades acadêmicas e de pesquisa.

A internet continuou sendo desenvolvida ao longo do tempo e, nos anos de 1994 e 1995, foram criados os navegadores, os quais serviam como ferramentas para acessar domínios de sites. Foi nesse momento que a internet deixou de ser de uso restrito acadêmico, sendo disponibilizada para a população em geral e podendo ser comercializada, tendo sido registrado o primeiro domínio comercial brasileiro no ano de 1995 (Lins, 2013). No entanto, com o surgimento da possibilidade de ganho monetário por meio da internet, também surgiu a possibilidade do cometimento de atos maliciosos para se ter lucro de forma ilegítima, utilizando-se da rede brasileira de computadores, que ainda não havia sido regulamentada no âmbito criminal.

A criação da Rede Mundial de Computadores possibilitou aos cidadãos brasileiros a capacidade de interagir virtualmente de forma rápida e eficaz. Porém, a criação da internet não trouxe apenas avanços positivos para a sociedade, trouxe também alguns aspectos negativos devido à possibilidade de comercialização por meio virtual e, sem regulamentação da rede virtual brasileira, proliferou-se um "enxame" de condutas maliciosas, tornando-a caótica (Bononi, 2021).

Os crimes cibernéticos englobam uma ampla gama de transgressões na esfera digital, podendo ser classificados em delitos quando o computador for a ferramenta utilizada para a execução do crime, sem provocar lesão ao bem jurídico-delitos nos quais a inviolabilidade dos dados e outro bem jurídico são lesados; delitos que sirvam como meio para realizar outro delito e delitos em que apenas os dados são afetados (Bononi, 2021). É fundamental compreender essas diferentes categorias para uma eficaz abordagem legal e regulamentação no ambiente virtual, visando proteger os direitos individuais e coletivos dos cidadãos.

As modalidades de crimes que ocorrem no meio digital ou que utilizam alguma ferramenta virtual para serem realizadas estão diretamente relacionadas à insegurança na internet. Nesse ambiente, indivíduos inexperientes tornam-se possíveis vítimas de fraudes as quais ocorrerem na forma *phishing*, que utiliza links maliciosos, frequentemente, disseminados por meio de *spams* em *e-mails* e *SMSs*,

CC BY NC ND

para redirecionar a vítima para um site malicioso, com o objetivo de roubar dados pessoais (Mitnick; Simon, 2005).

Outros métodos de transgressão da lei no meio virtual são a espionagem por meio de programas maliciosos como *Spywares*, que permitem ao *cracker* acesso aos dados presentes na máquina, às informações digitadas e a sistemas de *webcam*. Com sequestro de dados e informações pessoais presentes em uma máquina, os dados são criptografados e apenas o criador do *malware* possui a chave de descriptografia, exigindo pagamento, normalmente via *bitcoin* por ser difícil de rastrear, para devolver a máquina ao seu estado original, sem ter causado danos ao software da máquina por meio de *Bootkits* programados para excluir o sistema operacional (Grow *et al*., 2018).

No ano de 2012, ocorreu um caso que despertou a atenção da população brasileira e fez com que houvesse uma grande comoção na mídia. Esse fato ficou conhecido como o "caso Carolina Dieckmann". E, devido à sua gravidade, no dia 30 de novembro de 2012, as Leis nº 12.735/2012 e nº 12.737/2012 foram sancionadas, recebendo esta última lei o apelido de "Lei Carolina Dieckmann", com a qual foi acrescentado ao Código Penal Brasileiro o crime de invasão de dispositivo informático, isto é, celulares, notebooks, tablets, entre outros (Nascimento, 2016).

É mister mencionar que, no Brasil, a situação vivenciada por Carolina Dieckmann, atriz brasileira que teve fotos íntimas divulgadas na internet, após crackers terem invadido o seu e-mail, foi considerada o grande caso de crime cibernético praticado contra mulher. Ainda, vale destacar que esse ocorrido evidenciou o despreparo da legislação penal brasileira acerca do assunto e a lentidão de aplicação por não conseguir acompanhar o ritmo evolutivo da tecnologia.

REGULAMENTAÇÃO DOS CRIMES VIRTUAIS NO BRASIL

A Pornografia de vingança (revenge porn) é o crime cibernético mais conhecido. Nesse delito o autor, geralmente, é alguém com quem a vítima teve uma relação afetiva ou vínculo emocional que, após o rompimento do vínculo, compartilha vídeos e fotos íntimas da vítima como forma de prejudicar e humilhar o ex-companheiro (o). Essas imagens e vídeos são normalmente divulgadas nas

CC BY NC ND

redes sociais para que as pessoas, de forma geral (tanto as do círculo social do ex-casal como as demais), possam ver o registro, gerando assim constrangimento para a vítima, podendo inclusive atrapalhar a vida profissional da vítima. Esse tipo de crime revela aspectos preocupantes das relações interpessoais no ambiente digital e da necessidade de políticas públicas e medidas legais para coibir tais práticas (Silva, 2022).

Os crimes cibernéticos (ou cibercrimes) surgiram com o advento da internet e estão cada vez mais presentes nos noticiários do mundo inteiro, principalmente aqueles praticados contra mulheres. No Brasil, os crimes cibernéticos praticados contra as mulheres foram mais difundidos após o "caso Carolina Dieckmann", ocorrido em 2011, quando a atriz teve sua intimidade violada por um grupo de *crackers* que conseguiram invadir seu computador pessoal e extrair 36 (trinta e seis) imagens íntimas. Antes de divulgarem as fotos de Carolina Dieckmann, os criminosos a ameaçaram, exigindo que ela pagasse uma determinada quantia monetária. Pelo fato da vítima ter se negado a fazer o pagamento do valor exigido pelos criminosos, suas imagens foram amplamente divulgadas nas redes sociais.

Como exposto no livro “Caiu na net” da doutora e mestra em Antropologia Social Beatriz Accioly Lins, a jornalista Rose Leonel, uma das mulheres entrevistadas no livro, foi uma das vítimas da pornografia de vingança, entre os anos de 2005 e 2013. O ex- companheiro de Rose Leonel contratou um técnico para manipular diversas imagens da jornalista nua, utilizando de *deepfake*, isto é, de inteligência artificial para trocar o rosto de uma pessoa por outra e colocar em filmes, vídeos e/ou fotos da pessoa, no lugar de atrizes de filmes de entretenimento adulto, criando-se assim uma espécie de portfólio misturando fotos íntimas reais com as fotos manipuladas, que foram divulgadas através de um e-mail, com remetente anônimo, além de colocar todo esse material em CDs e distribuir na rua (Lins, 2021).

Depois do "caso Rose Leonel", a divulgação de imagens íntimas, sem permissão que a pessoa, tornou-se crime no Código Penal (CP/40), por meio da Lei nº. 13.772/18 (apelidada de Lei Rose Leonel), passando a ser crime o registro, não autorizado, de fotos e/ou vídeos íntimos. Essa legislação foi complementada pela Lei 13.718/18, que criminalizou a divulgação de cena sexo sem o consentimento de

CC BY NC ND

ambas as partes (Lins, 2021). Vale mencionar que essas leis representam um avanço significativo na proteção dos direitos das vítimas de pornografia de vingança e refletem a necessidade de uma abordagem legal mais abrangente e eficaz para lidar com os crimes cibernéticos.

Além do crime de pornografia, também é importante ressaltar o crime de sextorsão, o qual é composto pela junção das palavras “sexo” e “extorsão”. Esse crime diz respeito à exigência de envio de material audiovisual erótico ou à prestação de favores sexuais para que o autor do crime não divulgue informações confidenciais da vítima, ou para que este não divulgue vídeos e/ou fotos de conteúdo íntimo que diz já possuir. De forma resumida, essa prática corresponde a uma chantagem on-line (Gonçalves, 2019).

Apesar da prática de sextorsão ser um crime amplamente reconhecido pelo ordenamento jurídico brasileiro, diferente da pornografia de vingança e do *cyberstalking*, ainda não há no Brasil uma norma jurídica específica a respeito, dependendo da interpretação jurídica para que o crime seja tipificado e, assim, o criminoso seja punido. Entretanto, é possível que esse crime seja enquadrado no crime de extorção, estupro, assédio sexual, concussão, difamação, injúri, constrangimento ilegal e assédio sexual (Gonçalves, 2019).

Em relação ao aumento de casos de crimes cibernéticos praticados contra mulheres, pode-se perceber que o Brasil deu o primeiro passo para proteção das vítimas a partir da criação das Leis Carolina Dieckmann e Rose Leonel. Mas a falta de uma lei específica acerca da sextorsão torna-se preocupante, visto que, sem uma lei específica para reger tal crime, o combate desse crime dependerá, exclusivamente, de uma interpretação de outros artigos do Código Penal para tipificar o delito de extorsão. Isso pode afetar a devida penalização do criminoso e um prejuízo na luta contra os cibercrimes praticados contra mulheres (Lins, 2021).

A SaferNet, uma organização nacional de direito privado, sem fins lucrativos, que atua no Brasil, foi fundada com o objetivo de promover a defesa dos Direitos Humanos na Internet. Ao longo dos anos, essa organização vem coletando dados acerca dos cibercrimes, principalmente contra mulheres. Segundo registros do Canal

CC BY NC ND

de Ajuda da SaferNet, os pedidos de ajuda referentes a vazamentos ou ameaças de vazamentos tiveram um grande crescimento entre os anos de 2007 e 2017 (SaferNet, 2017).

Outro crime que ocorre no meio digital é o *cyberstalking*- é uma modalidade do crime de *stalking*, facilitada pelo grande uso das redes sociais. Nesse crime, o agente perseguidor, geralmente, é alguém que conhece a vítima ou é ou foi de convívio dela. Na maioria das vezes, os *stalkers* são ex-parceiros íntimos, que desenvolvem um sentimento de posse sobre o corpo da mulher, estes se utilizam das redes sociais, e-mails e SMSs para realizar o crime. Esse tipo de delito ocorre quando a vítima é perseguida de forma ferrenha, tendo sua liberdade tanto física quanto emocional restrita. Através da perseguição digital, o autor começa a enviar mensagens nas redes sociais, ameaçando sua integridade física e psicológica, buscando denegrir a mesma (Silva, 2022).

É importante ponderar que, apesar do *cyberstalking* ser recorrente, no Brasil ainda existe uma lacuna na legislação específica para tratar desse crime, e a falta de normativas claras dificulta a punição eficaz dos criminosos e a proteção adequada das vítimas. Nesse sentido, é crucial que haja uma atualização das leis e uma conscientização sobre a gravidade desse tipo de violência digital, a fim de garantir a segurança e a integridade das pessoas no ambiente online.

Ademais, o cyberstalking deve ser levado a sério desde o começo das ameaças, pois, caso não seja, as consequências podem envolver tanto a vítima quanto os seus familiares. Alguns stalkers podem agir com violência contra a vítima e seus familiares, com a prática, por exemplo, de cárcere privado, sequestro, espacamento, tortura, homicídio, estupro, entre outros (Silva, 2022). Visando proteção às vítimas, foi sancionada em 2021 a lei que tipifica o crime de *stalking*, alterando o Decreto-Lei nº. 3.914, de 1941 do Código Penal, acrescentando o Artigo 147-A, que descreve as características que compõem o referido crime.

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa (Brasil,1940).

CC BY NC ND

Outra prática de crime cibernético bastante empregada é o Catfishing, que corresponde à utilização de contas falsas buscando esconder a real identidade do autor. O criminoso utiliza essa estratégia para enviar ameaças e chantagens anônimas, visando subjugar a vítima ou causar-lhe medo. Além disso, o *catfisher* busca afetar a vida pessoal e profissional da vítima por meio de boatos e divulgações, minando assim sua liberdade (Castro; Zaganelli, 2020). Essa técnica ilustra como a identidade digital falsa pode ser utilizada para perpetrar crimes e atingir indivíduos de forma devastadora.

Além do *Catfishing*, existe outra possibilidade, o agressor pode lançar mão do *Stalkware*, que é um programa malicioso capaz de permitir ao stalker localizar a vítima, gravar o áudio de suas conversas, acessar o histórico de navegação e muito mais. Esse tipo de software representa uma grave ameaça à privacidade e à segurança das pessoas tanto no ambiente virtual como no real, evidenciando a necessidade urgente de medidas eficazes para combater essas práticas criminosas e proteger os indivíduos contra esse tipo de violação (Grow *et al*., 2018).

Como é possível observar, o surgimento de crimes cibernéticos levou o governo brasileiro a iniciar um processo de regulamentação da internet, de forma que o primeiro passo foi a criação da Lei nº. 12.735/2012, mais conhecida como Lei Azeredo, que alterou os decretos: Decreto- Lei nº 2.848 do Código Penal (CP/40), promulgado em 7 de dezembro de 194, Decreto- Lei nº 1.001, de 21 de outubro de 1969, do Código Penal Militar (CPM/69) e a Lei nº 7.716 de 5 janeiro de 1989.

> 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, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências (Brasil, 2012).

Essa lei foi proposta em 1999, entretanto, por meio da ementa supracitada, alguns artigos que não condiziam com o direito à liberdade de expressão da população foram vetados e estabelecido, em seu quarto artigo, os setores da polícia judiciária especializados no combate aos delitos em redes de computadores, dispositivos de comunicação ou sistemas informatizados.

CC BY NC ND

> Art. 4º 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 (Brasil, 2012).

Pouco tempo depois da criação da Lei nº. 12.735/2012, foi criada a Lei nº. 12.737/2012, também conhecida como “Lei Carolina Dieckmann”, que foi a primeira lei brasileira a tipificar criminalmente delitos informáticos cometidos no meio cibernético. Esta última lei incluiu ao Código Penal brasileiro os artigos 154-A, que trata da invasão de dispositivos informáticos, e a 154-B, que estabelece as condições para procedimentos legais, sendo necessário um processo de representação, a menos que o crime seja cometido contra a administração pública ou empresas concessionárias de serviços públicos. Vale ressaltar que essa lei foi o estopim para a revolução na forma de legislar sobre o meio digital.

> Art.154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (Brasil, 2012).

> Art.154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012)

Portanto, essas leis forneceram a base legal necessária para lidar com as primeiras tipificações de crimes digitais no Brasil. Todavia, elas não foram as únicas “peças” na composição do direito digital brasileiro. É importante lembrar que a Convenção de Budapeste também foi um marco no combate aos crimes virtuais, uma vez que expandiu a área de influência do direito virtual para fora das fronteiras brasileiras. Essa convenção reuniu diversos países na cidade de Budapeste, para deliberar sobre a regulamentação dos crimes virtuais e sobre o apoio entre países membros no combate a essas transgressões.

O APOIO INTERNACIONAL NO COMBATE AOS CRIMES VIRTUAIS

CC BY NC ND

A Convenção de Budapeste, formalmente adotada como o Decreto nº 11.491, de 12 de abril de 2023 no Brasil, é um acordo internacional estabelecido para combater crimes cibernéticos, tratando-se da primeira convenção internacional que busca padronizar as legislações acerca dos crimes virtuais dos países membros, promovendo a cooperação global para investigar e penalizar atividades ilegais na internet. Essa convenção aborda aspectos essenciais, como a definição de crimes digitais, a harmonização de políticas de segurança cibernética e a facilitação da troca de informações entre nações, sendo um marco crucial para a proteção contra crimes virtuais, especialmente os direcionados a grupos vulneráveis, como as mulheres.

A Convenção de Budapeste, em seu primeiro artigo, estabelece conceitos para os termos utilizados no meio digital, como sistema de computadores, dados de computador, provedores de serviços e dados de tráfego. Dados de computador referem- se a qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador, incluindo um programa capaz de fazer o sistema realizar uma tarefa; provedor de serviços é qualquer entidade pública ou privada que permite aos seus usuários se comunicarem por meio de um sistema de computador, bem como qualquer outra entidade que realize o processamento ou armazenamento de dados de computador em nome desses serviços de comunicação ou de seus usuários. Já dados de tráfego são quaisquer dados de computador referentes a uma comunicação por meio de um sistema informatizado, gerados por um computador que seja parte da cadeia de comunicação, indicando sua origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado (Brasil, 2023).

Além de definir os conceitos dos termos da informática, a Convenção de Budapeste também tipificou os tipos de transgressões virtuais, no meio penal, dos artigos segundo ao décimo primeiro. Os artigos segundo, terceiro e quarto são particularmente importantes para o desenvolvimento deste estudo, pois tratam do acesso ilegal, da interceptação ilícita e da violação de dados, que são os meios utilizados para obtenção dos dados sensíveis das mulheres brasileiras.

O Artigo 2° desse documento define o acesso ilegal como o acesso doloso e não autorizado à totalidade ou parte de um sistema de computador, cabendo aos

CC BY NC ND

países participantes o dever adotar medidas legislativas para tipificar este ato como crime em sua legislação interna. A tipificação pode incluir a exigência de violação de medidas de segurança, o objetivo de obter dados de computador ou outros objetivos fraudulentos, ou ainda, ser cometido contra um sistema de computador conectado a outro sistema (Brasil, 2023).

O Artigo 3° trata da interceptação ilícita, que é definida como a interceptação ilegal de transmissões não públicas de dados de computador para um sistema informatizado, a partir dele ou dentro dele, realizada por meios técnicos, a tipificação do crime pode incluir a exigência de que seja cometida com objetivo fraudulento ou contra um sistema de computador conectado a outro (Brasil, 2023).

O Artigo 4° aborda a violação de dados, estabelecendo que cada um dos países participantes deve adotar medidas legislativas para tipificar como crimes a danificação, eliminação, deterioração, alteração ou supressão dolosas e não autorizadas de dados de computador, sendo que a tipificação pode incluir a exigência de que a conduta resulte em sério dano para a vítima (Brasil, 2023).

Vale ressaltar que a nação brasileira se comprometeu a adotar as medidas descritas na convenção, atualizando suas leis, se necessário, para abordar adequadamente os tipos de crimes cibernéticos, garantindo, assim, que haja disposições legais claras e eficazes para lidar com essas transgressões. Além disso, o Brasil obrigou-se a cooperar com os demais países membros da convenção na investigação e no combate aos crimes cibernéticos, facilitando a extradição de suspeitos, colaborando em investigações transnacionais, resguardando, desse modo, os direitos essenciais à privacidade e à dignidade de todos os cidadãos brasileiros (Brasil, 2023).

CONSIDERAÇÕES FINAIS

Diante do exposto, verifica-se que a internet surgiu em um contexto extremamente instável da história (período da Guerra Fria, entre os anos de 1950 e 1990), no qual as duas maiores potências mundiais, daquele período, estavam disputando a supremacia ideológica e tecnológica, e que em consequência dos diversos avanços que ocorreram, desde aquela época, a rede mundial de computadores chegou em seu ápice para os dias atuais. Ademais, com a chegada e

CC BY NC ND

o desenvolvimento do meio virtual no Brasil, surgiu a possibilidade de comercialização das ferramentas e dos dados virtuais, o que permitiu que *crackres* desenvolvessem técnicas de praticar atos maliciosos.

Com o intuito de coibir a possibilidade de ganho monetário por vias eticamente questionáveis, surgiram, em novembro do ano de 2012, as Leis nº 12.735 e nº 12.737, que foram criadas após a comoção midiática gerada pelo "caso da Carolina. Dieckmann". Vale mencionar que a Lei Carolina Dieckmann (Lei nº 12.737) é uma das leis pioneiras na regulamentação dos crimes virtuais no Brasil. Juntando- se a isso, no ano de 2018, aconteceu outro caso que ganhou muita visibilidade: o "caso Rose Leonel", que foi motivo basilar para a criação da Lei nº. 13.772/18 e tornou crime o registro não autorizado de fotos e/ou vídeos íntimos.

Entretanto, analisando os dados apresentados, é possível perceber que ainda existem muitas lacunas nas leis que regulam as atividades maliciosas no meio virtual, o que se comprova pela falta de uma regulamentação específica para a prática do *cyberstalking* e da *sextorsão*. Outro fator a ser ressaltado é que o Brasil se comprometeu a seguir as normas estabelecidas pela convenção de Budapeste, validando- a por meio do Decreto nº 11.491/23. Mas, mesmo com as tipificações gerais dos crimes virtuais sendo descritas neste decreto, detecta-se a sua pouca eficácia devido à incapacidade de os órgãos policiais especializados acompanharem o ritmo no qual os crimes existentes são cometidos e novos crimes são criados.

A partir do exposto, fica evidente que é quase impossível que a regulamentação brasileira acompanhe o nível exponencial de evolução do meio virtual. Porém, faz-se necessário que o legislador se mantenha sempre atento e atualizado sobre as novas tecnologias e os métodos de cometimento de ilícitos, para regular, no melhor de suas capacidades, os crimes digitais que vitimam a população brasileira (principalmente as pessoas mais frágeis), garantindo um futuro mais seguro para todas as gerações atuais e as gerações que estão por vir.

REFERÊNCIAS

ABBATE, Janet. **Inventing the Internet.** Cambridge, MA: The MIT Press, 1999.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 mai. 2024.

BRASIL. Decreto-Lei nº. 2.848, de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940. p. 23911.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal; altera o decreto-lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. **Diário Oficial da União,** Poder Executivo, Brasília, DF, 03 dez. 2012. Seção 1, p. 1.

BRASIL. 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, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da União,** Poder Executivo, Brasília, DF, 30 dez. 2012. Seção 1, p. 1.

BRASIL. Lei nº. 13772, de 19 de dezembro de 2018. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. **Diário Oficial da União,** Poder Executivo, Brasília, DF, 20 dez. 2018. Seção 1, p. 2.

BRASIL. Decreto-Lei nº. 11.491, de 12 de abril de 2023. Convenção sobre o Crime Cibernético. **Diário Oficial da União,** Poder Executivo, Brasília, DF, 13 abr. 2023. Seção 1, p. 1.

BONONI, Fernando. **Crimes cibernéticos**: avanço legislativo no Brasil. Migalhas. 2021. Disponível em: https://www.migalhas.com.br/depeso/347513/crimesciberneticos--avanco-legislativono-brasi. Acesso em: 01 mai. 2024.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CASTRO, Ana Flavia Cera Daltro de; ZAGANELLI, Margareth Vetis. Catfishing: crime de falsa identidade? **Revista de Estudos Jurídicos UNESP**, Franca, 2020, a. 24, n. 40, p. 305-324, jul./dez. 2020. Disponível em: https://ojs.franca.unesp. br/index. php/estudosjuridicosunesp/issue/archive. Acesso em: 15 mai. 2024.

DODGE, Klaus; KITCHIN, Rob. **Mapping Cyberspace**. London: Routledge, 2001.

FACHINI, Tiago. **Lei Carolina Dieckmann**: tudo o que você precisa saber. PROJURIS. São Paulo, 5 set. 2023. Disponível em: https://www.projuris.com.br/blog/lei-carolina-dieckman-tudo-o-que-voce-precisa-saber-sobre/. Acesso em: 1 mai. 2024.

GONÇALVES, Fernada. **Sextorsão**. JusBrasil, 2019. Disponível em: https://www.jusbrasil.com.br/artigos/sextorsao/770622469. Acesso em: 1 mai. 2024.

GROW, Christopher; BROOKS, Charles; CRAIG, Philip; SHORT, Donold. **Cybersecurity Essentials**. California, Estados Unidos da America: Sybex, 2018.

LEINER, Barry; CERF, Vint; CLARK, David; KAHN, Robert; KLEINROCK, L; LYNCH, Daniel; POSTEL, Jon; ROBERTS, Lawrence; WOLFF, Stephen. **The Past and Future History of the Internet**. Mit, 01 fev. 1997. Disponível em: https://groups.csail.mit.edu/ana/Publications/PubPDFs/The%20past%20and%20future% 20history%20of%20the%20internet.pdf . Acesso em: 1 maio 2024.

LINS, Beatriz Accioly. **Caiu na net**: nudes e exposição de mulheres na internet. Rio de Janeiro: Telha, 2021.

LINS, Bernardo Felipe Estelitta. **A evolução da Internet: uma perspectiva histórica**. Belins. 2013. Disponível em: https://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf. Acesso em: 1 de mai.2024.

MITNICK, Kevin; SIMON, William. **A arte deInvadir**. Hoboken, New Jersey, Estados Unidos da América: Prentice Hall, 2005.

NASCIMENTO, Lucas Sousa do. **O Populismo Punitivo e a Lei Carolina Dieckmann**. 2016. 83 f. TCC (Graduação) - Curso de Direito, Universidade do Extremo Sul Catarinense – Unesc, Criciúma, 2016. Disponível em: https://core.ac.uk/reader/297691710. Acesso em: 10 mai. 2024.

SAFERNET BRASIL. **O que é sextorsão?**, 2017. Disponível em: https://new.safernet.org.br/content/o-que-%C3%A9-sextors%C3%A3o#. Acesso em: 1 mai. 2024.

SILVA, Mariana Almeida. **O combate ao cyberstalking no Brasil**: um estudo sobre a aplicação da Lei nº 14.132/2021. Ministério Público do Estado do Rio de Janeiro, dez. 2022. Disponível em: https://www.mprj.mp.br/documents/20184/3600511/Mariana+Almeida+da+. Acesso em: 20 mai. 2024.

CC BY NC ND