Revista CADERNO PEDAGÓGICO

REVISTA CADERNO PEDAGÓGICO – Studies Publicações Ltda.
ISSN: 1983-0882

Análise da responsabilização criminal dos criadores e propagadores de "*deep fakes*" no ordenamento jurídico brasileiro

Analysis of the criminal liability of the creators and propagators of "deep fakes" in the Brazilian legal system

Análisis de la responsabilidad penal de los creadores y propagadores de "*deep fakes*" en el ordenamiento jurídico brasileño

DOI: 10.54033/cadpedv21n6-075

Originals received: 05/10/2024
Acceptance for publication: 05/31/2024

Bruno Moraes Alves
Doutor em Direito
Instituição: Universidade Federal de Santa Catarina (UFSC)
Endereço: Sobral, Ceará, Brasil
E-mail: bruno_ma@hotmail.com

Ana Karen Vasconcelos Araújo
Pós-Graduanda em Direito Trabalhista e Previdenciário
Instituição: Faculdade Luciano Feijão (FLF)
Endereço: Sobral, Ceará, Brasil
E-mail: karenvasconcelosadv.ce@gmail.com

Juan Fonteles Cavalcante
Pós-Graduando em Direito Trabalhista e Previdenciário
Instituição: Faculdade Luciano Feijão (FLF)
Endereço: Sobral, Ceará, Brasil
E-mail: juanfontelesadv@gmail.com

Francisco Expedito Galdino Júnior
Pós-Graduando em Direito Trabalhista e Previdenciário
Instituição: Faculdade Luciano Feijão (FLF)
Endereço: Santana do Acaraú, Ceará, Brasil
E-mail: expeditogaldino@gmail.com

Luiz Henrique Lopes Rodrigues
Pós-Graduando em Direito Médico e da Saúde
Instituição: Faculdade Legale (FALEG)
Endereço: Santa Quitéria, Ceará, Brasil
E-mail: luizlopes100@gmail.com

Pedro Hygor Soares de Oliveira
Graduando em Direito
Instituição: Faculdade Luciano Feijão (FLF)
Endereço: Santa Quitéria, Ceará, Brasil
E-mail: pedrohygor03@gmail.com

RESUMO

O presente trabalho tem como objeto a investigação acerca da responsabilidade criminal dos criadores e difusores das "*deep fakes*", a qual é uma tecnologia utilizada para adulterar vídeos. Essa tecnologia vem sendo utilizada para a prática de diversos crimes, tais como a adulteração de meios de prova, a propagação de "*fake news*", a pornografia de vingança e a prática de crimes contra a honra, sendo importante averiguar se o direito brasileiro já possui meios eficazes de coibir tal conduta ou se é necessária a criação de um crime autônomo para punir a prática das "*deep fakes*". O método de abordagem utilizado para a confecção deste trabalho foi o dedutivo, e a técnica de pesquisa adotada foi a bibliográfica, através da análise de livros, artigos, notícias e legislações nas searas do Direito Penal e do Direito Digital. A conclusão obtida foi que, apesar de não existir previsão específica criminalizando a prática das "*deep fakes*", estas são utilizadas como meio de execução de outros crimes, de forma a não se fazer necessária a criação de um crime autônomo apenas para criminalizar tal conduta. Por outro lado, levando em consideração que a sensação de anonimato da internet, somada à dificuldade existente em se punir tais crimes, fazem com que os criminosos se sintam incentivados à prática de "*deep fakes*", é essencial a edição de uma qualificadora ou causa de aumento de pena para crimes praticados por intermédio dessas tecnologias. No tocante à responsabilidade dos propagadores desses vídeos falsos, se faz necessário analisar se o crime praticado por meio dessa tecnologia contempla, em seu texto, a possibilidade de punição também de seus difusores. Caso a resposta seja afirmativa, será possível a responsabilização do propagador da "*deep fake*" não somente pelo crime praticado, mas também pela qualificadora/causa de aumento de pena relativa a utilização dessa tecnologia para a prática do crime.

Palavras-chave: *Deep Fakes*. *Fake News*. Crimes Cibernéticos. Inteligência Artificial.

ABSTRACT

The purpose of this paper is to investigate the criminal liability of the creators and spreaders of "*deep fakes*", which is a technology used to tamper with videos. This technology has been used to commit various crimes, such as tampering with evidence, spreading *fake news*, revenge porn and crimes against honor, and it is important to ascertain whether Brazilian law already has effective means of curbing such conduct or whether it is necessary to create an autonomous crime to punish the practice of "*deep fakes*". The approach used to prepare this work was deductive, and the research technique adopted was bibliographical, through the analysis of books, articles, news and legislation in the fields of Criminal Law and Digital Law. The conclusion reached was that, although there is no specific

provision criminalizing the practice of "*deep fakes*", they are used as a means of executing other crimes, so there is no need to create an autonomous crime just to criminalize such conduct. On the other hand, taking into account that the feeling of anonymity on the internet, coupled with the difficulty in punishing such crimes, encourages criminals to commit "*deep fakes*", it is essential to create a penalty enhancer for crimes committed through these technologies. With regard to the responsibility of the propagators of these fake videos, it is necessary to analyze whether the crime practiced through this technology contemplates, in its text, the possibility of also punishing its disseminators. If the answer is yes, it will be possible to hold the propagator of the "*deep fake*" responsible not only for the crime committed, but also for the qualifier/cause of increase in penalty relating to the use of this technology to commit the crime.

Keywords: *Deep fakes*. *Fake news*. Cybercrime. Artificial Intelligence.

RESUMEN

El objetivo de este trabajo es investigar la responsabilidad penal de los creadores y difusores de "*deep fakes*", que es una tecnología utilizada para alterar vídeos. Esta tecnología ha sido utilizada para cometer diversos delitos, como la alteración de pruebas, la difusión de noticias falsas, el porno de venganza y los delitos contra el honor, y es importante determinar si la legislación brasileña ya cuenta con medios eficaces para frenar estas conductas o si es necesario crear un delito independiente para castigar la práctica de los *deep fakes*. El abordaje utilizado para la elaboración de este trabajo fue deductivo, y la técnica de investigación adoptada fue bibliográfica, analizando libros, artículos, noticias y legislación en las áreas de Derecho Penal y Derecho Digital. La conclusión a la que se llegó fue que, si bien no existe un precepto específico que tipifique la práctica de las "*deep fakes*", éstas son utilizadas como medio de ejecución de otros delitos, por lo que no es necesario crear un delito autónomo sólo para tipificar dichas conductas. Por otro lado, teniendo en cuenta que la sensación de anonimato en internet, unida a la dificultad de castigar este tipo de delitos, incita a los delincuentes a cometer "*deep fakes*", es imprescindible crear un agravante de pena para los delitos cometidos a través de estas tecnologías. En cuanto a la responsabilidad de los propagadores de estos vídeos falsos, es necesario analizar si el delito cometido a través de esta tecnología incluye en su texto la posibilidad de castigar también a sus propagadores. Si la respuesta es afirmativa, será posible responsabilizar al propagador del "*deep fake*" no sólo por el delito cometido, sino también por la cualificación/causa de aumento de pena relativa al uso de esta tecnología para cometer el delito.

Palabras clave: *Deep fakes*. *Fake news*. Ciberdelincuencia. Inteligencia Artificial.

1 INTRODUÇÃO

A população global presencia a Quarta Revolução Industrial, a qual possui como alguns de seus protagonistas as inteligências artificiais, os “softwares” e a nanotecnologia.

Um dos produtos desse avanço tecnológico foi a criação de “*deep fakes*”, os quais consistem na utilização de inteligência artificial para adulterar vídeos, acrescentando rostos ou falas diferentes dos originais, simulando assim a verdade.

A mencionada tecnologia, que de início tinha como principal finalidade a sátira a determinados indivíduos ou situações, está cada vez mais sendo utilizada para objetivos ilícitos, dentre os quais podemos citar a criação e propagação de “*fake news*” em época de eleições e de guerra, a “sextorsão”, o “*catfishing*” e a adulteração de meios de prova, de modo a afrontar diversos direitos previstos constitucionalmente, como o direito à honra e à imagem.

No ordenamento pátrio vigente, inexiste previsão legal expressa que criminalize, por si só, a criação ou divulgação dos “*deep fakes*”. Contudo, existem determinadas situações previstas como crime que podem ser praticadas tendo como meio de execução os “*deep fakes*”. Nesse sentido, se faz necessária uma análise das circunstâncias do caso concreto, de modo a observar se a conduta praticada por intermédio do “*deep fake*” se amolda a algum crime, devendo sempre serem observados os princípios da proibição de analogia prejudicial ao réu no direito penal e o da vedação da proteção deficiente.

O primeiro tópico se dedica a fazer um resumo sobre as revoluções industriais ao longo da história, até o momento atual, no qual se vive a Quarta Revolução Industrial. Além disso, cuida também de conceituar os crimes cibernéticos, suas espécies e principais características.

O segundo tópico, por sua vez, se destina a abordar o surgimento e a popularização das “*deep fakes*”, através do fenômeno das “*fake news*”, analisando os malefícios que essa tecnologia trouxe e a forma como o ordenamento jurídico pátrio lida com essa questão, de modo a se discutir acerca da necessidade de criação de uma legislação própria para coibir tal conduta.

No tocante à metodologia, foi utilizada a pesquisa bibliográfica, através da análise de livros, artigos e leis e notícias relativas às relações informáticas e ao direito penal, sendo utilizado o método dedutivo.

Através da análise e discussão acerca dos temas trazidos nos tópicos mencionados, o objetivo geral do presente trabalho é averiguar de que modo os agentes que criam e propagam "*deep fakes*" podem ser responsabilizados criminalmente no direito brasileiro, discutindo a necessidade – ou não – de criação de uma legislação específica para punir essa espécie de crime.

2 CRIMINALIDADE CIBERNÉTICA

A Quarta Revolução Industrial acarretou diversas mudanças no modo de viver da sociedade, sobretudo com o desenvolvimento e aperfeiçoamento da inteligência artificial.

Essa modificação na estrutura social trouxe inúmeros efeitos, tanto positivos quanto negativos. Entre os negativos, merece destaque a proliferação dos crimes praticados por meio – ou contra – sistemas informáticos, denominados "crimes cibernéticos".

Por conta disso, este tópico aborda as revoluções enfrentadas pela sociedade até chegarmos ao momento atual: a Quarta Revolução Industrial, bem como a importância da adequação do direito penal para o enfrentamento dos crimes virtuais, classificando-os e analisando suas características.

2.1 A QUARTA REVOLUÇÃO INDUSTRIAL

A sociedade vive em constante mudança, buscando sempre a criação de novos meios para facilitar o trabalho e a vida em comunidade. Por conta de tal fato, a humanidade desenvolveu, ao longo da história, diversos mecanismos, os quais acarretaram profundas mudanças na estrutura social de suas épocas.

A sociedade atual vivencia o que Schwab (2016) denomina "Quarta Revolução Industrial", que tem como característica principal o aprimoramento das inteligências artificiais e da nanotecnologia:

> Algumas dessas inovações estão em sua fase de 'infância' e ainda não mostraram todo o seu potencial. A quarta revolução industrial não se define por cada uma destas tecnologias isoladamente, mas pela convergência e sinergia entre elas. (Rosa, 2019, p. 07).

Um desdobramento marcante dessa revolução é a digitalização das relações de trabalho. Seja em e-books, em aplicativos de táxi – como o Uber – ou de músicas– a exemplo, o Spotify – a realidade é que, cada vez mais, a sociedade tem os mais diversos produtos e serviços disponíveis apenas com o acesso à internet. (Aires; Moreira; Freire, 2017)

Essa digitalização das relações humanas acabou por criar uma nova face à vida social: a dimensão virtual, ou dimensão disruptiva. Conforme Lima Filho (2021, p. 221), nessa dimensão: "Seres humanos e máquinas trabalham de forma tão estreita e similar, que às vezes se torna difícil restringir certas atividades como exclusividade de somente um dos dois, enjeitando-se o outro. "

A Quarta Revolução Industrial se diferencia das demais por três aspectos importantes: a velocidade da difusão de seus produtos; a sua profundidade, uma vez que essa revolução modifica não somente a forma de produção do mercado, mas também envolve questões políticas, econômicas e sociais; e seu impacto sistêmico, pois ele implica uma completa transformação da sociedade. (Schwab, 2016)

Sobre a velocidade com que os inventos dessa revolução se propagam, assevera Harari (2017, p. 375):

> Nos últimos dois séculos, o ritmo das mudanças se tornou tão rápido que a ordem social adquiriu um caráter dinâmico e maleável. Agora existe em um estado de fluxo permanente. Quando falamos de revoluções modernas, tendemos a pensar em 1789 (a Revolução Francesa), 1848 (as revoluções liberais) ou 1917 (a Revolução Russa). Mas o fato é que, atualmente, todo ano é revolucionário. Hoje, até mesmo uma pessoa de 30 anos pode dizer honestamente a adolescentes incrédulos: "quando eu era jovem, o mundo era completamente diferente". A internet, por exemplo, só se disseminou no início dos anos 1990, há pouco mais de vinte anos. Hoje não podemos imaginar o mundo sem ela.

Como se nota, a Quarta Revolução Industrial acarretou uma profunda mudança na estrutura social de todo o mundo.

REVISTA CADERNO PEDAGÓGICO – Studies Publicações Ltda.
ISSN: 1983-0882

O desenvolvimento dessas tecnologias, em especial a inteligência artificial e a nanotecnologia, trouxe inúmeros benefícios para a sociedade, como o acesso facilitado a diversos produtos e serviços, "veículos autônomos, impressão em 3D, nanotecnologia, biotecnologia, ciência dos materiais, armazenamento de energia e computação quântica" (Schwab, 2016, p. 15), entre outras inovações.

Entretanto, o aperfeiçoamento dessas técnicas, bem como o desenvolvimento da dimensão virtual na vida dos indivíduos abriu margem à uma nova espécie de crimes: os cibernéticos, que serão objeto de estudo dos próximos tópicos.

2.2 CARACTERÍSTICAS DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos, também denominados "crimes informáticos" ou "crimes virtuais", são aqueles praticados por intermédio das tecnologias da informática ou contra estas.

Nesse sentido, os crimes informáticos são conceituados como sendo "qualquer ação típica, antijurídica e culpável praticada por pessoa física ou jurídica, com o uso criminoso envolvendo processamento de dados e/ou transmissão de dados, sem a necessidade de conexão à internet." (Maues; Duarte; Cardoso, 2018, p. 171)

Em decorrência das inúmeras formas como a informática pode ser empregada nesses delitos, os crimes cibernéticos podem ser divididos em crimes próprios e impróprios, existindo autores que inclusive admitem a existência da modalidade mista, a exemplo de Lima Filho (2021).

Os crimes próprios, também denominados "puros" são aqueles nos quais o objetivo para a prática do crime é lesionar a própria tecnologia. Isso significa que, quando tratamos dessa espécie de crime, o bem jurídico penal a ser protegido é a própria tecnologia da informação. (Lima Filho, 2021)

Lacerda e Silva (2021, p. 15) exemplificam condutas que podem ser consideradas crimes cibernéticos próprios: "Como crimes próprios, têm-se exemplos dos vírus que invadem os sistemas para destruir informações, roubar

informações ou até mesmo danificar o aparelho, seja ele smartphones, computadores ou tablets. ”

Por outro lado, os crimes cibernéticos impróprios ou impuros são aqueles nos quais o animus de seu autor não é o ataque à tecnologia informacional, mas sim um crime diverso, previsto no ordenamento jurídico. Nessa modalidade de crime, o sistema computacional não é a “vítima”, mas sim o meio de execução do crime. (Lima Filho, 2021).

Diversas espécies de crimes podem ser praticadas por intermédio de tecnologias. Lacerda e Silva (2021, p. 15) citam alguns exemplos de delitos praticados por esse meio:

> Já crimes impróprios contempla um vasto rol, como o induzimento, instigação ou auxílio a suicídio ou a automutilação realizada por meio de redes de computadores e divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia por qualquer meio de comunicação de massa ou sistema de informática ou telemática.

Uma observação deve ser feita: os exemplos elencados pelos autores contemplam apenas crimes nos quais, em sua própria redação, existe a previsão de serem praticados por meio da rede de computadores. Entretanto, existe também a possibilidade de outras espécies de crimes serem praticadas por meio da internet.

Um exemplo seriam os crimes contra a honra, como a calúnia, a difamação e a injúria, previstos nos arts. 138 a 140 do Código Penal (Brasil, 1940). Esses delitos não possuem em sua conceituação o fato de a conduta ser praticada por intermédio da internet, tampouco elencam alguma qualificadora ou causa de aumento de pena decorrente de sua prática por meio dessa plataforma. Entretanto, é perfeitamente possível admitir a prática de um crime de, por exemplo, difamação, por meio de redes sociais.

O fato de um indivíduo publicar determinada postagem contendo informação sabidamente falsa sobre outrem, e que lhe degrade a reputação, é considerado crime de difamação, e, nesse caso, seria uma difamação praticada por meio da internet, sendo, portanto, um crime cibernético impróprio.

Essa forma de crime virtual também pode ser denominada “crime cibernético comum”, uma vez que se trata da prática de crime comum, no qual a tecnologia informacional é apenas uma forma de execução do crime, não atingindo o núcleo do tipo penal. A esse respeito, dispõe a CPI dos Crimes Cibernéticos:

> Os crimes virtuais comuns são aqueles em que os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal, constituindo-se em apenas mais um meio de execução desses delitos, tal como ocorre nos seguintes crimes, já tipificados pela lei penal: o estelionato (art. 171 do CP), a ameaça (art. 147 do CP – Código Penal), os crimes contra a honra (arts. 138 a 140 do CP), a veiculação de pornográfica infantil (art. 241-A do Estatuto da Criança e do Adolescente – Lei nº 8.069/90), o crime de violação ao direito autoral (art. 184 do CP), entre outros. (Brasil, 2016, p. 75)

É necessário ressaltar que, apesar de nos crimes cibernéticos impuros o objetivo principal do crime ser atingir outros bens jurídicos que não a tecnologia da informação, esta pode ser indiretamente lesionada. Do mesmo modo, nos crimes cibernéticos puros, apesar de a finalidade central ser lesionar computadores, tablets, softwares etc., outros bens podem ser atingidos reflexamente. (Lima Filho, 2021).

Sobre tal questão, asseveram Jesus e Milagre (2016, p. 53):

> Estas classificações podem se fundir, como, por exemplo, no delito em que um bem jurídico informático é agredido para que o agente possa cometer o crime-fim, diga-se, agredir outro bem jurídico, ou mesmo no caso em que da agressão ao bem jurídico informático outros bens também são afetados, ainda que não informáticos. Imaginemos, por exemplo, a hipótese onde o agente invade dispositivo alheio e altera informação fazendo a pessoa ser classificada como procurada pela polícia. Danos maiores podem advir.

Exemplos de crimes cibernéticos mistos seriam “a transferência ilícita de valores em uma “homebanking” ou a prática de “salemislacing” (retirada diárias de pequenas quantias em milhares de contas, também conhecida como retirada de saldo).” (Brasil, 2016, p. 75).

Deixando de lado a questão relativa à classificação dos crimes cibernéticos, deve ser analisado um outro aspecto importante referente a esses delitos: as dificuldades envolvendo a coibição dessas condutas e punição de seus agentes.

Três pontos centrais devem ser destacados: a mutabilidade das técnicas utilizadas nos crimes cibernéticos, a definição do local do crime e a identificação de sua autoria. (Lima Filho, 2021)

O primeiro empecilho apontado tem relação com o dinamismo inerente à Quarta Revolução Industrial, uma vez que, conforme exposto, essa revolução tem como uma de suas características centrais a velocidade com que as tecnologias são desenvolvidas e difundidas pelo mundo. (Schwab, 2016)

Por conta da rapidez com que a informática evolui, se torna difícil ao Poder Legislativo acompanhar tais mudanças. Tal fato faz com que existam lacunas legislativas no ordenamento jurídico, o que acarreta, por diversas vezes, a impunibilidade de condutas ilícitas praticadas por meio da internet ou do sistema informático.

A segunda dificuldade diz respeito à definição do local do crime em crimes cibernéticos (Lima Filho, 2021), bem como de qual seria a autoridade competente para julgá-los. Diferente de crimes comuns, os quais ocorrem na realidade palpável, os crimes cibernéticos ocorrem em uma outra dimensão: a virtual. Por conta disso, nem sempre é possível identificar o local em que ocorreu o crime, o que dificulta bastante a aplicação do direito ao caso concreto. (Piaia; Costa; Willers, 2019)

Um exemplo pode ser dado: se um indivíduo, no Brasil, comete um crime de estelionato contra uma pessoa que está no Chile, utilizando-se de seu aparelho celular, qual seria a lei aplicada? E qual seria o Estado competente para aplicar essa lei?

O princípio da territorialidade, adotado pelo Código Penal Brasileiro, em seu art. 5º, prevê: “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. ” (Brasil, 1940).

Desse modo, caso uma conduta, considerada crime, seja praticada no território brasileiro, deverá o agente provocador desse crime ser julgado de acordo com a lei penal brasileira.

É possível, ainda, aplicar a lei brasileira a crimes que não ocorreram no território brasileiro, hipóteses denominadas pelo Código Penal de "extraterritorialidade condicionada". Nesses casos, será necessário cumprir os requisitos estabelecidos no art. 7º do Código Penal para que se possa aplicar a lei brasileira a crime cometido no exterior. (Greco, 2017)

Todavia, quando se trata de crimes praticados por meio de redes de computador, fica difícil compreender qual seria a lei aplicável em cada caso específico. Sobre tal tema, assevera Pinheiro (2021, p. 43):

> Alguns outros princípios do Direito devem ser repensados dentro do escopo do Direito Digital, como o princípio da territorialidade. Onde fica a porta? Até onde um ordenamento jurídico tem alcance? O problema não está apenas no âmbito da Internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais.

O Código Penal, em seu art. 6º, ao tratar sobre o local do crime, adotou a teoria da ubiquidade, pela qual "considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". (Brasil, 1940)

Isso significa que, se existe alguém, "no Estado do Rio de Janeiro, que invade o computador de outrem, localizado em São Paulo, teríamos o juízo onde está o dispositivo invadido como competente para processar e julgar o delito informático". (Jesus; Milagre, 2016, p. 61)

A respeito da autoridade competente para julgar os crimes, estabelece o Código de Processo Penal que "A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução." (Brasil, 1941)

Pelo que se compreende pela análise do artigo supratranscrito, trazendo para o contexto dos crimes digitais, observa-se que a autoridade competente para julgar o crime será a do local em que ocorreu – ou deveria ter ocorrido – o

resultado do crime. Dessa forma, utilizando o exemplo anterior, se uma pessoa que está no Brasil comete um crime contra um indivíduo situado no Chile, utilizando-se de seu aparelho celular, o país competente para o julgamento será o Chile, pois é o local onde ocorreu ou deveria ocorrer o dano.

Interessante observar a ressalva que Jesus e Milagre (2016, p. 61-62) fazem a respeito da possibilidade de um crime ser praticado em determinado território, porém com a origem da conexão mascarada:

> Já no que diz respeito a condutas ilícitas praticadas em território estrangeiro, não se aplicariam as normas brasileiras, considerando a soberania do país, sendo que a questão deverá ser tratada pela extradição. Logicamente que a autoridade brasileira é competente para processar um crime digital praticado por agente brasileiro no exterior, com vítima no Brasil, mas dependerá que este agente adentre território nacional. Logo, crimes cometidos por meio de proxies, vpns, entre outros recursos para mascarar a origem da conexão, onde o agente está no Brasil e só se vale de uma conexão do exterior, podem ser processados aqui, desde que, claro, identificado o criminoso. E aí reside mais um problema, pois provedores estrangeiros muitas vezes se recusam a fornecer dados de acesso a aplicações feitas por brasileiros, mas armazenados no exterior.

Por fim, uma outra grande dificuldade que existe em relação à punição pelos crimes digitais é a dificuldade em se identificar quem é seu autor. Muitos indivíduos utilizam perfis anônimos ou mesmo falsos para causar ataques cibernéticos, o que dificulta a investigação criminal dessa espécie de crime.

A solução encontrada, atualmente, para se chegar ao autor de delitos cibernéticos é o rastreamento do IP da máquina, o que corresponderia ao endereço onde está situado o dispositivo computacional em questão.

Necessário ressaltar, ainda, que a Lei nº 12.965/14, também denominada “Marco Civil da Internet” impõe aos provedores de internet a obrigação de manter os registros de de acesso – IP’s das máquinas – por um prazo específico. (Lima Filho, 2021)

Pelo exposto nesse capítulo, se observa que a Quarta Revolução Industrial ocasionou a evolução das tecnologias informáticas, o que acarretou diversas mudanças na estrutura social, tanto positivas quanto negativas.

Uma dessas modificações foi a disseminação de crimes cibernéticos, os quais ainda encontram dificuldades no campo de aplicação da lei penal em nosso ordenamento jurídico.

3 A RESPONSABILIDADE CRIMINAL DOS CRIADORES E DIFUSORES DE *"DEEP FAKES"*

O ambiente virtual, além de dar ensejo à criação de novos tipos de crimes, próprios de seu meio, fez também com que condutas preexistentes ganhassem uma nova dimensão, ainda maior que a física. Nesse contexto, as *"fake news"* se difundiram, ganhando maior popularidade entre os internautas. Posteriormente, foram criados mecanismos tecnológicos que transformaram as *"fake news"* em algo ainda mais crível e perigoso – os *"deep fakes"*.

Nesse tópico, serão abordados a origem e os perigos que as *"fake news"*, em especial os *"deep fakes"*, podem ocasionar à sociedade. Ao final, será realizada uma análise sobre a suficiência – ou não – da atual legislação brasileira no combate a essas condutas.

3.1 O ADVENTO DAS *"FAKE NEWS"*

As *"fake news"*, ou "notícias falsas" são, como o próprio nome sugere, informações inverídicas. Com o advento e popularização da *internet*, sobretudo das redes sociais, a propagação dessas informações falsas ganhou uma dimensão aindamaior.

Antes, a divulgação de notícias era adstrita a jornais e revistas, possuindo parâmetros de controle de qualidade, de modo a assegurar a veracidade das informações divulgadas. Por outro lado, na atualidade, qualquer pessoa com acesso à *internet* pode publicar uma notícia. Do mesmo modo, indivíduos conectados ao website em que a informação foi publicada podem ter acesso a ela, independentemente de a notícia ser verdadeira ou falsa.

Essa praticidade que os meios tecnológicos trouxeram faz com que, cada vez mais, a *internet* seja sucateada com mais informações.

O problema reside no fato de que essas informações nem sempre são verídicas. Entretanto, apesar de não se tratarem de dados verdadeiros, a maior parte dos indivíduos que acessa essas informações não toma os cuidados necessários para verificar suas fontes, acabando por acreditar que o que é noticiado é a realidade. (Terra; Orsini; Abreu, 2021)

Um exemplo recente da prejudicialidade das "*fake news"* foi o que ocorreu no ápice da pandemia de COVID-19 no Brasil. No início, foram divulgadas notícias de que o vírus não seria tão prejudicial quanto os jornais alegavam, o que fez com que as pessoas não cumprissem adequadamente o isolamento social necessário. Posteriormente, com a fabricação da vacina, mais informações falsas se espalharam, dessa vez afirmando que a vacina contra o coronavírus seria prejudicialà saúde, o que acarretou atraso na vacinação contra o vírus. (Terra; Orsini; Abreu, 2021).

O resultado da massiva propagação dessas notícias falsas não poderia ser outro: "em Abril de 2019, o Brasil registrou a maior média móvel de mortes em decorrência da covid-19: cerca de 3 mil óbitos diários". (Após, 2021).

Faustino (2018) aduz que o desenvolvimento tecnológico ocasionou uma necessidade maior, por parte da população, de se manter informada de forma cada vez mais rápida, o que faz com que, de um lado, a demanda por informações cresça e, por outro, o compromisso com a realidade dos fatos caia. Isso porque os indivíduos já não têm mais tempo – nem vontade – de verificar se os fatos que estãolendo correspondem com a realidade. O simples fato de "estar por dentro" das principais notícias já basta.

Partindo desse pensamento, Faustino (2018) afirma a existência de um vínculo entre as *"fake news"* e a "pós-verdade" – termo considerado, em 2016, pelo Dicionário Oxford, como a palavra do ano – sendo a primeira uma espécie da segunda. A pós-verdade corresponderia aos motivos por trás das *"fake news"*, correspondendo à constatação de que a maior parte da população se importa menos com a realidade objetiva dos fatos do que de que forma aquela notícia apoia as suas crenças e motivações pessoais. Uma notícia falsa sobre determinado pronunciamento de um candidato teria como motivação objetivos políticos, por exemplo.

As notícias falsas são uma realidade recente, existindo desde o momento da evolução humana em que os indivíduos passaram a conseguir se comunicar, podendo desde então optar entre dizer a verdade ou uma mentira. (Nohara, 2018, *apud* Faustino, 2018)

Tal prática foi aperfeiçoada na Antiguidade Clássica, juntamente com a política e a retórica. Nessa época, foram desenvolvidas as "falácias", as quais consistiam em argumentos que, segundo o desenvolvimento lógico, deveriam ser considerados corretos, mas que eram, na realidade, uma espécie de "mentira lógica", possuindo erros em sua estrutura, sendo utilizadas para ocasionar uma lesão ao seu adversário. (Santos, 2015)

Apesar do ato de espalhar notícias falsas não ser uma criação recente, foi somente em 2016 que o termo *"fake news"* atingiu os noticiários de todo o mundo, com as eleições presidenciais dos Estados Unidos. Na época, foram divulgadas, sobretudo em redes sociais, diversas informações mentirosas a respeito dos candidatos que concorriam aos cargos governamentais. (Terra; Orsini; Abreu, 2021)

Dessa forma, "as *fake news* ganharam diversas nuances, como para fins eleitorais, através do *firehouse of falsehood*, fraudes ou simplesmente a desinformação pela desinformação, tais como correntes de *whatsapp."* (Furbino; Souza, 2021, p. 45)

As *"fake news"* podem ser enquadradas em três categorias, de acordo com sua finalidade. Dessa forma, as notícias falsas podem ter o intuito de: a) desviar a atenção da população do real problema – nesse caso, é lançada uma informação inverídica na *internet* para distrair os indivíduos, fazendo com que eles não prestem atenção em problemas relevantes e reais; b) promover determinado candidato em detrimento dos demais; e c) sucatear o leitor com um grande número de informações, de modo a fazê-lo não ter noção do que é realidade e do que é mentira. (Estabel; Luce; Santini, 2020, *apud* Terra; Orsini; Abreu, 2021)

No Brasil, não existe nenhum tipo penal específico que trate de criminalizar as *"fake news"*, existindo apenas, a depender do caso, um enquadramento dessa conduta nos crimes contra a honra. (Furbino; Souza, 2021).

> Atualmente, quem espalhar uma informação falsa pode ser punido por leis federais que não fazem referências à internet. São elas o Código Penal, de 1940, que trata de injúria, calúnia e difamação, o Código Eleitoral, de 1960, que já prevê penalidade pela divulgação de informações inverídicas, e a Lei de Segurança Nacional, de 1980, que estabelece punições apenas a quem difundir boatos que causem pânico na sociedade. (Grigori, 2018)

No entanto, existem projetos de lei em tramitação que tem como objetivo punir os criadores de *"fake news"*. "Até 2018, existiam 20 PLS impondo penalidades aos criadores de *fake news*, penalidades essas que iam desde R$1.500,00 (mil e quinhentos reais) de multa até 8 anos de reclusão." (Grigori, 2018)

Na seara cível, o Projeto de Lei de nº 7.604/2017 tem como proposta acrescentar um artigo à Lei nº 12.965/2014 (Marco Civil da Internet). Esse dispositivo teria como finalidade atribuir aos provedores de acesso à internet a responsabilidade pelas notícias falsas publicadas em seus domínios. (Faustino, 2018). Entretanto, tal artigo fere o disposto no art. 19 da mesma lei, o qual prevê queo provedor somente poderá ser responsabilizado por conteúdos publicados em seus *sites* se, após receberem ordem judicial para retirar o conteúdo, se mantiverem omissos. (Brasil, 2014)

Já na esfera criminal, o Projeto de Lei de nº 437/2017 tem como sugestão a inclusão de um novo tipo ao Código Penal, o que corresponderia ao crime de "divulgação de notícia falsa". (Faustino, 2018). A redação de tal artigo seria a seguinte:

> Art. 287-A – Divulgar notícia que sabe ser falsa e que possa distorcer, alterar ou corromper a verdade sobre informações relacionadas à saúde, à segurança pública, à economia nacional, ao processo eleitoral ou que afetem interesse público relevante.
> Pena – detenção, de seis meses a dois anos, e multa, se o fato não constitui crime mais grave.
> § 1º Se o agente pratica a conduta prevista no caput valendo-se da internet ou de outro meio que facilite a divulgação da notícia falsa:
> Pena – reclusão, de um a três anos, e multa, se o fato não constitui crime mais grave.
> § 2º A pena aumenta-se de um a dois terços, se o agente divulga a notícia falsa visando a obtenção de vantagem para si ou para outrem. (Brasil, 2017)

Como se denota pela leitura do artigo supracitado, seria exigido, para o enquadramento no crime, o prévio conhecimento de que a notícia divulgada é

falsa. Nesse caso, se um internauta compartilhar uma notícia falsa, porém acreditando que essa notícia é verdadeira, não estaria praticando nenhuma espécie de crime. Dessa forma, "aplicando termos característicos das ciências criminais ao estudo das *fake news*, o elemento subjetivo do tipo das *notícias falsas* está na conduta de reproduzir uma informação sabidamente falsa por parte daquele que a escreve." (Waldman; Horas, 2018, p. 343)

Waldman e Horas (2018) criticam a criação de um novo tipo penal apenas para criminalizar as *"fake news"*, informando que não se deve buscar solução na criação de novos crimes, uma vez que a conduta de divulgar informações falsas já estaria enquadrada em crimes já existentes – como os crimes contra a honra. Segundo o autor, a principal preocupação deveria ser encontrar instrumentos práticos para coibir e punir essas condutas no meio virtual.

O Projeto de Lei nº 215/2015, por outro lado, não busca criar um tipo novo, tampouco cita o termo *"fake news"*, mas traz uma causa de aumento de 1/3 da pena para quem cometer os crimes de injúria, calúnia e difamação através da *internet*. Atualmente, esse é o Projeto de Lei que está em fase de tramitação mais avançada, aguardando apresentação ao Plenário do Congresso Nacional. (Grigori, 2018)

Pelo exposto, observa-se que as *"fake news"* vêm ocasionando diversas mazelas para a sociedade, existindo inclusive projetos de lei com o objetivo de punir os autores dessa prática.

Entretanto, com o passar do tempo, a forma de praticar as *"fake news"* evoluiu, acarretando a criação dos *"deep fakes"*, os quais são o tema do próximo tópico.

3.2 "*DEEP FAKE*": UMA "*FAKE NEWS*" QUALIFICADA?

A evolução da tecnologia, em especial das inteligências artificiais, culminou na criação de *"deep fakes"*, os quais consistem na distorção de vídeos e imagens de modo a mascarar a verdade e a simular acontecimentos nunca ocorridos, o que por muitas vezes acaba por violar a honra e a imagem dos indivíduos que tem sua imagem utilizada sem consentimento.

A utilização de inteligência artificial para essa prática foi originariamente denominada *"fake video"*. Todavia, por ter se tornado popular graças a um usuário do Reddit, que se autodenominou "*deep fake"*, este termo se tornou a denominação utilizada para essa espécie de tecnologia. (Medon, 2021).

De acordo com Faustino (2018, p. 108): "O termo *deep fake* surge justamente pela união do termo *deep*, retirado do conceito de *deep learning* e o termo *fake* de *fake news"*.

"O termo passou então a ser associado a essa técnica, que opera a fusão de imagens em movimento, gerando um novo vídeo, cujo grau de fidedignidade é elevado a um patamar que somente com muita atenção se consegue notar se tratar de uma montagem". (Medon, 2021, p. 262)

De início, a tecnologia mencionada tinha como principal alvo a indústria cinematográfica, sendo utilizada para diversas funções, como trocar o rosto de dublês pelo rosto do ator principal, efeitos especiais etc. Nesse sentido, leciona Medon (2021, p. 269):

> A indústria cinematográfica também já se valeu desta técnica. Um dos casos mais famosos talvez tenha sido o do filme *Rogue One: Uma História Star Wars* (2016), da série homônima, quando se recriaram algumas personagens. O mais peculiar foi, sem dúvidas, o do *Comandante Tarkin*, interpretado pelo britânico Peter Cushing, pois este ator já havia falecido no ano de 1994. Valendo-se de técnicas computacionais, viabilizou-se a chamada "reconstrução digital" da imagem do já falecido ator, o que desperta questionamentos, como a necessidade de autorização dos herdeiros para a reconstrução de sua imagem. Note-se, contudo, a peculiaridade dessa situação: não se trata de reproduzir novamente imagens captadas em momento pretérito, mas de se criar novas imagens, a partir de capturas anteriores.

Conforme se observa, a princípio, os fins aos quais os *"deep fakes"* se destinavam eram completamente lícitos, auxiliando na produção de obras artísticas. Contudo, com o passar do tempo, a tecnologia foi se popularizando e se aperfeiçoando, ganhando espaço na seara humorística, motivo pelo qual começou a ser empregada para satirizar indivíduos e situações.

A utilização de *"deep fakes"* para a sátira, por si só, já gera questionamentos acerca de sua repercussão jurídica, tendo em vista que, a depender da situação concreta, pode ofender a dignidade das pessoas que aparecem nos vídeos.

Entretanto, com o passar do tempo, os *"deep fakes"* estão, cada vez mais, sendo utilizados para objetivos inquestionavelmente ilícitos, como a adulteração de vídeos de candidatos, de modo a manipular o resultado de eleições; a inserção do rosto de atrizes em vídeos pornográficos; a criação de perfis falsos para a prática de crimes e a adulteração de meios de prova.

Um exemplo de como os *"deep fakes"* podem influenciar na seara política através da propagação de notícias falsas pode ser observado abaixo:

> Outro exemplo vem de um vídeo feito por um comediante norte-americano, utilizando esta tecnologia, para alertar as pessoas acerca dos seus perigos, em que o ex-Presidente norte-americano Barack Obama aparece falando mal do então Presidente Donald Trump, a partir de uma fusão de imagens em movimento do próprio Obama, associadas à voz do comediante, que imitava o ex-presidente. No vídeo, o suposto Obama chama Donald Trump de um "total e completo idiota". A perfeição da montagem é capaz de levar pessoas desatentas à certeza inabalável de que se tratava de uma comunicação real de Obama. (Medon, 2021, p. 261)

Podemos mencionar também a recente publicação de um *"deep fake"* de Volodymyr Zelensky, atual presidente da Ucrânia, país que se encontra em guerra com a Rússia, no qual o mesmo aparece anunciando rendição ao exército russo. (Wakefield, 2022).

Nota-se, portanto, que o emprego da inteligência artificial para a criação de *"deep fakes"* pode ter impactos catastróficos, podendo influenciar totalmente o cenário político e a segurança de um Estado, pondo em risco a própria democracia.

Além disso, o aperfeiçoamento e a difusão de *"deep fakes"* também auxiliou na prática da pornografia de vingança. "Segundo pesquisa divulgada pela Deeptrace em setembro de 2019, 96% das *deepfakes* existentes à época eram pornográficas, assolando em 100% mulheres quando o conteúdo era pornográfico." (Medon, 2021, p. 261).

É de conhecimento geral que a sociedade atual, apesar dos avanços, ainda está estabelecida sobre uma estrutura eminentemente patriarcal, onde a cultura do machismo assola a vida de milhões de mulheres por todo o mundo.

A pornografia de vingança, ou *"revenge porn"* é um reflexo dessa cultura, consistindo na publicação de vídeos de conteúdo sexual sem o consentimento da pessoa que figura no vídeo – em grande parte, do sexo feminino – como forma de retaliação a determinado acontecimento.

Essa conduta, já praticada antes da popularização dos *"deep fakes"*, se agravou ainda mais com a utilização dessa tecnologia – agora os autores de pornografia de vingança não somente publicam vídeos sexuais sem o consentimento da outra parte, mas podem, inclusive, criar vídeos simulando cenas sexuais que nunca ocorreram.

Os *"deep fakes"* são considerados por Faustino (2018) uma espécie do gênero *"fake news"*, uma vez que as *"deep fakes"*, assim como as *"fake news"*, possuem o objetivo de espalhar uma informação falsa, sendo os primeiros uma versão aprimorada do segundo.

Essa tecnologia é, portanto, ainda mais perigosa que as *"fake news"* tradicionais, uma vez que, devido sua sofisticação, as *"deep fakes"* acabam por parecer muito mais reais, passando um grau de credibilidade maior: é muito mais fácil suspeitar que uma mensagem ou um texto em um *blog* seja falsa do que um vídeo.

Por conta da prejudicialidade de tal prática para a sociedade, se faz necessária que o Estado possua mecanismos para coibir e punir essa conduta.

Diante de tal fato, o próximo tópico cuidará de analisar se o ordenamento jurídico brasileiro possui tais mecanismos ou se é necessária a edição de lei específica para regular as *"deep fakes"*.

3.3 HÁ NECESSIDADE DE MODIFICAÇÃO LEGISLATIVA?

Pelo narrado, observa-se que a popularização dos *"deep fakes"* deu novas facetas à prática de diversos crimes, sendo necessário, portanto, buscar uma forma de responsabilizar criminalmente os indivíduos que praticam crimes por intermédio dessa tecnologia, de modo que se assegure a proteção da sociedade em face dessaespécie de conduta.

Todavia, por ocorrer em ambiente virtual, existem inúmeras dificuldades para que ocorra a responsabilização criminal dos criadores e difusores desses vídeos, como a inexistência de legislação específica para regular essa espécie de crime e a dificuldade de identificação dos criadores dos vídeos alterados e da dimensão que esse conteúdo pode alcançar.

A prática do "*deep fake"*, por si só, não é considerada crime no ordenamento jurídico pátrio, restando a dúvida de qual seria a forma de responsabilizar criminalmente indivíduos que cometam crimes por intermédio dessa tecnologia.

Nesse diapasão, existe um embate entre dois importantes princípios do direito penal: o da proibição da proteção deficiente e o da vedação da analogia *in malam partem*.

A vedação da proteção deficiente impõe ao Estado o dever de proteger os direitos fundamentais dos indivíduos e de garantir sua aplicação. Dessa forma, o Poder Público não somente deve abster-se de violar os direitos fundamentais de seus cidadãos, mas deve adotar condutas positivas no sentido de protegê-los contra ataques de terceiros. (Estevão; Brito Filho, 2021)

A punição dos agentes que cometem crimes por meio de *"deep fakes"* não é somente um poder do Estado, mas um dever, de modo a garantir a democracia. A esse respeito, assevera Da Costa (2011, p. 33-34):

> Miguel Reale Júnior aponta que a aplicação correta do Direito Penal e de suas sanções constituem mais que um direito, um poder do Estado, que, almejando assegurar a harmonia social, não pode deixar de atuar e deixar ao talante dos particulares sua efetividade. Se assim agisse teríamos uma capitis diminutio, com a fragilização da soberania e o surgimento de uma profunda insegurança jurídica para a sociedade, de sorte que a eficácia da norma estaria limitada ao interesse da vítima ou de sua família, gerando inclusive ao infrator uma insegurança jurídica e ao Estado uma limitação da aplicabilidade da lei.

Desse modo, é devido assegurar que os direitos previstos constitucionalmente – tais como o direito à honra e a imagem – sejam resguardados diante de práticas criminosas, como é o caso da utilização de *"deep fakes"* para violar tais bens jurídicos.

Sobre a vedação da proibição insuficiente, assevera Streck (*apud* Rudolfo, 2011, p. 117): "A proibição de proteção deficiente pode definir-se como um critério estrutural para a determinação dos direitos fundamentais, com cuja aplicação pode determinar-se se um ato estatal – por antonomásia, uma omissão viola um direito fundamental de proteção."

Por outro lado, faz-se necessário observar que o ordenamento jurídico pátrio, ao consagrar, no art. 1º do Código Penal, o princípio da legalidade, o qual prevê que "não há crime sem lei anterior que o defina nem pena sem prévia cominação legal" (Brasil, 1940), proíbe que indivíduos sejam punidos pela prática de condutas não previstas em lei como crime.

Da redação do dispositivo mencionado derivaram dois subprincípios: o da reserva legal e o da anterioridade da lei penal.

O princípio da reserva legal prevê que somente uma lei em sentido estrito poderá criar novos tipos penais, não sendo possível, por exemplo, estabelecer um novo crime através de decreto. "Assim, somente a lei, na sua concepção formal e estrita, emanada e aprovada pelo Poder Legislativo, por meio de procedimento adequado, pode criar tipos e impor penas." (Capez, 2011, p. 60).

Entretanto, a reserva legal do tipo penal incriminador não esvazia seu conceito na mera necessidade de existência de lei penal em sentido estrito para prever determinada conduta como criminosa, exigindo, também, que a redação do dispositivo que estabelecer novo crime seja clara e precisa.

No tocante ao princípio da anterioridade da lei penal, esse fixa que um indivíduo não poderá ser punido por conduta que não era considerada crime na época em que praticada, ainda que sobrevenha lei que tipifique tal conduta como crime. É o chamado "*tempus regit actum"* ou "o tempo rege o ato". (Capez, 2011)

Dessa forma, a lei penal não poderá retroagir para maleficiar o réu, seja para condená-lo por conduta que não era considerada crime quando praticada, seja para agravar a pena de determinado crime de acordo com nova legislação.

De modo diverso, é possível a aplicação de lei penal superveniente ao crime praticado antes de sua vigência, desde que essa tenha por objetivo descriminalizar aconduta ou abrandar sua pena, nos termos do art. 2º do Código Penal. (Brasil, 1940)

Um corolário desse princípio é a vedação à analogia *in malam partem* no direito penal, consistente na interpretação de uma figura típica de modo extensivo,de modo a estender a abrangência de determinado crime para outras hipóteses similares, conforme exposto por Greco (2017, p. 177):

> O princípio da legalidade veda, também, o recurso à analogia *in malam partem* para criar hipóteses que, de alguma forma, venham a prejudicar o agente, seja criando crimes, seja incluindo novas causas de aumento de pena, de circunstâncias agravantes etc. Se o fato não foi previsto expressamente pelo legislador, não pode o intérprete socorrer-se da analogia a fim de tentar abranger fatos similares aos legislados em prejuízo do agente (*nullum crimen nulla poena sine lege stricta*).

Ressalte-se que a analogia pode ser dividida em analogia legal, que ocorre quando o julgador aplica uma lei que regula determinada situação a um caso semelhante, e em jurídica, quando são aplicados princípios gerais do direito para regular determinado caso no qual inexiste previsão normativa. (Greco, 2017)

Diante da garantia de inafastabilidade da jurisdição, um juiz não pode se esquivar de julgar determinado litígio utilizando-se da premissa de inexistência de legislação que regulamente o caso. Desse modo, quando é verificada a existênciade lacuna no ordenamento jurídico, faz-se necessário o recurso à analogia, aos costumes e aos princípios gerais do direito, conforme estabelecido pela Lei de Introdução às Normas do Direito Brasileiro (LINDB): “Art. 4º Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito”. (Brasil, 1942).

Pinheiro (2021), ao abordar as especificidades do direito digital, aduz que, nessa seara jurídica, os princípios prevalecem sobre as regras, tendo em vista que a tecnologia evolui de forma infinitamente mais veloz do que a atividade legislativa.

Por conta da velocidade dessa evolução, nasce um problema jurídico: a inexistência de leis próprias que regulem as especificidades do mundo digital. A solução encontrada pelo direito digital para resolver tal impasse, segundo Pinheiro (2021) seria a utilização da analogia.

Contudo, como exposto, quando adentramos na seara penal, não é possível usar analogia, costumes ou princípios de forma a prejudicar o réu, não

podendo, portanto, aplicar determinado tipo penal à uma hipótese semelhante com o objetivo de punir determinada conduta.

Faz-se necessário analisar, então, se no ordenamento jurídico pátrio existe a possibilidade de responsabilização penal dos criadores e difusores de *"deep fakes"*, pois, caso contrário, se fará necessária a criação de um novo tipo penal com o intuito de criminalizar tal conduta.

Como informado no primeiro tópico deste trabalho, existem duas espéciesde crimes cibernéticos: os próprios e os impróprios, sendo admitido, ainda, por alguns autores, a existência de um tipo misto.

Os crimes cibernéticos próprios seriam aqueles em que o próprio bem jurídico lesado é a tecnologia da informação; os impróprios são os crimes nos quais a tecnologia é usada como um meio para a prática de crimes já existentes, e os mistos seriam aqueles em que a tecnologia da informação é, ao mesmo tempo, o bem jurídico ofendido e o meio de execução de outro crime (Lima Filho, 2021).

No caso em questão, vislumbra-se que as espécies de crime cibernético que melhor se amoldam aos *"deep fakes"* seriam a modalidade imprópria e a mista, a depender da situação. Observe duas hipóteses: a) Determinado indivíduo invadiu o computador de terceiro, obtendo para si um vídeo qualquer dessa pessoa. Posteriormente, editou esse vídeo e sobrepôs a imagem do rosto da vítima em um vídeo pornográfico, publicando-o na *internet*; b) Determinado indivíduo, que já tinha, licitamente, a posse de um vídeo de terceiro, edita essa gravação, sobrepondo a imagem do rosto da vítima em um vídeo pornográfico, e o publica na *internet*.

No primeiro caso, o agente tanto invadiu um dispositivo informático, praticando, assim, um crime cibernético próprio, tendo em vista que ocasionou dano ao bem jurídico da tecnologia informática, quanto um crime cibernético impróprio, uma vez que usou artifícios tecnológicos para editar o vídeo e ferir a honra e a imagem da vítima. Seria, nesse caso, um crime cibernético misto.

Na segunda hipótese, por outro lado, a tecnologia da informação não foi lesionada, sendo apenas um meio para a prática de determinado crime, configurando-se, portanto, como crime cibernético impróprio.

Todavia, quanto à primeira situação, já existe, em nosso ordenamento jurídico, um tipo penal para punir a conduta praticada contra o sistema informático, qual seja, o delito de invasão de dispositivo informático, previsto no art. 154-A do Código Penal, tendo sido adicionado pela Lei Carolina Dieckmann. (Brasil, 2012)

Desse modo, não se faria necessária a existência de um novo tipo penal para a punição da conduta de invadir um dispositivo informático para praticar um *"deep fake"*. A prática dos *"deep fakes"* seria, portanto, um crime cibernético impróprio, uma vez que é usada apenas como meio para a execução de outros crimes.

Diante disso, nasce a questão: deveria, então, ser proibido o procedimento de criação de *"deep fakes"*, isto é, deveria a técnica empregada para a edição desses vídeos ser criminalizada?

A resposta é negativa. Criminalizar a técnica empregada para a criação de *"deep fakes"* seria uma solução ineficiente, uma vez que, conforme explanado, as tecnologias possuem um ritmo de mudança muito mais ágil do que a lei. Desse modo, quando uma lei criminalizando determinada técnica fosse publicada, já existiriam novas formas de praticar aquela conduta, tornando-se a lei completamente ineficaz (Lima Filho, 2021).

Dessa forma, a solução mais eficiente, segundo Lima Filho (2021), seria criminalizar condutas que podem ser praticadas através dessa tecnologia, e não a tecnologia em si.

Faz-se necessário, então, averiguar se já existem, no ordenamento jurídico brasileiro, hipóteses de criminalização de condutas que podem ser praticadas por intermédio de *"deep fakes"*.

Os bens jurídicos que são lesionados quando se cria e divulga um *"deep fake"* são a imagem e a honra dos indivíduos. Em caso de *"deep fakes"* relacionadas a conteúdos pornográficos, também é lesionada a dignidade sexual das vítimas.

O Código Penal Brasileiro, em seus arts. 138, 139 e 140, já prevê a punição do indivíduo que praticar delitos contra a honra de alguém, sendo divididos em calúnia, injúria e difamação.

Desse modo, não se faz necessária a edição de um novo tipo penal apenas para prever a prática de tais crimes através da utilização de *"deep fakes"*.

Caso alguém edite um vídeo de modo a fazer parecer que determinada pessoa está praticando um crime, o editor do conteúdo terá praticado o crime de calúnia (art. 138, CP). Se, por outro lado, no vídeo falsificado, o indivíduo não estiverpraticando um crime, mas estiver praticando um ato desabonador de sua conduta, será o criador do *"deep fake"* responsabilizado pelo crime de difamação (art. 139, CP). Na hipótese de injuriar alguém através dessa tecnologia, terá praticado o crime de injúria (art. 140, CP).

Waldman e Horas (2018, p. 345), ao traçarem comentários a respeito das *"fake news"*, aduzem a desnecessidade de criação de um novo tipo penal para criminalizar tal conduta:

> Os projetos de lei que aspiram criminalizar as "*fake news*" trata o direito de forma simplita" de modo que a edição de uma nova lei não é de grande valia se aplicabilidade e meios eficientes para identificar autores. Se o direito penal já possui os delitos de difamação, calunia e injuria, seria o direito tão pobre ao ponto de criar um novo tipo penal incriminador para, especificamente, as notícias falsas que são divulgadas pela internet. Antes dos anos 2000 quando a acesso à internet não era tão popular e acessível aos brasileiros, o maior meio de comunicação era a televisão – de acordo com site brasil.gov até hoje é predominante (BRASIL, 2018) entre os brasileiros – não houve tipo penal incriminador para notícias falsas transmitidas pela televisão, levando em consideração programassensacionalistas sobre crimes e notícias (fofocas) sobre famosos. Notícias falsas sempre existiram em uma sociedade, a única mudança fora o canal que as espalham.

Pelo exposto, observa-se que não se faz necessária a edição de um novo tipo penal apenas para criminalizar as *"deep fakes"*. Entretanto, é certo que a tecnologia facilitou bastante a prática dos crimes contra a honra, bem como ampliou seus danos, uma vez que qualquer pessoa pode ter acesso ao vídeo editado, e não apenas as pessoas do círculo social da vítima – como ocorre quando tais crimes nãosão praticados por meio da *internet*.

Além disso, a dificuldade de identificação dos infratores que praticam delitos por intermédio das redes de computadores faz com que exista um incentivo para a prática dessa espécie de crimes, em detrimento de crimes que não são praticados por meio de sistemas informacionais.

Uma possível solução para coibir a prática de crimes contra a honra através da *internet* seria a criação de uma qualificadora ou uma causa de aumento de pena para os indivíduos que se utilizassem da tecnologia para executar crimes.

Ressalte-se que já existe previsão semelhante no direito brasileiro. O art. 122 do Código Penal, ao tratar do crime de induzimento, instigação ou auxílio ao suicídio ou à automutilação, prevê, em seu §4º, que "a pena é aumentada até o dobro se a conduta é realizada por meio da rede de computadores, de rede social ou transmitida em tempo real". (Brasil, 1940)

A mesma solução poderia ser aplicada no caso de *"deep fakes"*, com a previsão de um aumento de pena ou de uma qualificadora em caso de crimes contra a honra ou contra a dignidade sexual realizados por meio dessa tecnologia.

Compreendida a responsabilização criminal dos criadores de *"deep fakes"*, surge a questão: os terceiros que não adulteraram o vídeo, mas que o compartilharam, deverão também responder pelo crime?

A resposta para essa indagação vai depender da espécie de crime praticado através das *"deep fakes"*. Os crimes de difamação e injúria não contemplam previsão de responsabilidade penal dos propagadores da informação falsa.

De forma diversa, o crime de calúnia, previsto no art. 138 do Código Penal fixa, em seu §2º, que "na mesma pena incorre quem, sabendo ser falsa a informação, a propaga ou divulga." (Brasil, 1940)

Nesse caso, duas situações podem existir: a primeira quando terceiro divulga informação sabendo ser falsa, e a segunda quando a compartilha de boa-fé, sem ter conhecimento de que se trata de vídeo adulterado. Na primeira hipótese, o agente será punido com a mesma pena prevista para o criador da informação falsa. Na segunda situação, não será responsabilizado.

O mesmo raciocínio poderá ser aplicado em eventual criação de qualificadora ou causa de aumento de pena para indivíduos que pratiquem tais crimes com o auxílio de *"deep fakes"*: caso compartilhem a *"deep fake"* sabendo que se trata de vídeo adulterado, serão responsabilizados, incidindo inclusive a qualificadora/ majoração da pena. Caso contrário, não terão responsabilidade penal alguma.

Pelo exposto, observou-se que, apesar de inexistir previsão legislativa específica que criminalize a prática do *"deep fake"*, não se faz necessária a

edição de um tipo penal próprio para essa conduta, sendo devido, entretanto, a criação de mecanismos para majorar a pena de quem se utilizar de tal tecnologia para cometer outros crimes, bem como de quem compartilhar tais conteúdos adulterados tendo conhecimento de que se trata de conteúdo falso.

4 CONCLUSÃO

O tema debatido no presente trabalho é de extrema relevância para a sociedade em geral e para a comunidade jurídica, uma vez que os *"deep fakes"* estão cada vez mais presentes na sociedade, afetando a vida diária de todos os indivíduos.

Do mesmo modo, é relevante para toda a comunidade acadêmica, visto que a compreensão sobre as causas e consequências da difusão das *fake news* e, em especial, das *deep fakes*, traz diversos questionamentos acerca dos limites éticos da tecnologia e de seu efeito em diversas searas do direito. Também é relevante no âmbito da sociologia, pois verificou-se que a prática de determinados crimes por intermédio das *deep fakes* – como, por exemplo, a "sextorsão", afeta mais determinado grupo social em detrimento de outro.

Dessa forma, a reflexão pormenorizada sobre esse tema é primordial para compreender seus desdobramentos, de modo a buscar uma forma de responsabilizar indivíduos que pratiquem crimes por intermédio de *"deep fakes"*, sem, contudo, desrespeitar as regras e princípios vigentes no ordenamento jurídico pátrio.

O primeiro tópico trouxe um panorama geral sobre a primeira, segunda e terceira revoluções industriais, abordando também a Quarta Revolução Industrial e seus impactos na sociedade. Ao final do capítulo, chegou-se à conclusão que essa revolução, apesar de ter trazido inúmeros benefícios de ordem prática à população global, também acarretou a criação e popularização dos crimes cibernéticos. Esses crimes crescem a cada dia, motivados, principalmente, por três fatores: a dificuldade de identificação de seus autores, a mutabilidade das técnicas utilizadas e a dúvida a respeito da definição do local do crime. Além disso, essa espécie de delito pode ser subdividida em crimes informáticos

próprios, impróprios e mistos. Os primeiros correspondem àqueles em que o bem jurídico violado é a própria tecnologia da informação, enquanto que os segundos são a espécie de crime cibernético em que atecnologia é utilizada como meio para a prática de outros crimes. Os mistos, por sua vez, são uma mistura dos dois, onde a tecnologia da informação é tanto o bem jurídico atingido quanto o instrumento da execução do delito.

O segundo tópico, por sua vez, abordou as características das *"fake news"* e como elas acarretaram o surgimento das *"deep fakes"*, expondo os perigos que essa prática acarreta para a sociedade, tais como a disseminação de notícias falsas, a sextorsão e a adulteração de meios de prova, sendo discutida também a questão acerca da necessidade – ou não – de criação de uma legislação específica para criminalizar tal conduta, à luz dos princípios de vedação da proteção deficiente e proibição de analogia *in malam partem*. Ao final do tópico, a conclusão obtida foi que, conforme previsto na hipótese desse trabalho, as *"deep fakes"* são um poderoso meio de execução para diversas espécies de crime, sobretudo crimes contra a honra, mas não são, por si só, um crime.

Apesar disso, não se faz necessária a edição de um tipo penal específico apenas para criminalizar tal conduta, uma vez que, diante da rapidez com que as tecnologias evoluem, não se mostra eficiente a criminalização da técnica empregada para criar as *"deep fakes"*, mas sim de seus resultados criminosos. Desse modo, a solução mais adequada seria a criação de uma qualificadora ou causa de aumento de pena para os crimes praticados por intermédio dessa prática, de modo a desincentivar a prática de tal ilícito.

A presente pesquisa teve como foco principal a busca por uma forma de combater a propagação de "*deep fakes"* maléficas através de punição estatal. Desse modo, é limitada no sentido de não explorar de forma abrangente as implicações morais e éticas da prática das "*deep fakes"*, como a questão sobre o consentimento do indivíduo e seu direito à privacidade e imagem, bem como em procurar soluções alternativas e preventivas para auxiliar o combate às "*deep fakes"*. Desse modo, são necessárias pesquisas que englobem tais temas de forma pormenorizada, de forma a contribuir para o avanço social e jurídico da sociedade.

REFERÊNCIAS

AIRES, Regina Wundrack do Amaral; MOREIRA, Fernanda Kempner; FREIRE, Patricia de Sá. Indústria 4.0: competências requeridas aos profissionais da quarta revolução industrial. **Anais do VII Congresso Internacional de Conhecimento e Inovação**, v. 1, n. 1, 2017. Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/314. Acesso em: 30 abr. 2024.

APÓS atingir pico de óbitos, Brasil tem queda de 90% na média diária de mortes por covid-19. **GZH SAÚDE**, 2021. Disponível em: https://gauchazh.clicrbs.com.br/saude/noticia/2021/10/apos-atingir-pico-de-obitos-brasil-tem-queda-de-90-na-media-diaria-de-mortes-por-covid-19-ckuxys2ts0007017fzwxl3u0e.html. Acesso em: 30 abr. 2024.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, RJ: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 abr. 2024

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 abr. 2024.

BRASIL. **Decreto-Lei nº 4.657, de 4 de setembro de 1942**. Lei de Introdução às normas do Direito Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em: 20 abr. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21 abr. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 abr. 2024.

BRASIL. **Projeto de Lei do Senado Federal nº 473 de 2017**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar o crime de divulgação de notícia falsa. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/131758. Acesso em: 20 abr. 2024.

CÂMARA DOS DEPUTADOS. **CPI – Crimes Cibernéticos**. Brasília: [s. n.], 2016. 254 p. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 30 abr. 2024.

CAPEZ, Fernando. **Curso de Direito Penal**: Parte Geral. 15. ed. São Paulo: Saraiva, 2011. 645 p.

DA COSTA, Fernando José. ***Locus delicti* nos crimes informáticos**. 2011. 355 f. Tese de Doutorado (Doutorado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php. Acesso em: 30 abr. 2024.

ESTEVÃO, Roberto da Freiria; BRITO FILHO, Cleudemir Malheiros. Princípio da proibição da proteção deficiente: função e missão do Direito Penal. *In*: **Revista da AJURIS**. Associação dos Juízes do Rio Grande.

FAUSTINO, André. ***Fake news* e a liberdade de expressão nas redes sociais na sociedade da informação**. 2018. 140 p. Dissertação de Mestrado (Mestrado em Direito da Sociedade da Informação) — Faculdades Metropolitanas Unidas, São Paulo, 2018. Disponível em: http://arquivo.fmu.br/prodisc/mestradodir/af.pdf. Acesso em: 25 abr. 2024.

FURBINO, Clara Santos; SOUZA, Thiago Izac de. *Fake news* contribuindo para o cibercrime: regulação e necessidade de tipificação atreladas à legislações internacionais. *In*: **XII Congresso RECAJ – UFMG Skema Business, 2021, Belo Horizonte**. Criminologia e Cybercrimes. p. 44 a 50. 2021. Disponível em: http://site.conpedi.org.br/publicacoes/f0d20hl5/k6f200vz. Acesso em: 25 abr. 2024.

GRECO, Rogério. **Curso de Direito Penal**: Parte Geral. 19.ed. Niterói: Impetus, 2017. v. 1. ISBN 978-85-7626-930-4.

GRIGORI, Pedro. **20 projetos de lei no Congresso pretendem criminalizar *fake news***. 11 maio 2018. Disponível em: https://apublica.org/2018/05/20-projetos-de-lei-no-congresso-pretendem-criminalizar-fake-news/. Acesso em: 24 abr. 2024.

HARARI, Yuval Noah. **Sapiens**: uma breve história da humanidade. Porto Alegre: L&PM Editores, 20 abr. 2024.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016. 231 p. ISBN 978850262724-6.

LACERDA, Anna Carolina Alves Moreira de; SILVA, Amanda Pedroso. Cibercrime: evolução do crime e a banalização dos crimes virtuais. *In*: HORITA,

Fernando Henrique da Silva; MORAIS, Fausto Santos de; OLIVEIRA, Camila Martins de. (Orgs.). **Direito Penal e Cibercrimes**. Belo Horizonte: Skema Business School, 2021. v. 1, p. 12-19.

LIMA FILHO, Paulo Roberto Aguiar de. O Direito Penal na Quarta Revolução Industrial. **Delictae Revista De Estudos Interdisciplinares Sobre O Delito**, v. 6, n. 10, p. 215-304, 2021. Disponível em: https://doi.org/10.24861/25265180.v6i10.150. Acesso em: 30 abr. 2024.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira. **RIOS Eletrônica** (FASETE), v. 18, p. 166-180, 2018. Disponível em: https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf. Acesso em: 30 abr. 2024.

MEDON, Filipe. O direito à imagem na era das deepfakes. **Revista Brasileira de Direito Civil – RBD Civil**: Belo Horizonte, v. 27, p. 251-277, jan/mar. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/viewFile/438/447. Acesso em: 30 abr. 2024.

PIAIA, Thami Covatti; COSTA, Bárbara Silva; WILLERS, Miriane Maria. Quarta revolução industrial e a proteção do indivíduo na sociedade digital: desafios para o direito. **Revista Paradigma**, v. 28, p. 122-140, 2019. Disponível em: https://revistas.unaerp.br/paradigma/article/view/1444/1287. Acesso em: 25 abr. 2024.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021. 573 p. ISBN 9786555598438.

RUDOLFO, Fernanda Mambrini. **A dupla face dos direitos fundamentais**: a aplicação dos princípios da proibição de proteção deficiente e de excesso de proibição no direito penal, especialmente quanto aos crimes sexuais. 2011. 193 f. Dissertação (Mestrado) – Universidade Federal de Santa Catarina, Florianópolis, SC, 2011. Disponível em: https://repositorio.ufsc.br/xmlui/handle/123456789/95755. Acesso em: 25 abr. 2024.

SANTOS, Marcelo Fernandes Pires dos. **Retórica, teoria da argumentação e pathos**: o problema das emoções no discurso jurídico. 2015. 151 f. Dissertação (Mestrado em Direito) — Universidade de Brasília, Brasília, 2015. Disponível em: https://repositorio.unb.br/handle/10482/18787#:~:text=Este%20estudo%20objetiva%20compreender%20por,a%20explana%C3%A7%C3%A3o%20do%20sistema%20jur%C3%ADdico. Acesso em: 25 abr. 2024.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016. 167 p. ISBN 978-85-7283-978-5.

TERRA, Cristiane Izabela de Souza; ORSINI, Adriana Goulart de Sena; ABREU, Camila Cristina de Moura. Crimes cibernéticos: phishing e *fake news*

em tempos de pandemia. *In*: FREITAS, Sérgio Henriques Zandona; LANNES, Yuri Nathan da Costa; SILVA, Lucas Jerônimo Ribeiro da. (Orgs.). **Criminologia e cybercrimes**. Belo Horizonte: UFMG, 2021. v. p. 29-35. Disponível em: http://site.conpedi.org.br/publicacoes/f0d20hl5/k6f200vz. Acesso em: 26 abr. 2024.

WAKEFIELD, Jane. Guerra na Ucrânia: os 'presidentes deepfake' usados na propaganda do conflito. **BBC News**, São Paulo, SP, 18 de março de 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60791955. Acesso em: 26 abr. 2024.

WALDMAN, Ricardo Libel; HORAS, Matheus dos Santos. Uma caracterização das *fake news*: o exemplo da greve dos caminhoneiros. **Direito, governança e novas tecnologias I** [Recurso eletrônico on-line] organização CONPEDI/UNISINOS, p. 338-353, Florianópolis, 2018. Disponível em: http://site.conpedi.org.br/publicacoes/34q12098/9l053031. Acesso em: 26 abr. 2024.