UNIVERSIDADE PRESBITERIANA MACKENZIE

STÉPHANIE MARTINEZ DUARTE

PERFIS FALSOS EM REDES SOCIAIS CONTEMPORÂNEAS: Uma análise quanto às responsabilidades Penal e Civil.

São Paulo

2021

STÉPHANIE MARTINEZ DUARTE

PERFIS FALSOS EM REDES SOCIAIS CONTEMPORÂNEAS: Uma análise quanto às responsabilidades Penal e Civil.

Trabalho de Conclusão de Curso apresentado à Universidade Presbiteriana Mackenzie do Estado de São Paulo como requisito parcial à obtenção do grau de Bacharel em Direito.

ORIENTADORA: Profa. Dra. Maria Patricia Vanzolini Figueiredo

São Paulo

2021

STÉPHANIE MARTINEZ DUARTE

PERFIS FALSOS EM REDES SOCIAIS CONTEMPORÂNEAS NA INTERNET: Uma análise quanto às responsabilidades Penal e Civil.

Trabalho de Conclusão de Curso apresentado à Universidade Presbiteriana Mackenzie do Estado de São Paulo como requisito parcial à obtenção do grau de Bacharel em Direito.

Aprovada em:

BANCA EXAMINADORA

_____

Profª: Dra. Lia Felberg

Universidade Presbiteriana Mackenzie

_____

Profª. Dra. Maria Patricia Vanzolini Figueiredo

Universidade Presbiteriana Mackenzie

_____

Prof. Dr. Rodrigo Arnoni Scalquette

Universidade Presbiteriana Mackenzie

Aos meus pais, em especial, minha mãe, pelo incessante apoio; aos meus avós, em especial, meu saudoso avô, pelo exemplo que me motivou.

AGRADECIMENTOS

Primeiramente a Deus e ao Senhor Jesus Cristo, fonte de toda sabedoria e que guiaram os meus passos por toda a minha trajetória.

À Profa. Dra. Maria Patrícia Figueiredo Vanzolini, que me orientou e ensinou o que, de fato, é um trabalho de pesquisa, compartilhando seus conhecimentos com paciência e dedicação.

Ao meu companheiro, que me apoiou no momento em que eu mais precisei durante a elaboração desse trabalho de pesquisa.

Nossa tecnologia passou a frente de nosso entendimento, e a nossa inteligência desenvolveu-se mais do que a nossa sabedoria.
(Roger Revelle)

RESUMO

É possível visualizar que, com o surgimento da Internet no mundo, as interações sociais se alteraram drasticamente. Diante de um novo cenário, é preciso que haja novas regras de convivência entre os seres humanos.
Assim como no mundo real, na internet também são cometidos crimes. Com a diferença de que na Internet há crimes virtuais próprios e os impróprios, ou seja, crimes em que a internet é o crime-fim ou o crime-meio.
Após essa abordagem, é essencial que o leitor tome conhecimento do que é um perfil falso, bem como quais são as possíveis motivações de um usuário criá-lo, seja com intenção criminosa ou não.
O objetivo do presente trabalho é apresentar a responsabilidade possível de ser imputada ao usuário *fake* nos âmbitos civil e penal, mas, mais importante é saber como funciona o Direito Digital e como é possível uma investigação no sentido de identificar a pessoa responsável pelo dano causado. Dessa forma, o trabalho traz aspectos fundamentais dessa investigação.
No âmbito civil, a responsabilidade pela indenização da vítima, por um ato praticado por perfil falso, é um fardo que pode recair também ao provedor de aplicação ou de conexão, gerando uma grande discussão jurisprudencial acerca do artigo 19 do Marco Civil da Internet e os artigos 3 e 14 do Código de Defesa do Consumidor.
No âmbito penal, o trabalho se dedica a avaliar quanto ao enquadramento da criação de um perfil falso aos crimes de falsidade ideológica e falsa identidade, uma vez visualizada a possibilidade de um concurso de crimes entre os mencionados e aqueles praticados na internet através do uso de perfis falsos.
O trabalho ainda traz reflexões quanto à liberdade de expressão e a proibição do anonimato, previstos na Constituição Federal de 1988, bem como a importância da educação no meio eletrônico.
No mais, o trabalho apresenta o Projeto de Lei que tramita no Congresso com a finalidade de criminalização do uso de perfil falso, também trazendo a legislação comparada da Califórnia, onde essa previsão é existente.

Palavras-chave: Rede social. *Fake.* Perfil falso. Criminalização.

ABSTRACT

It is possible to see that with the emergence of the Internet in the world, social interactions have changed dramatically. In the face of a new scenario, there must be new rules for coexistence between human beings.

Just like in the real world, crimes are also committed on the internet. With the difference that on the Internet there are virtual crimes proper and improper ones, that is, crimes in which the Internet is the ultimate crime or the middle crime.

After this approach, it is essential that the reader becomes aware of what a fake profile is, as well as what are the possible motivations of a user to create it, whether with criminal intent or not.

The objective of this work is to present the possible responsibility to be imputed to the fake user in the civil and criminal spheres, but, more important is to know how Digital Law works and how an investigation is possible in order to identify the person responsible for the damage caused. Therefore, the work brings fundamental investigation aspects.

In the civil sphere, the responsibility for the compensation of the victim, for an act practiced for false profile, is a burden that can also fall on the application or connection provider, generating a great jurisprudential discussion about article 19 of the Marco Civil da Internet and the articles 3 and 14 of the Código do Consumidor.

In the criminal field, the work is dedicated to assessing the framing of the creation of a false profile to crimes of ideological falsehood and false identity, once the possibility of a contest of crimes between those mentioned and those practiced on the internet through the use of fake profiles.

The work also brings reflections on freedom of expression and the prohibition of anonymity, provided for in the Federal Constitution of 1988, as well as the importance of education in the electronic medium.

In addition, the paper presents the Project that is being processed in Congress for the purpose of criminalizing the use of false profiles, also bringing the comparative legislation of California, where this provision exists.

Keywords: Social network. Fake. Fake profile. Criminalization.

SUMÁRIO

INTRODUÇÃO

De início a presente pesquisa se dedica a explorar o conceito histórico de rede social, antes mesmo da abordagem virtual a que o tema se refere.

Nesse sentido, outros aspectos históricos são importantes a serem abordados, como a história da Internet e das redes sociais no meio virtual. Apenas com uma visão temporal é possível entender características essenciais desses assuntos e, só então, haver compreensão quanto aos aspectos mais aprofundados do tema.

Após uma abordagem histórica, é imprescindível que conheçamos as redes sociais virtuais mais utilizadas no momento, bem como os usuários interagem com essas ferramentas, para o que elas servem e como funcionam.

Habituados com o cenário, precisamos identificar as ações criminosas. Quais crimes são cometidos na internet? Quais desses crimes são cometidos mais comumente através de perfis falsos em redes sociais virtuais?

Outro ponto a serquestionado: por que uma pessoa criaria um perfil falso? Neste trabalho iremos abordar os principais motivos pelos quais alguém é levado a criar um perfil falso em uma rede social, bem como categorizar as formas de perfis encontrados nesse ambiente.

Ainda, os crimes cometidos na internet são os mesmos que podem ser cometidos no ambiente físico? Ou há crimes que apenas se dão no ambiente virtual? É possível separá-los?

Identificar o infrator de uma norma é essencial para o cumprimento da lei. Assim, para entender como acontece uma investigação para identificação de um perfil falso em rede social, precisaremos entender como a internet e a rede de computadores funciona, bem como os passos dessa investigação.

Independentemente de quem praticou um crime na internet, sabe-se que alguém foi lesado e essa pessoa tem direito a ser indenizada pelo seu bem lesado, seja no âmbito moral ou material.

Assim, qual é o limite de responsabilidade de indenização de uma vítima pelo prestador de serviço do site no âmbito do Direito Civil ou do Consumidor? Para responder a tal pergunta, faremos uma análise legislativa, doutrinária e jurisprudencial.

No âmbito penal, além da abordagem de outros crimes praticados por perfis falsos em redes sociais, analisaremos quanto à criminalidade da criação de um perfil falso em si. É possível que seja uma conduta tipificada como falsidade ideológica ou falsa identidade?

Uma análise jurisprudencial também é realizada quanto às questões penais, da mesma forma que é feita no âmbito civil.

A Constituição Federal de 1988 é uma lei com princípios fundamentais e que influencia em qualquer assunto no ramo do Direito. Assim, analisaremos se há limites impostos por ela na internet e, principalmente, nas redes sociais.

As ações nas redes sociais são tomadas por pessoas, assim como no mundo físico. Desta forma, é importante que observemos o quanto a educação em qualquer ambiente pode impactar em como se dão as relações entre as pessoas.

Chegando ao final, veremos se há leis ou projetos de lei no sentido de criminalizar a criação de perfis falsos no Brasil. Ainda, se essa criminalização pode ser identificada através de leis de outros países, realizando uma análise no âmbito do Direito comparado.

1 CONCEITOS E RESUMO HISTÓRICO

Introduzidos ao tema, faz-se necessário uma pequena linha do tempo dos acontecimentos e conceitos históricos de alguns pontos importantes para a melhor compreensão do assunto pelo leitor.

1.1 A HISTÓRIA DA INTERNET

Após o lançamento do primeiro satélite no espaço pela União Soviética em 1957, momento em que o mundo vivenciava a chamada Guerra Fria, segundo o que nos conta Eduardo Teixeira, o governo norte americano, em resposta ao ocorrido, lançou o projeto de pesquisa militar (ARPA: *Advanced Research Projects Agency*). Vejamos com mais detalhes sua explicação:

> Inicialmente a ideia era conectar os mais importantes centros universitários de pesquisa americanos com o Pentágono para permitir não só a troca de informações rápidas e protegidas, mas também para instrumentalizar o país como uma tecnologia que possibilitasse a sobrevivência de canais de informação no caso de uma guerra nuclear. [1]

Ou seja, com o medo de algum ataque de míssil que pudesse destruir o computador central localizado em Washington nos Estados Unidos, a ideia era distribuir as informações nele para outros computadores em outros locais do mundo através de uma rede de computadores interligados por uma rede subterrânea.

Esses computadores eram capazes de decifrar as mensagens recebidas de computadores da mesma rede, pois possuem a mesma linguagem, TCP/IP (*Transmission Control Protocol/Internet Protocol*), que lê a informação transmitida e a envia para o destino estabelecido pelo usuário. A partir de então verificamos o surgimento da Internet.

---

[1] TEIXEIRA, Eduardo Ariel de Souza. *Estudo Ergonômico da Interface De Produtos Web Focados Na Transmissão De Alta Velocidade*. 2004. Dissertação. Pontifícia Universidade Católica Do Rio De Janeiro, Rio de Janeiro, 2004. p. 50. Disponível em: <https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=resultado&nrSeq=5090@1> Acesso em: 19.02.2021

Nos explica, ainda, que o e-mail foi a primeira forma de comunicação na internet entre os pesquisadores.

Cada um desses computadores possuía um número de identificação, os chamados IP (*Internet Protocol*). Esse número serve como endereço para que o computador remetente da informação a envie para o local correto.

Explica também que a internet se tornou mais popular ao longo do século XX. Porém, em 1989, com a criação do *World Wide Web* (WWW, ou ainda W3, ou simplesmente *Web*), a internet pôde se tornar um meio de comunicação em massa. Isso porque essa era uma nova forma de navegar na internet mais simplificada e ilustrativa, o que atraiu muito todas as pessoas.

Com o surgimento de milhares de usuários ao redor do mundo, cada vez mais computadores se conectaram à rede. Assim, tornou-se inviável que cada um tivesse um único número de IP.

Para solucionar o problema da quantidade gigantesca de necessidade de números de IP, foi criado um novo Protocolo chamado de Servidor DHCP (*Dynamic Host Configuration Protocol*), que permite que sejam atribuídos IPs temporários aos dispositivos conectados à rede.

Ou seja, nossos dispositivos podem ser identificados com um número de IP diferente a depender do momento no tempo, uma vez que são rotativos entre os usuários em todo o mundo.

Mais a frente nos ateremos a explicar melhor o funcionamento da identificação de um computador na rede.

1.2 REDES SOCIAIS

Explorando as definições de rede social, diversos estudiosos tentaram conceituar a expressão “rede social”, de forma a abarcar todos pontos que envolvem o referido termo.

Em uma análise mais voltada para a área das ciências exatas, Paulo Alexandre de Castro[2] define rede por “um conjunto de itens, que chamamos de vértices (nós), com ligações entre eles, chamados de conexões (arestas)”.

Já Maria Inês e Regina Maria[3], mais direcionadas para uma perspectiva social, definem como rede social um conjunto de pessoas, organizações ou entidades sociais que estão conectadas por algum motivo, seja por relações de trabalho, informações ou amizade. Essas conexões constroem e reconstroem a estrutura social.

Imagina-se que as redes sociais começaram a surgir desde que o homem começou a se reunir em “bandos”. Isto é, desde que aconteceu o que os historiadores chamam de Revolução Cognitiva e que podemos presumir o surgimento de aspectos iniciais do que hoje chamamos de cultura.[4]

Porém, ideia de rede social é bem mais recente. Isto é, começou-se a pensar sobre esse conceito em anos posteriores. Para Regina Maria Marteleto[5], essa ideia já

---

[2] CASTRO, Paulo Alexandre de. *Rede complexa e criticalidade auto-organizada: modelos e aplicações.* 2007. Tese (Doutorado em Física Básica) – Universidade de São Paulo, São Paulo, 2007. p. 45. Disponível em: <https://www.teses.usp.br/teses/disponiveis/76/76131/tde-14012008-165356/pt-br.php> Acesso em: 05.04.2021

[3] TOMAÉL, Maria Inês; MARTELETO, Regina Maria. *Redes sociais:* posições dos atores no fluxo da informação. Encontros Bibli: Revista eletrônica De Biblioteconomia e Ciência Da informação, 2006. p. 75. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2006v11nesp1p75> Acesso em: 05.04.2021

[4] HARARI, Yuval Noah. *Sapiens:* uma breve história da humanidade. Tradução de Janaína Marcoantonio. Porto Algre: L&M Editores, 2020. p. 56

[5] TOMAÉL, Maria Inês; MARTELETO, Regina Maria. *Redes sociais*: posições dos atores no fluxo da informação. Encontros Bibli: Revista eletrônica De Biblioteconomia E Ciência Da informação, 2006. p. 75. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2006v11nesp1p75> Acesso em: 05.04.2021

pode ser observada desde os pensamentos de Hipócrates na memória da sua origem orgânica e próxima do imaginário do corpo.

Porém, é mais precisamente no século XX que essa ideia surge, de fato. Nesse sentido Gonçalo Costa Ferreira explica:

> É, no inicio do séc. XX, que surge a ideia de rede social, a ideia de que as relações sociais compõem um tecido que condiciona a ação dos indivíduos nele inseridos. A metáfora de tecido ou rede foi inicialmente usada na sociologia, para associar o comportamento individual à estrutura a qual ele pertence e transformou-se em uma metodologia denominada sociometria, cujo instrumento de análise se apresenta na forma de um sociograma.[6]

Dessa forma, podemos visualizar que o conceito vai muito além do ao que costumamos associar nos dias de hoje. Isto é, rede social é muito mais do que aplicativos existentes na internet.

Entretanto, segundo Pierre Lévy[7], ”a técnica e a tecnologia é indissociável da realidade social, as tecnologias não são adjetivos sociais, mas sim, parte integrante do coletivo social caracterizando os seus processos sócio-técnicos”.

Assim, contemporaneamente, é impossível dissociar as duas coisas: redes sociais e internet.

1.2.1 as redes sociais na internet

Notamos que o ambiente virtual proporcionou diversas e perceptíveis mudanças no meio social. Dentre elas, está o modo como as pessoas se relacionam umas com as outras.

Isso porque, nas ilustres palavras do Professor Damásio de Jesus:

---

[6] FERREIRA, Gonçalo Costa. *Redes Sociais de Informação*: uma história e um estudo de caso. 2011. Dissertação (Mestrado em Ciência da Informação) - Escola da Comunicações e Artes da Universidade de São Paulo, São Paulo, 2011. p.210. Disponível em: <https://www.scielo.br/pdf/pci/v16n3/13.pdf> Acesso em: 05.04.2021

[7] LÉVY, Pierre. *As tecnologias da inteligência*: o futuro do pensamento na era da informática. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1993. p. 79

> É preciso que se diga que a sociedade não é uma pedra, estática, mas um organismo de mudanças, em constante transformação. A tecnologia é um dos fatores que motivam as principais mutações sociais nesta era, chegando a ditar comportamentos e a criar costumes.[8]

Assim, diante das transformações decorrentes do ambiente cibernético, teremos um novo conceito de rede social, conforme as palavras de Hugo Filipe, *in verbis:*

> O termo “rede social” pode definir-se como um espaço virtual na Internet onde os utilizadores (pessoas, entidades ou empresa) podem criar ligações entre si, com o intuito de partilhar informações.
> Há vários tipos de redes sociais, destacando-se as relacionadas com relacionamentos, entretimento, profissionais e temáticas:
> As redes sociais de relacionamento têm como principal objetivo criar ligações entre as pessoas, a partilha de conteúdos e informações entre elas, como exemplo temos o Facebook.[9]

A primeira rede social da internet nasceu em 1995 e era chamada de *Classmates.* Seu principal objetivo era conectar pessoas que estudaram na mesma escola e que há muito tempo não tinham notícias uns dos outros. Essa rede social existe até hoje nos Estados Unidos. Porém, tem pouca adesão de usuários.[10]

Depois disso, diversas outras redes sociais foram criadas. Porém, outra rede social que é de extrema relevância ser citada por conta do sucesso de adesão no Brasil, é o *Orkut*.

Essa rede social nasceu em 2004, desenvolvida pelo Google e, para ingressar na plataforma, era necessário ser convidado por um usuário que já fizesse parte dela. Porém, era um experimento. Isso porque a plataforma não chegou a ter uma versão

---

[8] JESUS, Damasio Evangelista de; OLIVEIRA, Jose Antonio M Milagre de. *Manual de crimes informáticos***.** 1ª ed. São Paulo: Saraiva. 2015. p.27

[9] BAPTISTA, Hugo Filipe Fontainhas. *Identificação de perfis falsos nas redes sociais.* 2019. Projeto (Mestrado em Cibersegurança e Informática Forense) – Instituto Politécnico de Leiria, Leiria, 2019. p. 5. Disponível em: < https://iconline.ipleiria.pt/bitstream/10400.8/4550/1/Identificacao_de_perfis_falsos_nas_redes_sociais_2170086.pdf> Acesso em: 07.05.2021

[10] GOGONI, Ronaldo. *Qual foi a primeira rede social criada na internet?*. São Paulo, 2020. Disponível em: <https://tecnoblog.net/author/ronaldogogoni/> Acesso em: 06.04.2021.

completa, mas sim o que chamamos de versão *Beta*. Ou seja, estava em desenvolvimento.

Em que pese o criador ter sido um turco e o público alvo eram os norte-americanos, o Brasil foi o principal utilizador da plataforma, com 50% das contas existentes.

Nessa rede as pessoas avaliavam umas às outras, deixavam depoimentos no perfil inicial de cada usuário e, o que podemos considerar como a principal forma de conexão entre os usuários, criando uma rede de pessoas com algo em comum, eram as chamadas “comunidades”.

Era comum encontrar comunidades com discursos de ódio, teorias da conspiração, banalidades etc.

O *site* durou em média 10 anos e nunca superou a versão *Beta*. Assim, começaram a surgir diversos problemas relacionados ao uso da plataforma, que não detinha uma moderação atenciosa no controle dos usuários.

Em determinado momento o *site* começou a apresentar diversos problemas como *spam* (*links* maliciosos que podiam roubar dados de quem clicava) e o uso indevido e não autorizado da imagem de pessoas em comunidades.

Assim, após um longo período de utilização, o *Orkut* foi descontinuado em 2014 por ter perdido espaço para outras redes sociais, principalmente o *Facebook,* sobre o qual abordaremos mais adiante.

Todo esse histórico do *Orkut*, é fruto da pesquisa apresentada em forma de vídeo pelo canal do *Youtube* chamado “Meteoro Brasil”.[11]

[11] QUEM MATOU O ORKUT. Direção e Produção: *Canal Meteoro Brasil*. Curitiba. 2021. Disponível em: <https://www.youtube.com/watch?v=joat8DME_UI> Acesso em: 06.04.2021.

Uma vez explorado o conceito do termo rede social, bem como um breve histórico das redes sociais mais utilizadas na internet, é necessário, para o desenvolvimento desse trabalho, uma breve descrição das principais redes sociais atualmente mais utilizadas na internet.

Dentre as redes sociais existentes no mundo virtual, as mais comumente utilizadas são chamadas: *Instagram, Facebook, Twitter, Linkedin* e *Whatsapp.*

Todas essas redes possuem a opção de os usuários conversarem privativamente através de mensagens, bem como a criação de grupos de conversas também privadas aos usuários do grupo.

Ainda, todas possuem termos de uso, nos quais os usuários devem concordar para ingressar.

Nesses termos consta a conduta mínima esperada do usuário e os limites nos quais ele se responsabiliza a não ultrapassar.

1.2.1.1. Facebook

O início do Facebook se deu em 2003, quando estudantes da Universidade de Harvard, nos Estados Unidos, desenvolveram uma rede social exclusiva para o campus. Em 2004, Zuckerberg, um dos referidos estudantes, criou o thefacebook.com, que se tornou o Facebook no ano seguinte. Porém, chegou no Brasil na versão em português apenas em 2007.[12]

O Facebook, dentre as redes sociais que serão citadas, é o que mais possui campos de informações do usuário, ou seja, nessa rede o usuário pode, além de fotos

[12] FACEBOOK. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/facebook/> Acesso em: 07.04.2021

e legendas, compartilhar dados pessoais como: idade, religião, local de trabalho, local de estudo dentre outras. Ainda, conta com o maior número de usuários do mundo.

1.2.1.2 Instagram

Fora criado em 2010 e tomou grande proporção em poucos meses. O Brasil é um dos países com maior número de usuários.[13]

O Instagram é uma rede social em que as pessoas se dedicam, na maior parte dos casos, à postagem de fotos e vídeos, que podem ser acompanhados de legendas.

1.2.1.3 Twitter

Fora criado em 2006, nos Estados Unidos. Porém, só ganhou popularidade em 2008.[14]

O Twitter é uma rede de postagem de pequenos textos. Na ferramenta também é possível o compartilhamento de imagens com legendas. Além disso, uma das principais ferramentas do Twitter, os Trending Topics, disponibiliza aos usuários os assuntos mais falados do mundo no momento.

1.2.1.4 Linkedin

Fundado em 2003 na Califórnia nos Estados Unidos e foi comprado pela Microsoft em 2016. Tornou-se a principal rede social profissional do mundo. O Brasil é o terceiro país do mundo com maior número de usuários nessa rede.[15]

---

[13] INSTAGRAM. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/instagram/> Acesso em: 07.04.2021

[14] TWITTER. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/twitter/#:~:text=O%20Twitter%20foi%20fundado%20em,conte%C3%BAdos%20escritos%2C%20fotografias%20e%20v%C3%ADdeos./> Acesso em: 07.04.2021

[15] LINKEDIN. *CanaTech.* Disponível em: <https://canaltech.com.br/empresa/linkedin/#:~:text=O%20LinkedIn%20foi%20lan%C3%A7ado%20por,..de%20usu%C3%A1rios%20em%20200%20pa%C3%ADses.> Acesso em: 07.04.2021

O Linkedin é uma rede de postagem muito parecida com o Facebook, com a diferença de que o foco das postagens, bem como a conexão entre as pessoas, se dá no âmbito profissional.

1.2.1.5 Whatsapp

Fundado em 2009 nos Estados Unidos, revolucionou a telecomunicação no mundo, uma vez que substituiu praticamente por completo o uso de mensagens via SMS, que custavam caro para os usuários.

Hoje, o aplicativo é gratuito e oferece aos usuários serviços de mensagens de texto e áudio criptografadas, chamadas de voz e vídeo, envio e recebimento de diversos tipos de arquivos, além do compartilhamento de localização entre os usuários.[16]

Ainda, o Whatsapp é uma ferramenta de troca de mensagens privadas, também com a possibilidade de criação de grupos em que apenas os usuários selecionados possam ver determinadas mensagens.

1.2.2 Perfis falsos nas redes sociais contemporâneas

Dentro das redes sociais os usuários podem criar perfis com dados como: foto, idade, domicílio, local de trabalho, locais de formação acadêmica, religião etc.

Porém, nem sempre o usuário criador de um perfil coloca suas reais informações nele. Algumas pessoas criam perfis com informações que não condizem com sua realidade ou não são suficientes para identificá-la.

[16] WHATSAPP. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/whatsapp/#:~:text=O%20WhatsApp%20foi%20fundado%20em,Brian%20Acton%20e%20Jan%20Koum.&text=Focado%20em%20sua%20miss%C3%A3o%20de,em%20mais%20de%20180%20pa%C3%ADses.> Acesso em: 07.04.2021

Para Hugo Filipe[17], a finalidade da criação desses perfis falsos em redes sociais é, normalmente, de cometer algum delito ou tirar algum proveito financeiro omitindo sua real identidade.

Porém, neste trabalho acredita-se que não necessariamente. Há a possibilidade de que uma pessoa crie um perfil falso com outras intenções e que veremos mais adiante.

Entretanto, tendo em vista que a criação de perfis falsos pode estar atrelada, muitas das vezes, às condutas reprováveis pela sociedade, segundo Hugo Filipe[18], as plataformas tendem a utilizar de meios para reprimir esse tipo de conduta, de forma a identificar automaticamente esses perfis. O referido autor explana melhor quanto às ferramentas de inibir a criação de perfis falsos, vejamos:

> [...]Para ajudar a combater esse problema foram desenvolvidas algumas ferramentas, uma delas "About This Account" que permite verificar a informação relativa à conta como data de registo da conta, país onde a conta se localiza, contas com followers comuns, usernames utilizados no último ano e anúncios que essa conta tem ativos.
>
> Outra ferramenta colocada ao dispor do utilizador, consiste em realizar a validação da conta, para isso o utilizador deve solicitar ao Instagram essa validação, apresentado uma cópia do seu documento de identificação. Na altura da redação deste documento esta ferramenta estava temporariamente desativada.
>
> Uma outra ferramenta consiste na permissão de uso de aplicações de autenticação de dois fatores para login nas contas. Neste caso permitido é o uso do Duo Mobile ou Google Authenticator.
>
> A autenticação de dois fatores fornece uma camada de segurança extra visto que o utilizador necessita de ter conhecimento de dois fatores para poder fazer login, como por exemplo a password para entrada na rede social e por exemplo um código que é enviado para uma aplicação móvel ou e-mail.[19]

[17] BAPTISTA, Hugo Filipe Fontainhas. *Identificação de perfis falsos nas redes sociais.* 2019. Projeto (Mestrado em Cibersegurança e Informática Forense) – Instituto Politécnico de Leiria, Leiria, 2019. p.15.
[18] Ibid, p.24.
[19] Ibid, p.16.

Ainda, em artigo publicado na Revista da Faculdade de Direito de São Paulo, vemos uma análise importante quanto ao problema que pode existir em caso de haver uma maior exigência de certificação de usuários. Vejamos:

> O problema que se apresenta é que quanto maiores as medidas para a certificação dos dados (p.ex. solicitação de comprovante de residência, número de cartão de crédito, comparecimento pessoal em estabelecimento da empresa que disponibiliza a rede social, ou outros meios de comprovação), maior é a confiança depositada no sistema e, assim, maiores os prejuízos que podem ocorrer no caso de um roubo de identidade.[20]

Mesmo com a tentativa de inibir a criação de perfis falsos e, ainda, identificar quais são perfis com dados e informações que não condizem com a realidade do usuário criador do perfil, há a dificuldade de rastrear a pessoa que está “por trás”.

Isso porque, conforme explanado no tópico 1.1, os endereços de IP, que poderiam ser usados para identificar os computadores dos usuários, são rotativos e podem não trazer tanta segurança de que essa identificação será possível.

Neste diapasão, Eliane Coser nos ensina:

> Há quem possa dizer que não existe anonimato na internet se é possível localizar um usuário pelo endereço de IP, entretanto, a realidade prática é completamente diversa. Isso porque não é possível atribuir um endereço de Internet Protocol para cada dispositivo conectado à rede mundial, haja vista que o sistema de conexões adotado mundialmente (protocolo TCP/IP) possui um número de disponibilidade de endereços limitado e reduzido, que não comportaria a taxação de IP fixo para cada dispositivo eletrônico produzido, pois, em pouco tempo, enfrentaríamos o esgotamento de endereços IPs
> [...] encontrar a origem de uma informação unicamente pelo endereço de Internet Protocol é uma tarefa, se não impossível, muito difícil, até mesmo para quem detém grande conhecimento técnico na área de informática.
> [...]
> As redes sociais verdadeiras são prejudicadas pela ausência de sistemas seguros gue não permitem evitar que falsos perfis sejam inseridos, representando personagens de ficção literária, cinematográfica ou mesmo pessoas reais diferentes daquelas que criaram o perfil virtual. Os falsos perfis permitem aplicações inovadoras, porém apresentam riscos de infração à propriedade intelectual, calúnia, difamação, injúria, falsidade

[20] REVISTA DA FACULDADE DE DIREITO DE SÃO PAUO: Regulação tecnológica e jurídica das redes sociais (*social networks).* São Paulo: Universidade de São Paulo, v. 100, jan/dez 2005. p. 631-634.

> ideológica, entre outras infrações jurídicas que diminuem a confiança no sistema e, portanto, seu funcionamento otimizado. [21]

Dessa forma, pudemos visualizar a problemática que envolve a criação de perfis falsos. As plataformas tentam de diversas formas criar mecanismos que dificultem essa prática e então manter a qualidade e segurança do serviço, uma vez que a dificuldade de rastrear um usuário criador de um perfil falso é imensa e, como veremos mais a frente, os provedores desses sites podem acabar sendo responsabilizados por danos causados por esses perfis a outros usuários.

Segundo artigo publicado na Revista da Faculdade de Direito de São Paulo[22], os perfis falsos em redes sociais podem representar personagens de ficção literária, cinematográfica ou mesmo pessoas reais diferentes daquelas que criaram o perfil virtual. Neste sentido, os falsos perfis permitem aplicações inovadoras, porém apresentam riscos de infração à propriedade intelectual, calúnia, difamação, injúria, falsidade ideológica, entre outras infrações jurídicas que diminuem a confiança no sistema e, portanto, seu funcionamento otimizado.

Assim, passaremos a ver adiante quais os principais tipos de perfis que se utilizam do anonimato na internet.

1.2.3 Tipos de perfis falsos nas redes sociais contemporâneas

O presente tópico trará como foco uma pesquisa realizada por um graduando, para fins de Trabalho de Conclusão de Curso de Tecnologias da Informação e

[21] FONTANA, Eliane; COSER, Thomas Felipe. *Perfil Falso Na Rede E O Anonimato*: Uma Visão (Polêmica) À Luz Do Marco Civil Da Internet. In: SEMINÁRIO INTERNACIONAL: DEMANDAS SOCIAIS E POLÍTICAS NA SOCIEDADE CONTEMPORÂNEA, VIII Mostra de trabalhos jurídicos científicos, 2015. Rio Grande do Sul: Universidade de Santa Cruz do Sul, 2015. p. 10-11. Disponível em: < https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13174/2387> Acesso em: 18.10.2020.

[22] REVISTA DA FACULDADE DE DIREITO DE SÃO PAUO: Regulação tecnológica e jurídica das redes sociais (*social networks).* São Paulo: Universidade de São Paulo, v. 100, jan/dez 2005. P.625

Comunicação do Centro de Ciências, Tecnologias e Saúde da Universidade Federal de Santa Catarina[23].

A pesquisa levou em consideração as possíveis motivações para criação de perfis falsos, ou, como comumente chamados nas redes sociais: *fakes.*

Assim, expusemos o que nos interessava da referida pesquisa para tentar identificar alguns tipos de perfis que podem ser encontrados nas redes sociais, fazendo, inclusive, menção aos termos de uso dessas plataformas. Porém com diversas contribuições pertinentes ao estudo do presente tema.

Dentre os perfis identificados, temos: clássico,plagiadores de identidade, robôs, humorísiticos e os criminosos.

O denominado clássico pela referida pesquisa, o perfil falso clássico tem como característica principal a falta de informações básicas, nome de usuário, foto de perfil ou foto de capa, além da quantidade baixa de seguidores/amigos ou, que possuem, mas sem que seja possível identificar de quem realmente se trata o perfil.

Já os plagiadores são aqueles que copiam de perfis reais fotos e informações pessoais de outras pessoas.

Ou seja, o usuário contém fotos e informações de uma pessoa e, às vezes, pode enganar até pessoas muito próximas às vítimas, se fazendo passar por alguém que não é.

Os perfis falsos “robôs” têm essa denominação justamente por atuarem como máquinas ou até mesmo criados por elas, por sua vez comandados por algoritmos que executam publicações automáticas em seus perfis nas redes sociais.

Dentre essas contas “robôs”, podemos dividi-las em duas categorias: As criadas para fins de aumento de popularidade e para fins de disseminação de

[23] ARROYO, Danilo Wohnrath. *A criação de perfil falso nas redes sociais Facebook e Twitter*: motivações e tipos. Araranguá. 2019. P. 34-47. Disponível em: <https://repositorio.ufsc.br/handle/123456789/203028> Acesso em 01.12.2020.

mentiras, para ambas as finalidades, pode haver a comercialização desses perfis falsos.

Veremos com mais detalhes, nos próximos tópicos, as diferenças entre os dois casos, bem como exemplos em noticiários dessas comercializações e esquemas.

Os perfis falsos criados ou operados por robôs para fins de aumento de popularidade são assim denominados para fins de diferenciação neste trabalho.

A finalidade desses perfis é tornar um usuário real mais “popular” na Internet. Há empresas que criam perfis falsos e vendem em massa para usuários que queiram exercer mais influência nas redes sociais.

Isso porque há uma “cultura cibernética” nas redes sociais de que, com um grande número de seguidores, retuítes (quando alguém compartilha algo dito por outra pessoa no Twitter), curtidas e comentários em suas publicações, maior sua influência no mundo digital.

Temos como exemplo o caso investigado pelo jornal *New York Times* em relação a uma empresa designada Devumi, que vendia seguidores na rede social *Twitter*. Segundo o *New York Times* a empresa detinha cerca de 200 milhões de contas falsas, sendo que 3.5 milhões delas foram criadas automaticamente e poderiam ser vendidas várias vezes.[24]

Outro tipo de perfil falso criado são aqueles responsáveis pelo compartilhamento de conteúdos falsos como se verdadeiros fossem. Popularmente chamados de *fake news.*

[24] CONFESSORE, Nicholas; DANCE, Gabriel; HARRIS, Richard. The Follower Factory. *The New York Times.* New York, 7 jan. 2018. Disponível em: < https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html> Acesso em: 07.05.2021.

São diversos os tipos de mentiras divulgadas por esse tipo de perfil. Claire Wardle[25] categorizou as *fake news* da seguinte forma:

a) sátira/paródia: caso em que não há intenção de enganar, mas possui um potencial de enganar pessoas;
b) falsa conexão: associar a uma imagem, título ou legenda a algo que não possui conexão alguma;
c) conteúdo enganoso: atribuir falsa informação a uma pessoa ou assunto;
d) falso contexto: quando um conteúdo verdadeiro é associado a um contexto que distorce sua essência;
e) conteúdo impostor: informações falsas divulgadas e atribuídas a fontes reais que, na verdade, não foram as verdadeiras criadoras do conteúdo;
f) conteúdo manipulado: uma informação verdadeira manipulada propositalmente a enganar;
g) conteúdo fabricado: conteúdo total ou parcialmente falso, intencionalmente criado a gerar desinformação.

Esse assunto tem ficado cada vez mais evidente na mídia. Isso porque essas *fake news* possuem um potencial destrutivo de imagem, bem como de construir uma imagem. Influenciam na política, nas relações sociais, na economia e em diversos setores da vida humana que operam de acordo com as informações divulgadas.

Na política temos observado diversas investigações no sentido de que políticos se utilizavam desse recurso para prejudicar seus adversários durante as campanhas eleitorais.

Segundo matéria do UOL, foram identificadas diversas contas de *whatsapp*, criadas e manejadas por robôs, que disparavam *fake news* em prol do atual Presidente da República, bem como de forma pejorativa de seus adversários políticos na época

[25] WARDLE, Claire. Fake news. It's complicated. *First Draft*, New York, 16 fev. 2017. Disponível em: < https://firstdraftnews.org/latest/fake-news-complicated/> Acesso em: 07.06.2021.

de campanha eleitoral. Ainda, sabe-se que muitas dessas contas continuam operando até o momento.[26]

Segundo artigo elaborado por duas procuradoras do Ministério Público Federal[27], a divulgação de boatos não caracteriza, por si só, crime. A não ser que nesses "boatos" contenham delitos de calúnia, injúria ou difamação, bem como o crime de racismo etc.

Já os perfis humorísticos, costumeiramente, seguem um modelo de um sujeito, personagem, indivíduo ou entidade real, com o nome e imagem de perfil iguais ao do que supostamente teria o personagem do perfil criado. Possuem como objetivo a postagem de frases irônicas e *posts* sarcásticos.

1.2.4 Perfis falsos criminosos e a definição de crimes próprios e impróprios na internet

O presente tópico se dedica a detalhar um pouco mais sobre práticas criminosas comumente cometidas por perfis falsos nas redes sociais, fazendo uma breve demonstração da tipificação penal de cada um desses crimes.

Antes de darmos início ao aprofundamento do tema, faz-se necessário diferenciar crimes cometidos na Internet e crimes contra a Internet.

Segundo a definição do Professor Damásio, podemos ter um crime-meio e um crime-fim. Vejamos:

[26] MILITÃO, Eduardo; REBELLO, Aiuri. Rede de fake news com robôs pró-bolsonaro mantém 80% das contas ativas. *UOL*. Brasília, 19 set. 2019. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2019/09/19/fake-news-pro-bolsonaro-whatsapp-eleicoes-robos-disparo-em-massa.htm> Acesso em: 07.05.2021

[27] OLIVEIRA, Neide M. C. Cardoso; GOÉS, Silvana Batini (ed.). *FAKE NEWS e COMO INVESTIGAR.* Rio de Janeiro: Ministério Público Federal, 2018. p.2 Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/orientacoes/documentos/11-texto-sobre-fake-news-gacc.pdf> Acesso em: 09/04/2021

> O crime virtual pode ser um crime-meio, mas vem se desenvolvendo como crime-fim, o que demandou, aliás, a tipificação de alguns crimes informáticos próprios, com a edição das Leis n. 12.735/2012 e n. 12.737/2012. Ademais, não só hackers podem praticar um crime-fim informático, mas qualquer pessoa.
>
> [...]
>
> Fato é que a maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não.[28]

Assim, a pessoa pode utilizar a Internet para praticar crimes que poderiam ser praticados no mundo físico, como crimes contra a honra, incitação à violência, pedofilia entre outros.

Crime contra a Internet é aquele que o usuário pratica um delito que prejudique uma rede ou uma base de dados.

Entre os exemplos desse tipo de crime estão: disseminação de vírus, invasão de sistemas, *phishing* etc.

Segundo Olivo, *phishing* é a técnica que se utiliza da engenharia social para fazer suas vítimas, persuadindo-os com objetivos de capturar as informações pessoais e depois usá-las de forma a causar-lhes prejuízos. [29]

Marcelo Crespo faz essa divisão entre crimes virtuais próprios e impróprios. Vejamos:

> Neste sentido, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados) são delitos de risco informático ou próprios, ao passo que aquelas outras condutas que se dirigem contra bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.
> Os crimes virtuais próprios são crimes que somente podem ser praticados pela internet, ou seja, condutas que somente podem ser realizadas através da rede mundial de computadores.

---

[28] JESUS, Damasio Evangelista de; OLIVEIRA, Jose Antonio M Milagre de. *Manual de crimes informáticos*. 1ª ed. São Paulo: Saraiva. 2015. p. 49

[29] OLIVO, CK. *Avaliação de características para detecção de phishing de email.* Dissertação(mestrado), Pontifícia Universidade Católica do Paraná, Curitiba, 2010. P. 1. Disponível em: < https://www.ppgia.pucpr.br/pt/arquivos/mestrado/dissertacoes/2010/cleber_kiel_olivo_-_final.pdf> Acesso em: 07.05.2021

> Os crimes virtuais próprios também podem ser definidos como conduta praticada contra bens jurídicos informáticos
> Entretanto, o bem jurídico tutelado nos crimes virtuais próprios, no entendimento de Silveira, o qual destaca o artigo 154-A, o qual é abordado no tópico seguinte, "chega-se ao bem jurídico tutelado como sendo a liberdade individual, a privacidade e a intimidade das pessoas como um todo".
> Neste diapasão, pode-se complementar que são crimes que violam inicialmente a informação ou a privacidade como bem jurídico principal, e que de forma secundária atingem os dados ou sistemas.
> Os crimes virtuais impróprios são condutas já conhecidas, crimes já de conhecimento da sociedade, uma vez que já são tipificados pelo ordenamento jurídico penal e que podem ser praticados por qualquer meio, inclusive pela internet.
> Logo, este tipo de crime além de ser o já tradicionalmente tipificado no ordenamento agregando o uso de modernas tecnologias, representa que os ilícitos penais tradicionais, outrora tipificados, podem ser cometidos de uma nova forma, ou seja, por meio de novo *modi operandi.* [30]

Neste diapasão, Patrícia Peck explana como é importante que existam normas capazes de regulamentar essas e outras condutas na internet:

> Alguns podem alegar que ideal é a liberdade total, a falta justamente de regras. Bem, pode até funcionar, mas se em algum momento alguém se indispuser com outro e a situação parar na justiça, vai fazer falta não ter criado a regra do jogo e não ter passado ela no próprio jogo, de forma clara, objetiva, entre os participantes. Na era da informação, é a própria informação que garante a proteção legal.[31]

Assim, a internet pode ser o meio pelo qual se comete um crime ou, ainda, ser o alvo da conduta danosa. Em ambos os casos as normas devem existir como forma de tentar minimizar tais condutas, bem como puni-las adequadamente de acordo com o caso concreto.

1.2.4.1 Cyberstalkers

Uma das práticas muito preocupante na internet é o *stalking*, ou, em português, a perturbação.

[30] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais***.** São Paulo. Saraiva, 2011. p. 57 a 87
[31] PINHEIRO, Patrícia Peck*. Direito Digital*. São Paulo: Saraiva, 2016. p.451

Segundo o psicólogo J. Reid Meloy[32], o *cyberstalking* é o que chamamos quando há uma invasão indesejada na vida de alguém por meio da internet.

Marcelo Mazzola[33] explica que essa prática pode ser incentivada por três fatores: possibilidade de contato com mais pessoas, inclusive as desconhecidas, comunicação à distância e a garantia do anonimato.

Luciana Amiky[34], em seu trabalho acadêmico, acrescenta mais uma vantagem desse meio: a própria vítima oferece recursos para tanto, expondo suas fotos, dados, rotina, etc.

Até então, não tínhamos uma legislação específica para esse tipo de crime. O que dificultava e muito o trabalho de tentar punir aqueles que praticavam o *stalking.* Uma vez que nossa legislação Penal, bem como todo nosso ordenamento jurídico, obedece ao princípio da reserva legal, previsto no artigo 5º, II da Constituição Federal, em que ninguém será obrigado a fazer ou deixar de fazer algo senão em virtude de lei.

Porém, no dia 31 de março de 2021 foi sancionada a Lei nº 14.132/2021, que tipificou o Crime de perseguição.

A lei acrescentou ao artigo 147 do Código Penal, em que se prevê o crime de ameaça, o crime de perseguição, passível de pena de reclusão de seis meses a dois anos. Ainda, passível de causa de aumento nos casos em que a perseguição se der em razão do sexo feminino.

[32] MELOY, J. Reid. *The psychology of stalking.* San Diego: Elsevier Science, 1998. p. 10
[33] MAZZOLA, Marcello Adriano. *I nuovi danni.* Padova: Dott. Antonio Milini, 2008, p.1050
[34] AMIKY, Luciana Gerbovic. *Stalking*. 2014. Dissertação (Mestrado em Direito) – Pontífica Universidade Católica de São Paulo, São Paulo, 2014. p. 11-13

Segundo informações da UOL[35], a Lei estava em tramitação desde 2019, tendo sua pena agravada quando passou pelo trâmite de aprovação na Câmara dos Deputados.

Importante salientar que essa Lei revogou o artigo 65 da Lei de Contravenções Penais, que previa a possibilidade de punição pela perturbação da tranquilidade de alguém. Porém, com uma pena muito mais branda. Esse ponto será de suma importância para quando formos analisar jurisprudências que julgaram no sentido de condenação com base nesse artigo.

Portanto, tendo em vista a garantia do anonimato oferecido pelo uso de um perfil falso, a prática do *cyberstalking* tem se tornado cada vez mais comum no meio social.

1.2.4.2 Divulgadores de discursos de ódio

Segundo Rosane Leal, podemos caracterizar o discurso de ódio da seguinte forma, *in verbis:*

> [...]o discurso do ódio refere-se a palavras que tendem a insultar, intimidar ou assediar pessoas em virtude de sua raça, cor, etnicidade, nacionalidade, sexo ou religião, ou que têm a capacidade de instigar violência, ódio ou discriminação contra tais pessoas
> [...]
> Ele também pode ser definido como "uma manifestação segregacionista, baseada na dicotomia superior (emissor) e inferior (atingido) e, como manifestação que é, passa a existir quando é dada a conhecer por outrem que não o próprio autor. [36]

[35] DUARTE, Marcella. O que é stalking? Prática comum na web agora é crime que prevê prisão. *Tilt*, São Paulo, 01 abr. 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/04/01/curte-stalkear-pratica-agora-e-crime-e-pode-dar-tres-anos-de-prisao.htm>. Acesso em: 09.04.2021.

[36] SILVA, Rosane Leal et al. Discurso de ódio em redes sociais*:* jurisprudência brasileira. *Revista Direito GV*, São Paulo, v. 14, 2011. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/23964/22729> Acesso em: 09/04/2021.

De acordo com o que foi analisado pelos Termos de Uso das principais plataformas utilizadas como redes sociais, a criação de um perfil falso não é, necessariamente, uma violação, mas sim a finalidade para qual o perfil foi criado. Porém, estariam em desacordo com esses Termos quando houvesse uma propagação de discurso de ódio através desses perfis e, ainda, quando estes utilizassem de informações pessoais de perfis reais para aplicação de atividades ilícitas. [37]

Segundo Fábio Camelo[38], o anonimato aumenta a sensação de que não será punido pelos seus feitos, incentivando essa prática.

Quais crimes poderiam ser cometidos em um discurso de ódio? Levando em consideração ao conceito de Rosane Leal, tendo em vista uma ofensa a raça, cor, etnia, nacionalidade, sexo ou religião, podemos vislumbrar a Lei 7.715/89 em seu art. 1º, que prevê punição de reclusão de dois a cinco anos para quem comete essas práticas.

Ocorre que, não vislumbramos nesse artigo nada com relação à ofensa quanto à orientação sexual e identidade de gênero.

Em pesquisa no site do Senado Federal verifica-se que há um Projeto de Lei nº 672/2019 tramitando para alterar a referida Lei e, então, acrescentar quanto à ofensa à orientação sexual e à identidade de gênero.

Christiano e Cristina Victor, comentaram quanto à criminalização da LGBTfobia pelo Supremo Tribunal Federal, vejamos:

> Em razão do evidente atraso legislativo, o Supremo Tribunal Federal (STF) acabou sendo provocado a fim de se posicionar na proteção das pessoas

[37] ARROYO, Danilo Wohnrath. *A criação de perfil falso nas redes sociais Facebook e Twitter*: motivações e tipos. Araranguá. 2019. P. 29. Disponível em: <https://repositorio.ufsc.br/handle/123456789/203028> Acesso em 01.12.2020.
[38] CAMELO, Fábio Assunção Berlim. *Detecção Automática de Discursos de Ódio em Comentários de Jornais Online*. Dissertação (Bacharelado em Ciências da Computação) – Universidade Federal Fluminense, Rio de Janeiro, 2017. P. 9. Disponível em: < https://app.uff.br/riuff/bitstream/1/5753/1/tcc-fabio-assuncao-berlim-camelo.pdf> Acesso em: 07.05.2021.

> pertencentes ao grupo LGBT, por meio de duas ações constitucionais: o Mandado de Injunção nº 4733, de 2012, movido pela Associação Brasileira de Lésbicas, Gays, Bissexuais, Travestis, Transgêneros e Intersexos (ABGLT) e a Ação Direta de Inconstitucionalidade por Omissão (ADO) nº 26, movida pelo Partido Popular Socialista (PPS), em 2013. Em junho de 2019 concluiu-se o julgamento conjunto de ambas as ações pelo Supremo Tribunal Federal. Os votos dos ministros (notadamente o mais longo deles, do decano da Corte, Celso de Mello), todavia, permitem diversas reflexões jurídicas, principalmente acerca dos fundamentos, dos efeitos e das implicações penais decorrentes do julgamento.[39]

Após o julgamento dessas demandas, tivemos o seguinte resultado, na palavras de Christiano e Cristina Victor:

> O Tribunal, por unanimidade, conheceu parcialmente da ação direta de inconstitucionalidade por omissão. Por maioria e nessa extensão, julgou-a procedente, com eficácia geral e efeito vinculante, para: a) reconhecer o estado de mora inconstitucional do Congresso Nacional na implementação da prestação legislativa destinada a cumprir o mandado de incriminação a que se referem os incisos XLI e XLII do art. 5º da Constituição, para efeito de proteção penal aos integrantes do grupo LGBT; b) declarar, em consequência, a existência de omissão normativa inconstitucional do Poder Legislativo da União; c) cientificar o Congresso Nacional, para os fins e efeitos a que se refere o art. 103, § 2º, da Constituição c/c o art. 12-H, caput, da Lei nº 9.868/99; d) dar interpretação conforme à Constituição, em face dos mandados constitucionais de incriminação inscritos nos incisos XLI e XLII do art. 5º da Carta Política, para enquadrar a homofobia e a transfobia, qualquer que seja a forma de sua manifestação, nos diversos tipos penais definidos na Lei nº 7.716/89, até que sobrevenha legislação autônoma, editada pelo Congresso Nacional, seja por considerar-se, nos termos deste voto, que as práticas homotransfóbicas qualificam-se como espécies do gênero racismo, na dimensão de racismo social consagrada pelo Supremo Tribunal Federal no julgamento plenário do HC 82.424/RS (caso Ellwanger), na medida em que tais condutas importam em atos de segregação que inferiorizam membros integrantes do grupo LGBT, em razão de sua orientação sexual ou de sua identidade de gênero, seja, ainda, porque tais comportamentos de homotransfobia ajustam-se ao conceito de atos de discriminação e de ofensa a direitos e liberdades fundamentais daqueles que compõem o grupo vulnerável em questão; e e) declarar que os efeitos da interpretação conforme a que se refere a alínea “d” somente se aplicarão a partir da data em que se concluir o presente julgamento [...][40]

[39] SANTOS, Chistiano Jorge; GARCIA, Cristina Victor. A Criminalização Dalgbtfobia Pelo Supremo Tribunal Federal do Brasil. *Revista Direito UFMS.* Mato Grosso do Sul, v. 5, n.2, 2019. P. 294-317. Disponível: <https://periodicos.ufms.br/index.php/revdir/article/view/9845> Acesso em: 07/05/2021.
[40] Ibid, p. 317.

Sendo assim, vislumbramos mais crimes comumente cometidos por perfis falsos na Internet, haja vista que a intenção é ofender e não ser punido, sabendo que poderia ser nos termos da Lei.

1.2.4.3 Chantagistas

Outro tipo de perfil falso é aquele criado com a finalidade de extorsão mediante ameaças de divulgação de fotos ou vídeos íntimos na internet.

Esse crime, inclusive, pode estar associado ao crime de *stalking* visto no tópico 1.2.4.1.

Podemos ver um exemplo desse tipo de situação, segundo reportagem do G1[41], que conta que os criminosos se passavam por mulheres para trocar mensagens íntimas e depois, fingiam serem policiais para fazer ameaças.

Há também casos em que criminosos invadem o computador ou celular das vítimas, roubam suas fotos e depois as chantageiam através de perfis falsos.

Um caso que ficou muito famoso na mídia, foi o caso da atriz Carolina Dieckmann, que, segundo reportagem do G1[42], recebeu ameaças de extorsão de divulgação de fotos suas através de um e-mail com o endereço vempropapai200101@hotmail.com, ou seja, um perfil falso, visto que não possibilita a identificação do remetente. Como os criminosos obtiveram essas fotos ainda é um mistério sendo investigado, porém, acredita-se que eles invadiram o computador da atriz.

---

[41] GRIZOTTI, Giovani. Golpistas usam perfis falsos nas redes sociais para extorquir dinheiro de vítimas no RS. *G1*. Rio Grande do Sul, 23 set. 2019. Disponível em: <https://g1.globo.com/rs/rio-grande-do-sul/noticia/2019/09/23/golpista-usam-perfis-falsos-nas-redes-sociais-para-extorquir-dinheiro-de-vitimas-no-rs.ghtml> Acesso em: 07.05.2021.

[42] SUSPEITOS DO ROUBO DAS FOTOS DE CAROLINA DIECKMANN SÃO DESCOBERTOS. *G1*. Rio de Janeiro, 13 mai. 2012. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html> Acesso em: 07.05.2021.

Após o ocorrido e devido à grande repercussão do caso, foi editada e sancionada a Lei nº 12.737, de 30 de novembro de 2012 - Lei Carolina Dieckmann, que inclui o crime de invasão de dispositivo informático ao Código Penal em seu artigo 154.

Nessa lei podemos claramente visualizar que se trata de um crime próprio, conforme conceito abordado por Marcelo Crespo e demonstrado no tópico 1.2.4 deste trabalho.

Temos também o crime de extorsão previsto no artigo 158 do Código Penal e que pode ser aplicado em ambos os casos.

1.2.4.4 Praticantes de outros crimes

Segundo nos conta Felipe e Marcelo[43], um dos crimes mais comumente cometido na internet na sociedade moderna é a pornografia infantojuvenil. Em que se tem um ambiente facilitador de distribuição de material relacionado.

Eles ainda elaboraram uma tabela com os principais crimes cometidos na Internet e suas respectivas tipificações. Vejamos:

[43] CAIADO, Felipe; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: Ministério Público Federal. *Crimes Cibernéticos.* Brasília: 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018. p. 11. Disponível em: < https://memorial.mpf.mp.br/ce/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos> Acesso em: 07.05.2021.

Tabela 1 - Principais crimes cometidos na Internet e suas respectivas tipificações.

Crime	Tipificação
Estelionato e furto eletrônicos (fraudes bancárias)	arts. 155, §§ 3º e 4º, II, e 171 do CP
Invasão de dispositivo informático e furto de dados	art. 154- A do CP
Falsificação e supressão de dados	arts. 155, 297, 298, 299, 313-A, 313-B do CP
Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infantojuvenil	arts. 241 e 241-A, do ECA (Lei nº 8.069/1990)
Assédio e aliciamento de crianças	art. 241-D, do ECA (Lei nº 8.069/1990)
Ameaça	art. 147 do CP
Cyberbullying (veiculação de ofensas em blogs e comunidades virtuais)	arts. 138, 139, 140 do CP
Interrupção de serviço	art. 266, parágrafo 1º, do CP
Incitação e apologia de crime	arts. 286 e 287 do CP
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	art. 20 da Lei nº 7.716/1989
Crimes contra a propriedade intelectual artística e de programa de computador	art. 184 do CP e Lei nº 9.609/1998
Venda ilegal de medicamentos	art. 273 CP

Fonte: MPF, 2018.

Assim, podemos visualizar que diversos são os crimes praticados na internet e, muitos deles, são praticados através de perfis falsos em rede sociais, demonstrando a grande relevância do tema.

2. RESPONSABILIZAÇÃO PENAL PELA CRIAÇÃO DE PERFIL FALSO NAS REDES SOCIAIS CONTEMPORÂNEAS NA INTERNET

O presente tópico se dedicará ao estudo da responsabilização penal dos usuários que se utilizam de perfis falsos em redes sociais para o cometimento de crimes na internet.

2.1. OS CRIMES DE FALSIDADE IDEOLÓGICA E FALSA IDENTIDADE NO ORDENAMENTO BRASILEIRO

Os crimes de Falsidade Ideológica e Falsa Identidade estão tipificados nos artigos 299 e 307 do Código Penal, respectivamente, em que temos as seguintes redações:

> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
>
> Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, de quinhentos mil réis a cinco contos de réis, se o documento é particular.[44]
>
> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.(g.n.)[45]

Guilherme Nucci explica a intenção do artigo 299 do Código Penal nos seguintes termos:

> O crime de falsidade ideológica é o ato de omitir, ou seja, deixar de inserir ou não mencionar, em documento público ou particular, declaração dissociada da realidade que neste documento deveria constar, ou ainda inserir ou fazer inserir falsa ou diversa declaração que deveria ser escrita,

[44] BRASIL. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 07 dez. 1940. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em 14.03.2021.
[45] BRASIL. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 07 dez. 1940. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em 14.03.2021.

> com o objetivo de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante[46].

Porém, as dúvidas que ficam são as seguintes: um perfil falso pode ser equiparado a uma declaração dissociada da realidade? Ainda, o que é um fato juridicamente relevante?

É mister a resposta de tais perguntas para que possamos pensar no enquadramento da prática ao tipo penal supracitado, o que analisaremos mais adiante.

Quanto ao crime de falsa identidade, tipificado no artigo 307 do Código Penal, pode ser explorado da seguinte forma, segundo os autores Emerson e Higor: “Ação de se atribuir ou atribuir a outra pessoa falsa identidade para obter vantagem em proveito próprio ou de outro indivíduo ou para proporcionar algum dano.”[47]

Assim, quanto ao referido dispositivo, vemos que o ponto central para a possibilidade de enquadrarmos da conduta de criação de perfil falso ao tipo penal é se, necessariamente, deve haver uma finalidade danosa.

Explanados os referidos tipos penais, visualizaremos, mais à frente, quanto à possibilidade de enquadramento da conduta de criação de perfil falso aos crimes de falsidade ideológica e/ou falsa identidade.

2.1.1 Perfis falsos nas redes sociais contemporâneas na internet e os crimes de falsidade ideológica e falsa identidade

Diante do já exposto, abordaremos uma análise quanto ao uso de perfis falsos e os crimes de falsidade ideológica e falsa identidade.

O presente tópico pode ser considerado um dos pontos centrais deste trabalho, uma vez que o intuito do mesmo é trazer a implicações jurídicas, mais

[46] NUCCI, Guilherme de Souza. *Manual do Direito Penal.* 7ª ed. São Paulo. Revista dos Tribunais, 2011. p. 989.
[47] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes Cibernéticos***.** Ameaças e Procedimentos de Investigação. Rio de Janeiro. Brasport, 2012. p. 105

especificamente no ramo do Direito Penal, quanto à criação de perfis falsos nas redes sociais.

No tópico 2.1, pudemos observar quanto aos artigos 299 e 307 do Código Penal, referentes aos crimes de falsidade ideológica e falsa identidade, respectivamente.

Vimos que, para enquadrar a criação de perfis falsos ao crime de falsidade ideológica, precisaríamos responder às seguintes perguntas: um perfil falso pode ser equiparado a uma declaração dissociada da realidade? Ainda, o que é um fato juridicamente relevante?

Para Patrícia Peck, tudo que é preenchido em cadastros na Internet tem característica declaratória[48], respondendo à nossa primeira pergunta no sentido que, um perfil falso, ao preencher os dados com informações falsas está incorrendo em uma declaração dissociada da realidade.

Com relação ao fato juridicamente relevante, temos uma questão muito subjetiva, mas que caminha no sentido de, dolosamente, prejudicar alguém. Vejamos o que diz Edgar Magalhães Noronha: “é mister que a declaração falsa constitua elemento substancial do ato de documento. Uma simples mentira, mera irregularidade, simples preterição de formalidade etc., não constituirão.”[49]

Assim, adotamos a ideia de que é possível enquadrar a ação ao tipo penal, porém, dependerá de caso a caso, uma vez que é essencial para configuração do delito a finalidade com que aquele perfil foi criado.

Com relação ao crime de falsa identidade, previsto no artigo 307 do Código Penal, a questão central para enquadrar a criação de perfil falso ao tipo penal também é quanto à finalidade do ato, uma vez que o texto penal nos traz, como pré-requisito, a intenção de obtenção vantagem própria ou alheia.

[48] PINHEIRO, Patrícia Peck. *Direito Digital.* São Paulo: Saraiva, 2016. p. 450
[49] NORONHA, Edgard Magalhães. *Direito Penal*. São Paulo: Rideel, 1980 17 ed., vol. 4, p. 161

Então, já que para ambos os tipos penais há a necessidade de se averiguar a finalidade da criação do perfil, como podemos diferençar uma situação da outra?

Segundo Nathalia Paz[50], a diferença entre os dois tipos penais está no fato de que, no crime de falsa identidade, a pessoa se passa por uma outra pessoa que existe, ou seja, utiliza dados de alguém e se faz passar por ela, enquanto que, no crime de falsidade ideológica, a pessoa adultera uma declaração ou documento.

Ou seja, quando alguém se faz passar por outra pessoa, comete o crime de falsa identidade, já quando adultera informações sobre si para que não seja identificado, não necessariamente se passando por outra pessoa, comete o crime de falsidade ideológica.

No sentido da caracterização de falsa identidade na criação de perfis falsos, Eliane ressalta:

> [...] Situação mais grave é quando perfil falso é utilizado para difamar e ofender pessoas, propalando informações falsas sobre ela ou utilizando o perfil para prática de atos ilegais, de modo que a situação deverá ser analisada sob o crivo do Direito Penal. Nesse ponto, cabe ressaltar, ainda, que, caso o fato não constitua crime mais grave (a exemplo de estelionato e pedofilia), a utilização de perfil falso configura crime de falsa identidade, previsto no artigo 307 do Código Penal.
>
> Portanto, se a circunstância de uso do perfil falso ilustra um caso de utilização indevida de identidade e imagem, a toda evidência está presente uma situação não só de anonimato, mas também de fato típico para responsabilização na esfera criminal.[51]

[50] PAZ, Nathália. O que é falsidade ideológica? *Identidade*, IdBlog, São Paulo, 2020. Disponível em: <https://blog.idwall.co/o-que-e-falsidade-ideologica/#:~:text=A%20falsidade%20ideol%C3%B3gica%2C%20como%20falado,pessoa%20se%20passa%20por%20outra.> Acesso em 07.04.2021

[51] FONTANA, Eliane; COSER, *Thomas Felipe. Perfil Falso na Rede e o Anonimato*: Uma Visão (Polêmica) À Luz Do Marco Civil Da Internet. In: SEMINÁRIO INTERNACIONAL: DEMANDAS SOCIAIS E POLÍTICAS NA SOCIEDADE CONTEMPORÂNEA, VIII Mostra de trabalhos jurídicos científicos, 2015. Rio Grande do Sul: Universidade de Santa Cruz do Sul, 2015. Disponível em: < https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13174/2387> Acesso em: 18.10.2020. p. 12

2.1.2 Concurso de crimes e os perfis falsos nas redes sociais contemporâneas na internet

Segundo o Professor Damásio[52], quando um sujeito, mediante unidade ou pluralidade de ações ou de omissões, pratica dois ou mais delitos, surge o concurso de crimes ou de penas (*concursus delictorum*).

O Concurso de crimes pode ser de três tipos: material, formal ou crime continuado. Estão previstos nos artigos 69; 70 e 71 do Código Penal, respectivamente.

Concurso material é aquele cometido por agente que, mediante mais de uma conduta, pratica dois ou mais crimes. Se idênticos, trata-se de concurso material homogêneo, se não, heterogêneo. Ainda, o artigo 69 do CP prevê que as penas devem ser cumulativas.

Concurso formal é quando há apenas uma conduta, porém, mais de um crime. Também pode ser homogêneo, quando os crimes estão no mesmo tipo penal ou heterogêneos quando são crimes diferentes.

Para haver concurso de crime formal, é necessário que haja pluralidade de crimes e uma unidade de comportamento.

Quanto à aplicação das penas, segundo os parágrafos do artigo 70, se as penas são idênticas, aplica-se uma só, aumentada de um sexto até metade; se as penas não são idênticas, aplica-se a mais grave, aumentada de um sexto até metade.

Segundo o Professor Damásio, temos crime continuado quando:

> ocorre o denominado crime continuado quando o agente, mediante mais de uma ação ou omissão, pratica dois ou mais crimes da mesma espécie e, pelas condições de tempo, lugar, maneira de execução e outras

[52] JESUS, Damásio Evangelista de. *Direito penal 1*: parte geral. 37ª ed. São Paulo: Saraiva. 2020 p.617

> semelhantes, devem os subsequentes ser havidos como continuação do primeiro. [53]

Segundo Andreucci[54], são requisitos do crime continuado: pluralidade de condutas; pluralidade de crimes da mesma espécie; continuação, tendo em vista as circunstâncias objetivas; e unidade de desígnio.

A natureza jurídica desse crime pode ser conceituada da seguinte forma, segundo o Professor Damásio, *in verbis:*

> O legislador presume a existência de um só crime; Por medida de Política Criminal, é aceita a teoria da ficção jurídica. Embora haja pluralidade de crimes, a lei presume a existência de crime único. Essa presunção, entretanto, só tem relevância na aplicação da pena. Para outros efeitos o delito continuado é considerado forma de concurso de crimes.[55]

O Código Penal determina duas regras quanto à aplicação de pena nesse caso: se as penas são idênticas, aplica-se uma só, com o aumento de um sexto a dois terços; se as penas são diversas, aplica-se a mais grave, aumentada de um sexto a dois terços.

Iniciados aos conceitos pertinentes ao crime continuado, podemos relacionar quanto aos perfis falsos nas redes sociais. Uma vez que, vemos que, tanto crime de falsa identidade, quanto no crime de falsidade ideológica, deve haver uma finalidade vantajosa para o criminoso.

Assim, o indivíduo que cria um perfil falso em uma rede social, passando-se ou não por outra pessoa, e comete um crime, deve incorrer no concurso de crimes, sendo a espécie a depender do caso concreto.

Condenar uma pessoa apenas por criar um perfil falso pode não ser a melhor saída, porém, ao condená-la por um crime que cometeu através desse perfil e

---

[53] Ibid, p.625-628
[54] ANDREUCCI, Ricardo Antonio. *Manual de direito penal*: de acordo com a Lei n. 13.869, de 2019, Lei de Abuso de Autoridade. 14. São Paulo Saraiva 2019 1 recurso online ISBN 9788553616329. p. 193
[55] JESUS, Damásio Evangelista de. *Direito penal 1*: parte geral. 37ª ed. São Paulo: Saraiva. 2020. p.625-628

simplesmente ignorar o fato de que ela se beneficiou do anonimato virtual, inclusive dificultando a investigação criminal, também não é.

Ou seja, os Tribunais poderiam levar em consideração os crimes de falsidade ideológica ou falsa identidade para cominar penas, no caso de concurso de crime material ou aumentá-las, nos casos de concurso de crime formal ou crime continuado.

2.2 ANÁLISE JURISPRUDENCIAL NO ÂMBITO PENAL

Após toda a pesquisa doutrinária, agora podemos nos dedicar à jurisprudencial, na qual podemos visualizar que diversos casos de tentativa de enquadrar a criação de perfil falso aos crimes de falsidade ideológica ou falsa identidade, não lograram êxito na condenação. Vejamos alguns exemplos:

> APELAÇÃO CRIMINAL. CRIME CONTRA A FÉ PÚBLICA (ART. 299,"CAPUT", DO CÓDIGO PENAL). SENTENÇA CONDENATÓRIA. RECURSO DA DEFESA. PLEITO ABSOLUTÓRIO POR INSUFICIÊNCIA DE PROVAS. NÃO ACOLHIMENTO. PALAVRAS DA VÍTIMA UNÍSSONAS E HARMÔNICAS, EM AMBAS AS FASES DA PERSECUÇÃO CRIMINAL, CORROBORADAS PELA PROVA DOCUMENTAL AMEALHADA AO FEITO. ELEMENTOS PROBATÓRIOS SUFICIENTES PARA EMBASAR O ÉDITO CONDENATÓRIO. PEDIDO DE RECONHECIMENTO DA ATIPICIDADE DO FATO. IMPOSSIBILIDADE. CONDUTA FORMAL E MATERIALMENTE TÍPICA. HIPÓTESE, NO ENTANTO, DE "EMENDATIO LIBELLI". ELEMENTARES DO TIPO PENAL DA FALSIDADE IDEOLÓGICA NÃO PREENCHIDOS. APELANTE QUE FEZ INSERIR DECLARAÇÃO FALSA EM PERFIL DE INTERNET, A FIM DE PREJUDICAR IMAGEM DE EX-COMPANHEIRA E PERTURBAR-LHE A TRANQUILIDADE. AÇÃO QUE MELHOR SE AMOLDA A CONTRAVENÇÃO PENAL PREVISTA NO ART. 65, DO DECRETO-LEI N. 3.688/41. REDEFINIÇÃO JURÍDICA EFETUADA DE OFÍCIO, COM A READEQUAÇÃO DA REPRIMENDA. POR ESSAS RAZÕES, INVIÁVEL A DESCLASSIFICAÇÃO PARA O CRIME DE FALSA IDENTIDADE. INFRAÇÃO DE MENOR POTENCIAL OFENSIVO. REMESSA DOS AUTOS AO JUÍZO DE ORIGEM. PLEITO SUBSIDIÁRIO DE RECONHECIMENTO DA PRESCRIÇÃO DA PRETENSÃO PUNITIVA DO ESTADO, EM

> CONCRETO, PREJUDICADO. RECURSO CONHECIDO E NÃO PROVIDO. DE OFÍCIO, READEQUAÇÃO TÍPICA DA CONDUTA. (TJ-SC, 2019, on-line) (g.n.)[56]

> APELAÇÃO CRIMINAL. ART. 299 DO CP. ELEMENTO SUBJETIVO ESPECÍFICO NÃO DEMONSTRADO. IN DUBIO PRO REO. RECURSO PROVIDO. O Juízo da 2ª Vara Federal de Franca/SP condenou o apelante como incurso nas sanções do art. 299 c/c art. 71, ambos do CP, pois, na condição de contador, inseriu informações ideologicamente falsas em perfis profissiográficos. Embora demonstradas a materialidade e a autoria, o conjunto probatório é insuficiente para demonstrar o elemento subjetivo específico do tipo penal do art. 299 do CP, consistente na finalidade de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Não há prova suficiente de que o réu dolosamente inseriu informações inverídicas nos PPPs. Também não há elementos indicativos de que o apelante e os corréus da ação penal nº 0001371-46.2015.403.6113 tenham agido com unidade de desígnios a fim de viabilizar o reconhecimento de atividade especial. Diante do quadro de incerteza, a dúvida deve ser revertida em benefício do acusado, em observância ao princípio do "in dubio pro reo". Recurso provido. (TRF-3, 2019, on-line) (g.n.)[57]

Em muitos casos, o julgamento se deu no sentido do artigo 65 da Lei de Contravenções penais. Porém, conforme vimos no tópico 1.2.4.1, esse texto penal já fora revogado. Vejamos:

> APELAÇÃO CRIMINAL - RECURSO DEFENSIVO - AMEAÇA - INTERNET - PROMESSA DE MAL INJUSTO E GRAVE CONFIGURADA - CONDENAÇÃO MANTIDA - PERTURBAÇÃO DA TRANQUILIDADE - CRIAÇÃO DE PERFIS FALSOS EM REDES SOCIAIS - PREJUÍZOS SOCIAIS CAUSADOS À VÍTIMA - MOTIVO REPROVÁVEL - RETOMADA DE RELACIONAMENTO AMOROSO - CONDENAÇÃO MANTIDA - ESTELIONATO - OBTENÇÃO DE VANTAGEM ECONÔMICA - ARDIL - FALSA IDENTIDADE VIRTUAL

[56] TJ-SC. APLEAÇÃO CRIMINAL: 00134605420148240023 Capital 0013460-54.2014.8.24.0023, Relator: Norival Acácio Engel, Data de Julgamento: 26/11/2019, Segunda Câmara Criminal. *JusBrasil*, 2019. Disponível em: <https://tj-sc.jusbrasil.com.br/jurisprudencia/794762222/apelacao-criminal-apr-13460542014824 0023-capital-0013460-5420148240023/inteiro-teor-794762227> Acesso em: 10.05.2021

[57] TRF-3.Apelação Criminal: 00045947020164036113, Relator: Desembargador Federal José Lunardelli, Data de Julgamento: 12/03/2019. Décima primeira turma. *JusBrasil,* 2019. Disponível em: < https://trf-3.jusbrasil.com.br/jurisprudencia/910083085/apelacao-criminal-ap-45947020164036113-sp>. Acesso em: 10.05.2021

- POSTERIOR REPARAÇÃO DO DANO - IRRELEVÂNCIA - INTELIGÊNCIA DA SÚMULA Nº 554, DO STF - CONDENAÇÃO MANTIDA - PENAS DE MULTA - ADEQUAÇÃO - RECURSO MINISTERIAL - AMEAÇA - PROMESSAS DE MAL INJUSTO E GRAVE PRATICADAS EM SEQUÊNCIA - CONTINUIDADE DELITIVA CONFIGURADA - ESTELIONATO - PENA-BASE - CIRCUNSTÂNCIAS ESPECIALMENTE GRAVES - EXACERBAÇÃO NECESSÁRIA PARA A REPRESSÃO E PREVENÇÃO DO CRIME - AGRAVAMENTO DO REGIME PRISIONAL - NÃO CABIMENTO - VEDAÇÃO À SUBSTITUIÇÃO DA PENA - INTELIGÊNCIA DA LEI 11.340/06. - Comete o crime de ameaça o indivíduo que envia mensagens eletrônicas à vítima, prometendo difamá-la gravemente em redes sociais e, ainda, sugerindo males indeterminados que poderiam acometer sua família. - A criação de perfis sociais falsos em redes sociais, por meio dos quais o agente se faz passar pela vítima e através dos quais difama pessoas de suas relações, além de publicar relatos indecorosos e infamantes em seu nome, configura a contravenção penal prevista no art. 65, da Lei de Contravencoes Penais. - A obtenção de depósitos bancários em nome do agente, obtidos através do ardil de criar perfis falsos de personagens virtuais para ludibriar a vítima, convencendo-a de que uma destas personagens necessita de ajuda financeira, configura a hipótese descrita no art. 171, caput, do Código Penal. - A fixação dos dias-multa deve ser aplicada proporcionalmente à magnitude do injusto penal, e o valor de cada dia-multa deve ser apurado em conformidade com a capacidade econômica do acusado. - A pena de multa deve ser destin ada ao Fundo Penitenciario Nacional, não podendo ser pago à vítima como forma de reparação do dano causado pelo crime, por inexistência de previsão legal. - Se as ameaças foram praticadas seguidamente, ao longo de todo um semestre e através de meios os mais variados e contendo promessas de males injustos e graves diversos em prejuízo da vítima, impõe-se o reconhecimento da continuidade delitiva, na forma do art. 71, do Código Penal. - Praticado o estelionato em condições especialmente reprováveis, tendo sido a vítima induzida a erro por seu amante ao longo de 04 (quatro) anos, com a criação de numerosos perfis virtuais falsos para mantê-la em erro e com absoluta desconsideração de sua estabilidade afetiva, impõe-se a aplicação da pena-base em quantum especialmente elevado. - O agravamento do regime prisional, uma vez preenchidos os requisitos previstos no art. 33, § 2º, c, exige que as circunstâncias sejam excepcionalmente desfavoráveis ao agente. - A vedação à substituição da pena corporal somente se autoriza, para o agente primário que não cometeu o crime com violência ou grave ameaça à pessoa, quando excepcionalmente graves as circunstâncias judiciais. - A vedação prevista na Lei Maria da Penha proíbe apenas a

> substituição da pena corporal por pena de natureza pecuniária isoladamente, restando autorizada, contrario sensu, a substituição por pena de prestação pecuniária cumulada com outra pena restritiva de direitos de natureza diversa. (TJ-MG, 2015, on-line) (g.n.) [58]

Não foram encontrados julgados que versassem apenas sobre a criação de perfis falsos e os crimes de falsidade ideológica ou falsa identidade, bem como não levam em consideração na aplicação da pena. Em todos os julgados encontrados, há crime ou crimes que foram cometidos através da utilização de perfis falsos, porém não houve a condenação pelos crimes de falsa identidade ou falsidade ideológica, apenas menção.

Ou seja, visulaizamos o que a doutrina chama de princípio da concussão, em que o crime de falsidade ideológica, reconhecido nesses casos, é “absorvido” pelo crime-fim cometido pelo usuário. Assim, o usuário acaba sendo condenado apenas pelo crime “final” e não pela falsa identidade ou falsidade ideológica ao criar o perfil falso em uma rede social.

[58] TJ-MG – Apelação Criminal: 10480110105404001 MG, Relator: Agostinho Gomes de Azevedo, Data de Julgamento: 20/08/2015. *JusBrasil*, 2015. Disponível em: <https://tj-mg.jusbrasil.com.br/jurisprudencia/225500906/apelacao-criminal-apr-10480110105404001-mg> Acesso em: 10.05.2021.

3. RESPONSABILIZAÇÃO CIVIL PELA CRIAÇÃO DE PERFIL FALSO NAS REDES SOCIAIS CONTEMPORÂNEAS NA INTERNET

A principal questão, referente ao tema em pauta neste trabalho, no ramo do Direito Civil, diz respeito à responsabilização por dano causado por um usuário a outro nas redes sociais.

Tendo em vista a dificuldade que se tem em identificar a pessoa “por trás” de um usuário, o principal alvo para responder por essa ação seria o provedor do site.

Ou então, até mesmo que *a posteriori* identificado, o provedor deve ser o requerido inicial, uma vez que só ele detém informações passíveis dessa identificação, bem como é o único capaz de retirar da rede o conteúdo ou usuário ofensivo, cabendo sua cooperação com a Justiça.

A responsabilidade dita neste presente tópico diz respeito não só ao pagamento de indenização, mas também quanto à exclusão desse usuário da rede, bem como a de responsabilidade pela fiscalização para evitar maiores danos.

Mais a frente traremos mais detalhes quanto às investigações conduzidas no sentido de identificar um usuário “escondido atrás” de um perfil falso nas redes sociais.

Ainda, traremos análises jurisprudenciais mais aprofundadas. Porém, podemos adiantar, nesse sentido, a contribuição de Eliane quanto ao posicionamento de nossos Tribunais:

> Uma é que a questão da remoção do conteúdo de um perfil na rede por meio de ação judicial é desnecessária quando ao servidor erige uma responsabilidade que lhe é afetada quando do recebimento das informações pessoais do usuário. Assim, quem deve de maneira imprescindível fiscalizar a correta conexão entre o conteúdo publicado e os dados referidos é o servidor. Nesse sentido já o era nas jurisprudências que antecederam a construção do marco civil, onde os Tribunais do país decidiram em muito sobre a culpa *in ommitendo* e culpa *in vigilando* do servidor que se recusava a retirar o conteúdo criminoso ou ilegal ou abusivo. Em suma: o servidor omitir em remover, ou por meio de seus filtros ou, por que provocado.[59]

[59] FONTANA, Eliane; COSER, Thomas Felipe. Perfil Falso Na Rede E O Anonimato: Uma Visão (Polêmica) À Luz Do Marco Civil Da Internet. In: SEMINÁRIO INTERNACIONAL: DEMANDAS SOCIAIS E POLÍTICAS NA SOCIEDADE CONTEMPORÂNEA, VIII Mostra de trabalhos jurídicos científicos, 2015. Rio Grande do Sul: Universidade de Santa Cruz do Sul, 2015. p. 13. Disponível em: < https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13174/2387> Acesso em: 18.10.2020.

Para Patricia Peck, a melhor forma de, minimamente, tentar se eximir de toda a responsabilidade pelos atos de seus usuários, é deixando bem claro nos termos de uso quanto à conduta que deve ser adotada, bem como criando ferramentas que dificultem a prática de criação de perfis falsos, através de autenticação por outros fatores que não só usuário e senha. [60]

Para analisar essa questão, é imprescindível trazer à baila o artigo 19 do Marco Civil da Internet, que determina o seguinte:

> Art. 19 Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.[61]

Assim, verificamos que há uma responsabilidade subsidiária e subjetiva dos provedores, uma vez que condicionada à não contribuição com a Justiça.

Segundo explica Victor Hugo[62], a responsabilização objetiva dos provedores inviabilizaria o direito de expressão por conta da censura prévia que os sites fariam na tentativa de não sofrerem sanções.

Em artigo publicado na Revista da Faculdade de Direito de São Paulo[63], podemos visualizar um resumo muito claro sobre o posicionamento dos tribunais brasileiros, bem como a demasiada exigência de diversos fatores de autenticação pode demandar ainda mais riscos aos provedores.

---

[60] PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2016. p. 449-450

[61] BRASIL. LEI Nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 23 abr. 2014. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 10.05.2021

[62] GONÇALVES, Victor Hugo Pereira. *Marco civil da internet comentado*. 1ªed. São Paulo: Atlas, 2017. p. 149

[63] REVISTA DA FACULDADE DE DIREITO DE SÃO PAUO: Regulação tecnológica e jurídica das redes sociais (*social networks).* São Paulo: Universidade de São Paulo, v. 100, jan/dez 2005.p. 631-634

É dito que no Brasil o posicionamento quanto à responsabilização dos provedores por ato de terceiro é muito controverso. Os casos em que os magistrados decidem por responsabilizá-los defendem que os *websites* apenas atuam como um classificado, divulgando relações as quais não possui qualquer vínculo ou responsabilidade, já o outro lado defende haver comissão paga quando o negócio se aperfeiçoa, atuando o *website* como intermediário e, portanto, o sujeito à responsabilidade solidária nos termos do Parágrafo único art. 7º do Código de Defesa do Consumidor, que diz o seguinte:

> Art. 7° Os direitos previstos neste código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e eqüidade.
>
> Parágrafo único. Tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo (g.n)[64]

Ainda, segundo o artigo 3 do mesmo Código, temos uma definição de fornecedor em que é possível enquadramento dos provedores, vejamos:

> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.[65]

Caso se entenda que o provedor se encaixa nessa descrição, teremos a aplicação da culpa objetiva pelos danos causados, nos termos do artigo 14 do Código de Defesa do Consumidor, ainda que em seu §3º, II esteja prevista a exclusão da culpa por culpa exclusiva de terceiro, uma vez que um usuário *fake* está na plataforma e causa danos a outros usuários através dela, gerando discussão quanto à consideração deste usuário como terceiro.

---

[64] BRASIL. LEI Nº 8.0878, de 11 de setembro de 1990. Código de Defesa do Consumidor. Diário Oficial da União, Brasília, DF, 11 set. 1990. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 10.05.2021

[65] Ibid

Ou seja, a discussão jurisprudencial e doutrinária gira em torno da aplicação do artigo 19 do MCI ou dos artigos 3 e 14 do Código de Defesa do Consumidor. A aplicação de um ou de outro dirá se o provedor deve ou não ser responsabilizado a pagar indenização à vítima de atos ilícitos praticados por perfis falsos.

3.1 ANÁLISE JURISPRUDENCIAL NO ÂMBITO CIVIL

Neste tópico traremos casos que permitam um estudo mais aprofundado do posicionamento dos Tribunais no sentido de responsabilização dos provedores por conteúdo ofensivo ou criminoso gerado por perfis falsos.

O primeiro caso já se encontra em sede de Recurso Extraordinário[66]. Seu início se deu em Primeira instância, no Juizado Especial Cível de São Paulo, quando o requerido, que tomou conhecimento de um perfil existente no Facebook com seus dados e fotos, após diversas denúncias feitas por diversas pessoas no próprio site, bem como feito Boletim de Ocorrência, verificou que o site continuava inerte sem tirar o usuário do ar. Desta forma, decidiu ingressar com ação de obrigação de fazer e de pagar.

Foi concedida a antecipação de tutela no sentido de obrigar o Facebook a tirar o perfil falso do ar. O que o fez assim que pôde para localizar o endereço do perfil na rede.

Ocorre que a discussão continuou quanto ao pedido de reparação civil. O Facebook alegou que agiu nos moldes do artigo 19 do Marco Civil da Internet quando procedeu com a exclusão do perfil e, por isso, não poderia ser responsabilizado. Assim, teve êxito em primeira instância.

[66] STF. Recurso Extraordinário: 1.037.396. Relator: Ministro Dias Toffoli. Data de Julgamento: 10/03/2020. *JusBrasil,* 2020. Disponível em: < https://www.jusbrasil.com.br/processos/151812037/processo-n-1037396-do-stf> Acesso em: 10.05.2021

O autor recorreu e a Turma Recursal entendeu que a não responsabilização do provedor feriria garantias constitucionais de defesa ao consumidor. Desta forma, o autor teve êxito após ter recorrido.

O Facebook, ora recorrente, interpôs Recurso Extraordinário, por intermédio de alegação de violação dos arts. 5º, IV, IX e XIV, e 220, §§ 1º e 2º da CF/1988. Isso porque a análise sistemática do mencionado art. 19 evidenciaria uma escolha do legislador, vinculada a privilegiar princípios como a liberdade de expressão, a vedação da censura e a reserva de jurisdição.

Ainda, a Procuradoria Geral da República expressou parecer favorável ao Recurso Extraordinário e o processo ainda aguarda julgamento do Supremo Tribunal Federal.

Em outro caso[67], podemos visualizar um fato semelhante. O autor tomou conhecimento de um perfil existente no Facebook com seus dados e fotos, após diversas denúncias feitas por diversas pessoas no próprio site, verificou que o site continuava inerte sem tirar o usuário do ar. Desta forma, decidiu ingressar com ação para que o perfil fosse excluído, bem como para recebimento de indenização por danos morais, uma vez que o perfil falso compartilhava difamações e injúrias à vítima.

O processo foi julgado a favor da vítima, em que o juiz reconheceu que não seria possível dissociar o provedor da internet do prestador de serviço descrito no artigo 3º do Código de Defesa do Consumidor.

Assim, foi decidido, nos termos do artigo 14 do mesmo Código, que o provedor, como prestador de serviço, possui responsabilidade objetiva e deve pagar indenização ao autor.

[67] TJ-MG. Apelação Cível: 10000180966970001. Relator: Desembargador Marcos Lincoln. Data de Julgamento: 09/10/2018. *JusBrasil,* 2018. Disponível em: < https://tj-mg.jusbrasil.com.br/jurisprudencia/916414050/apelacao-civel-ac-10000180966970001-mg/inteiro-teor-916414096> Acesso em: 10.05.2021

4. PERFIS FALSOS E A CONSTITUIÇÃO FEDERAL DE 1988

Ainda que o tema central do presente trabalho se dê nos ramos do Direito Penal e Civil, é importante averiguar que a má utilização das redes sociais por perfis falsos pode gerar danos em outras esferas do Direito, como o Direito Constitucional e o Direito Digital.

No ramo do Direito Constitucional, a criação e utilização de perfis falsos para divulgação de conteúdo gera um embate quanto à liberdade de expressão e à proibição ao anonimato, previstos no art. 5º da Constituição Federal, inciso IV.

Nesse sentido, Eliane Fontana pode nos ensinar, in verbis:

> Não obstante a isso, de forma mais ampla, no art. 5º, LVI, da Constituição Federal consta positivada como direito fundamental a liberdade de manifestação do pensamento e, logo em seguida, a normativa expõe uma restrição ao exercício ilimitado de tal direito fundamental, proibindo o anonimato, de modo que fique garantido o exercício do direito de resposta proporcional ao agravo e eventual responsabilização civil e criminal do autor da manifestação, garantindo a existência livre, digna e igual dos indivíduos.[68]

Para essa autora, a internet dificulta a aplicação da vedação ao anonimato pela facilidade com que se é possível criar um perfil falso nas redes sociais. Porém, as garantias constitucionais devem ser aplicadas também na internet, aplicando a lei por analogia, o que acaba por, nem sempre, haver uma interpretação justa para o caso concreto.

[68] FONTANA, Eliane; COSER, Thomas Felipe. *Perfil Falso Na Rede e o Anonimato*: Uma Visão (Polêmica) À Luz Do Marco Civil Da Internet. In: SEMINÁRIO INTERNACIONAL: DEMANDAS SOCIAIS E POLÍTICAS NA SOCIEDADE CONTEMPORÂNEA, VIII Mostra de trabalhos jurídicos científicos, 2015. Rio Grande do Sul: Universidade de Santa Cruz do Sul, 2015. p. 4. Disponível em: < https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13174/2387> Acesso em: 18.10.2020.

Uma ótica apresentada por essa mesma autora nos parece muito razoável quando ela escreve quanto à necessidade de se averiguar a finalidade do usuário para qual o usuário *fake* é utilizado, vejamos:

> A proteção à liberdade de expressão mencionada pelo referido diploma legal, que consiste até mesmo em um princípio estabelecido pelo artigo 2º do MCI, não abrange a vedação à exclusão de perfis baseados em informações falsas, de modo que administrador de um website poderá gerir a sua rede excluindo perfis com fins escusos sem necessitar de autorização judicial. Entretanto, cabe questionar o que vem a constituir um perfil falso sob a ótica da vedação constitucional ao anonimato e, de outro lado, o exercício da liberdade de expressão amplamente protegida pelo Marco Civil da Internet, haja vista que nem todo perfil baseado em informações inverídicas é destinado a fins escusos.
>
> Contudo, embora haja sua expressa vedação ao anonimato na Constituição Federal, precisamente no artigo 5º, inciso IV, deve ser observada a finalidade e as circunstâncias de seu uso, no qual o indivíduo usa um perfil lastreado em informações que não correspondem à sua verdadeira identificação[...][69]

Ainda, quanto à liberdade de expressão, porém relacionada aos direitos de terceiro, como o direito à privacidade e à intimidade, bem como os direitos autorais, Patrícia Peck[70] nos ensina que a liberdade de expressão deve ter limites baseados em ética e nas leis vigentes. Porém, uma censura prévia prejudicaria o direito à liberdade de expressão. Assim, a melhor forma de haver uma conscientização quanto a isso é que essas questões estejam claramente expostas nos termos de uso para ciência do usuário.

Em um artigo publicado na Revista da Faculdade de Direito de São Paulo, podemos observar outro ponto de vista quanto a preocupação com o anonimato na internet: os riscos de estabelecer-se normas que prejudiquem atividades importante no meio virtual. Vejamos, *in verbis*:

> [...] o anonimato é vedado pela CF88, em seu artigo 5°, IV. A vedação constitucional busca assim, atribuir responsabilidade àqueles que exercem a liberdade de pensamento evitando os abusos que podem decorrer da impunidade facilitada pela ocultação. Os excessos devem ser sempre evitados: a demasiada preocupação com a privacidade, expressa na forma

[69] Ibid, p. 14
[70] PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2016. p. 449-450

> de normas rígidas, pode fazer com que outros valores sejam perdidos. A regulação apressada e sem reflexão pode causar o término de uma série de atividades empreendedoras legítimas e inovadoras. e também prejudicar o livre fluxo de informações necessário para a promoção de objetivos individuais, comunitários e sociais.[71]

Assim, a criação de perfis falsos pode interferir no âmbito constitucional, pois, ao realizarem postagens expondo qualquer opinião, em que pese o direito à liberdade de expressão, quando o fazem de forma anônima, incorrem numa prática vedada pela Constituição.

[71] REVISTA DA FACULDADE DE DIREITO DE SÃO PAUO: Regulação tecnológica e jurídica das redes sociais (*social networks).* São Paulo: Universidade de São Paulo, v. 100, jan/dez 2005. p. 635-636

5. INVESTIGAÇÃO DIGITAL PARA IDENTIFICAÇÃO DE UM PERFIL FALSO NAS REDES SOCIAIS CONTEMPORÂNEAS NA INTERNET

O presente tópico se aterá a explicar, de forma sucinta e abreviada, alguns termos importantes para entendermos como se dá uma investigação digital. Trata-se de um tema complexo e extenso, digno de um estudo aprofundado e individual.

Primeiramente, precisamos entender como funciona e o que é um IP. Temos que diferenciar que há dois tipos de IPs.

Para haver uma conexão com a Internet, é necessário um dispositivo que conecte o computador à rede, esse dispositivo pode ser um modem ou um roteador.

Pode ser que tenhamos diversos computadores ligados a um só dispositivo (modem e/ou roteador). Assim, conforme Victor Martins[72], temos os IPs públicos e os privados.

Os computadores possuem um número de IP próprio, mas que ficam privados. Já os IPs públicos estão presentes nesses dispositivos responsáveis por conectar o computador à internet e são rotativos, na medida em que são distribuídos e redistribuídos pelas empresas de comunicação responsáveis e também chamamos de IP da aplicação.

Esses IPs públicos são distribuídos pelos administradores de sistema autônomos.

Ainda, é importante entendermos a diferença entre ao que o Legislador se refere à “administrador de sistema autônomo” e “provedor de aplicações de internet” quando editou o Marco Civil da Internet.

O professor Marcel Leonardi[73] explica que o provedor de aplicações de internet é gênero do qual as demais categorias são espécies. Trata-se daquele que

[72] MARTINS, Victor. Investigação digital: procedimentos para rastreamento de IP, *SajAdv*, Minas Gerais, 03 dez. 2018. Disponível em: <https://blog.sajadv.com.br/investigacao-digital-ip/> Acesso em: 10.05.2021

[73] LEONARDI, Marcel. *Internet:* elementos fundamentais. in Responsabilidade Civil na Internet e nos demais meios de comunicação, coordenado por Regina Beatriz Tavares da Silva e Manoel J. Pereira dos Santos. 2. ed. São Paulo: Saraiva, 2012.

fornece serviços relacionados ao funcionamento da Internet. Já o administrador de sistema autônomo, diz respeito ao provedor de conexão ou de acesso, que tem a finalidade de conectar o usuário por meio do roteamento de IPs. No Brasil, podemos citar algumas empresas consideras como provedores de conexão para ficar mais claro: TIM; CLARO; VIVO etc.

Sabemos que cada uma das redes sociais citadas no tópico 1 possuem servidores que armazenam os dados, estes são os chamados provedores de aplicação.

Para entender como é possível que haja um rastreamento de um IP, precisaremos, primeiramente, entender também o conceito de *log*.

Vejamos o conceito de Ricardo Clemente:

> Os logs são fontes riquíssimas de informação e são gerados pelos servidores e pelas aplicações conforme eventos significativos acontecem. Um log é definido como um conjunto de registros com marcação temporal, que suporta apenas inserção, e que representa eventos que aconteceram em um computador ou equipamento de rede. Estes registros constituem a fonte básica de informação tanto para a detecção e resolução de problemas quanto para informações de negócio, como métricas de acesso e comportamento de usuários. [74]

Ou seja, *log* de dados são os registros desses IPs. Segundo Victor Martins[75], é um arquivo de texto gerado por um software para descrever eventos sobre o seu funcionamento, utilização por usuários ou interação com outros sistemas.

Segundo nos explica o Perito Victor Martins[76], o primeiro passo de uma investigação digital, consiste em obter o endereço de IP da aplicação e do computador do usuário.

---

[74] CLEMENTE, Ricardo Gomes. *Uma Arquitetura Para Processamento De Eventos De Log Em Tempo Real.* 10 dez. 2008. Tese (Banco de dados) Puc-Rio - Pontifícia Universidade Católica do Rio De Janeiro, Rio de Janeiro, 2008. P. 15. Disponível em: < https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=especifico&nrSeq=12571@1>. Acesso em 10.05.2021.

[75] MARTINS, Victor. Investigação digital: procedimentos para rastreamento de IP, *SajAdv*, Minas Gerais, 03 dez. 2018. Disponível em: <https://blog.sajadv.com.br/investigacao-digital-ip/> Acesso em: 10.05.2021.

[76] Ibid.

Para isso, é preciso do acesso aos *logs* armazenados pelo provedor de aplicação ou os de conexão.

Essas informações podem ser consultadas de forma idônea por um perito de informática, mas tomando todos os cuidados específicos para não acarretar na ilicitude da prova.

Ocorre que, essa guarda de registro pelo servidor pode envolver algumas questões de proteção de dados pessoais.

Denota-se essa preocupação na redação do Marco Civil da Internet (MCI) em seus artigos 13 e 15. No artigo 13 está prevista a responsabilidade de guarda desses *logs* pelos provedores de conexão, porém, estabelece prazo de um ano.

Esse prazo é ainda mais curto quando se trata dos provedores de aplicação, sendo de seis meses, segundo o artigo 15.

Segundo explicam os procuradores do Ministério Público, Felipe e Marcelo, essas previsões podem acarretar dificuldades para os andamentos da investigação. Vejamos, *in verbis:*

> O MCI de fato apresentou alguns avanços, diversos dos quais ainda pendem de devida regulamentação. Contudo, foi duramente criticado por peritos em informática e advogados especialistas em direito digital, em diversos aspectos tais como a guarda de registros (logs) de acesso e privacidade de usuários e liberdade de expressão.
>
> Os logs oferecem informações essenciais para iniciar adequadamente uma investigação, a qual fica bastante comprometida sem o fornecimento devido de dados que possibilitem a identificação de qual usuário estava vinculado a um endereço IP identificado como origem de um suposto crime.
>
> Para piorar ainda mais esse exíguo prazo de armazenamento definido, o Decreto nº 8.771, de 11 de maio de 2016, que regulamentou a Lei nº 12.965/2014, definiu em seu art. 11 que "o provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados". Isso é praticamente um convite aos criminosos para utilizarem redes WiFi abertas para o cometimento de delitos.[77]

[77] CAIADO, Felipe; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: Ministério Público Federal. Crimes Cibernéticos. Brasília: 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018.

Ainda nas explicações dos procuradores, outra Lei pode ser um obstáculo na investigação, pois para obter esses dados de IP, data e hora, quanto para a obtenção de conteúdo de comunicação armazenadas nos servidores das empresas, é necessária a quebra de sigilo telemático e a autorização judicial, para que os provedores de aplicações de internet os forneçam.

Para a obtenção desse conteúdo, é necessária ordem judicial que autorize a interceptação telemática, observando-se os rigores da Lei nº 9.296/1996.

Eles, ainda, complementam:

> É importante notar que os registros de conexão à internet, bem como os registros de acesso a aplicações de internet podem ser obtidos mediante ordem judicial para formação de conjunto probatório em processo judicial cível ou penal, nos termos do art. 22 do MCI. Já as comunicações telemáticas somente podem ser obtidas para formação de conjunto probatório em investigação criminal ou instrução processual penal, a exemplo das comunicações telefônicas, nos termos do parágrafo único do art. 1º da Lei nº 9.296, de 24 de julho de 1996, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal.[78]

Superados esses passos, é elaborado um laudo pericial para que seja possível avaliar quanto à autoria do ato ilícito.

P. 12 Disponível em: < https://memorial.mpf.mp.br/ce/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos> Acesso em: 07.05.2021

[78] DOMINGOS, Fernanda Teixeira Souza (coordenação). *Crimes Cibernéticos:* coletânea de artigos. Brasília: MPF, 2018. p.42-43

6. FUTURO DA RESPONSABILIZAÇÃO PENAL QUANTO À CRIAÇÃO DE PERFIS FALSOS NAS REDES SOCIAIS

Não há na legislação referência expressa a perfis falsos, nem mesmo na Lei do Marco Civil da Internet.

Assim, analisaremos se há necessidade de alterar a legislação para incluir esse tipo de conduta na legislação penal para torná-lo um fato típico.

Para o Professor Damásio, sem legislação há insegurança jurídica quando o assunto é tecnologia. Pois, para ele, a chamada "sociedade da informação" pode ser também chamada de "sociedade dos riscos". Segundo ele, esses riscos podem ser aceitos ou mitigados.

Nesse sentido, ele nos ensina:

> É cediço que, pelo princípio da legalidade, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Ninguém pode ser responsabilizado por fato que a lei desconsidera como de relevância penal.[79]

Assim, se seguíssemos nesse raciocínio, para haver o enquadramento de perfis falsos como falsidade ideológica ou falsa identidade, deveria haver previsão legal expressa nesse sentido.

Porém, conforme dito pelo ex Ministro Sepúlveda Pertence, do Supremo Tribunal Federal, nem todos os delitos cibernéticos necessitam de nova tipificação, eis que em muitos casos a tecnologia é só um novo meio utilizado para concretização de delitos conhecidos.[80]

---

[79] JESUS, Damasio Evangelista de; OLIVEIRA, Jose Antonio M Milagre de. *Manual de crimes informáticos*. 1ª ed. São Paulo: Saraiva. 2015. p. 19

[80] TRF-1. Habeas Corpus: 76.689/PB. Relator: Desembargador Hilton Queiroz, Data de julgamento: 28 nov. 2011, *JusBrasil*, 2011. Disponível em: < https://trf-1.jusbrasil.com.br/jurisprudencia/2315156/habeas-corpus-hc-29296-go-20010100029296-8> Acesso em: 10.05.2021.

Neste Diapasão, o Professor Damásio explica que se trata de uma nova técnica no meio virtual para o cometimento de mesmos crimes. Vejamos, *in verbis:*

> Temos o primeiro princípio: não se legisla sobre técnica! Qualquer tentativa de legislar sobre técnicas e métodos de um ataque resulta em uma legislação por demais específica e pouco eficaz, com rápida obsolescência. Muito menos se legisla sobre vulnerabilidade.
>
> Logo, identifica-se primeiramente um comportamento que possa ser concretizado por uma ou mais técnicas informáticas, que existam ou que venham a ser criadas. comportamento este que mereça a tutela penal e, neste sentido, se eleva tal comportamento ao status de "crime", se realmente corresponder a uma atividade reprovável.
>
> Até mesmo ao se definirem os elementos que fazem parte de um comportamento, deve-se ter cautela em não especificá-los ao extremo a ponto de não poder abranger condutas que "ao lado" sejam ofensivas ao bem jurídico e que não poderão ser enquadradas. [81]

Porém, para ele, isso não significa que pouco importa a técnica. Então, ele continua:

> Conhecer a técnica é fundamental para o operador do Direito. Não se pode exercer com dignidade a advocacia em direito digital sem conhecer a fundo as técnicas.
>
> [...]
>
> Muitas condutas protegidas pela tutela penal não abrangem determinadas técnicas. Diga-se, muitas técnicas isoladamente praticadas não representam condutas incriminadoras.
>
> [...]
>
> é mister que não se considere a máxima "o que vale é conduta, pouco importando a técnica.[82]

Assim, é preciso refletir se a criação de Perfis falsos em redes sociais é uma técnica ou um comportamento. Para que, só então, possamos estabelecer regras quanto a isso e não cometamos o erro de se tornar uma norma absoleta em pouco tempo, visto que a internet é rapidamente modificada e, consequentemente a forma que são praticados crimes também.

---

[81] JESUS, Damasio Evangelista de; OLIVEIRA, Jose Antonio M Milagre de. *Manual de crimes informáticos*. 1ª ed. São Paulo: Saraiva. 2015. p. 42

[82] Ibid. p 42

6.1 A EDUCAÇÃO NO MEIO ELETRÔNICO

Muito se fala em criminalização de condutas inadequadas na Internet. Porém, sabe-se que a principal ferramenta para tornar a convivência agradável e confortável entres os seres humanos em meio social é a educação.

Assim, no meio digital não seria diferente. É necessário que passemos a educar os usuários de redes sociais no mundo cibernético da mesma forma que educamos as pessoas para viverem em sociedade.

Essa educação baseia-se na conscientização dos direitos e deveres de cada um, bem como a análise crítica do que se vê, para que assim diminuamos o número de golpes, fraudes e disseminação de inverdades no meio virtual.

Nesse sentido, Patrícia Peck explora a ideia da conscientização dos usuários:

> Não podemos esquecer, entretanto, que na Internet as leis também são aplicadas. Por isso, é fundamental que quem participa dela, seja por meio de um blog muito visitado ou apenas por meio das redes sociais, conheça seus direitos e deveres, de forma a produzir com comprometimento.[83]

Segundo o Professor Damásio, temos que a grande motivação dos crimes praticados no mundo virtual se deve ao despreparo do Brasil, vejamos *in verbis:*

> A realidade, hoje, é que grande parte dos crimes digitais se deve à ignorância dos usuários, despreparo das autoridades investigativas e, principalmente, à banalização e difusão das técnicas e ferramentas para aplicação de golpes. Pode-se dizer também que os criminosos digitais, em sua maioria, não praticariam crimes do mundo real, porém interessam-se pela prática delituosa virtual, amparados pela falsa sensação de anonimato e conhecedores do despreparo das autoridades em investigarem delitos desta natureza.[84]

[83] PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2016. p. 449
[84] JESUS, Damasio Evangelista de; OLIVEIRA, Jose Antonio M Milagre de. *Manual de crimes informáticos*. 1ª ed. São Paulo: Saraiva. 2015. p. 8

Podemos finalizar esse tópico concluindo, através das palavras de Adriano Augusto Fidalgo[85], que Educação Digital significa haver a transmissão de valores éticos e de cidadania para o ambiente virtual, respeitando- se a dignidade da pessoa humana e o bem comum.

Nesse sentido, ele comenta sobre o projeto organizado pelo Ministério Público para implementar essa conscientização nas escolas, vejamos:

> Por entender que só a repressão é insuficiente e que a prevenção é o melhor caminho a seguir na conscientização das pessoas, em especial das crianças e dos adolescentes, principais vítimas desses delitos, as Procuradorias da República nos Estados de São Paulo e Rio de Janeiro, por incentivo de seus aludidos grupos especializados de combate a crimes cibernéticos, firmaram convênios com a Organização Não Governamental SaferNet Brasil7 8, para atuação conjunta na área de prevenção a tais crimes. Assim, o Ministério Público Federal começou a promover, em parceria com a referida ONG, desde 2009, na sede da Procuradoria da República em São Paulo e, a partir de 2010, também na sede da Procuradoria da República no Estado do Rio de Janeiro, as Oficinas denominadas "Promovendo o uso responsável e seguro na internet", destinadas aos professores das redes pública e privada de ensino nos respectivos estados. Essa iniciativa ocorreu, à época, também nas Procuradorias da República em João Pessoa, na Paraíba; em Manaus, no Amazonas; em Belém, no Pará e em Fortaleza, no Ceará.[86]

Dessa forma, a conscientização é muito importante no sentido de tomadas de decisões no âmbito das redes sociais, visto é possível restringir informações pessoais para visualização de usuários selecionados nas redes sociais, bem como há diversas outras ações para prevenção de acabar sendo vítima de um crime virtual.

[85] FIDALGO, Adriano Augusto (Ed.). *Cibernética Jurídica:* Estudos sobre Direito Digital. Paraíba: eduepb, 2020. P.25

[86] OLIVEIRA, Neide M.C. Cardoso de; MORGADO, Marcia. Projeto "Ministério Público Pela Educação Digital Nas Escolas". In: Ministério Público Federal. Crimes Cibernéticos. Brasília: 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018. Disponível em: < https://memorial.mpf.mp.br/ce/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos> p.253

6.2 PROJETO DE LEI Nº 7.758 DE 2014.

Há o Projeto de Lei nº 7.758/14 tramitando no Congresso que tem como objetivo acrescentar ao Código Penal, no artigo 307, que trata do crime de falsidade ideológica, a modalidade eletrônica pelo uso de perfis falsos.

O Projeto propõe que a punição seja de detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Foi encaminhado à Comissão de Constituição e Justiça, cujo relator emitiu parecer no sentido de que a Lei necessita de “reparos”, uma vez que vai de encontro com Lei Complementar nº 95, de 1998, com as alterações introduzidas pela Lei Complementar nº 107, de 2001.

Isto é, apresenta erros formais em sua elaboração. Vejamos:

> A ementa não faz referência ao cerne do projeto, apenas à alteração na legislação penal – “acrescenta dispositivo ao art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal”. O artigo inaugural tem o defeito oposto, indica o objetivo do projeto – “tipifica penalmente o uso de falsa identidade na rede mundial de computadores” – sem mencionar que para tanto altera a legislação em vigor.
>
> O caput do art. 2º do PL 7758/14 indica que “o art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte parágrafo único”, porém o texto legal indicado é de substituição do caput do art. 307 do Código Penal. Verifica-se ainda a ausência das iniciais maiúsculas NR entre parênteses para sinalizar a modificação de dispositivos legais vigentes; bem como da cláusula de vigência.
>
> A hipótese parece ser de inclusão de um art. 307-A no Código Penal, de modo a que se preserve o tipo penal de falsidade ideológica, previsto no art. 307, e que se tipifique, não por parágrafo único, mas por novo dispositivo (art. 307-A), a conduta criminosa prevista.

Diversos apontamentos são realizados de forma elogiosa ao mérito do Projeto, que podem ser visualizados na íntegra no Anexo I.

Ainda, no site da Câmara há uma enquete no sentido de consultar a população quanto tornar a criação de perfil falso crime.[87]

O referido projeto já foi aprovado na Comissão de Constituição e Justiça e de Cidadania (CCJC) em 04/08/2015.

Desde então o projeto não teve mais andamento.

6.3 CRIMINALIZAÇÃO DE PERFIS FALSOS NO DIREITO COMPARADO

O Direito comparado é sempre uma perspectiva importante a ser observada quando o assunto é a criação de novas regras. Em que pese também ser importante observar as diferenças pertinentes a cada país, pois nem sempre as mesmas regras são viáveis para países diferentes, por questões culturais, sociais, econômicas etc.

Quanto à criminalização de perfis falsos, podemos visualizar uma Lei nos Estados Unidos, no Estado da California, que entrou em vigor em 2011.

A lei tem previsão de multa de mil dólares para os usuários que se fizerem passar por outra pessoa.

Para a penalização, é preciso que haja a intenção de prejudicar, intimidar, ameaçar ou fraudar uma pessoa.

O texto da lei, no entanto, não cita questões de liberdade de expressão, como perfis que fazem paródias e sátiras a personalidade.

Podemos visualizar o tópico 528.5., que foi inserido por essa atualização de 2011, conforme:

[87] Disponível em: <https://www.camara.leg.br/noticias/451303-camara-lanca-enquete-sobre-uso-de-perfil-falso-na-internet/> Acesso em: 10.05.2021.

> a) Não obstante qualquer outra disposição da lei, qualquer pessoa que, conscientemente e sem consentimento, se passar por outra pessoa real por meio ou em um site da Internet ou por outros meios eletrônicos para fins de ferir, intimidar, ameaçar ou fraudar outra pessoa é culpada de uma ofensa pública punível de acordo com a subdivisão (d).
> (b) Para os fins desta seção, uma falsificação de identidade é confiável se outra pessoa razoavelmente acreditar, ou acreditou razoavelmente, que o réu foi ou é a pessoa que foi falsificada.
> (c) Para os fins desta seção, "meios eletrônicos" incluirão a abertura de uma conta de e-mail ou uma conta ou perfil em um site de rede social na Internet em nome de outra pessoa.
> (d) Uma violação da subdivisão (a) é punível com uma multa não superior a mil dólares ($ 1.000), ou por prisão em uma prisão do condado não superior a um ano, ou por essa multa e prisão.
> (e) Além de qualquer outro recurso civil disponível, uma pessoa que sofre danos ou perdas em razão de uma violação da subdivisão (a) pode mover uma ação civil contra o infrator por danos compensatórios e medidas cautelares ou outras medidas equitativas nos termos dos parágrafos (1), (2), (4) e (5) da subdivisão (e) e subdivisão (g) da Seção 502.
> (f) Esta seção não deve impedir o processo sob qualquer outra lei.) (tradução minha) [88]

Segundo o Senador que propôs essa demanda, trata-se de uma atualização da lei de falsa representação que foi promulgada em 1872. [89]

[88] PENAL CODE -PEN. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=13.&part=1.&chapter=8.&article=> Acesso em: 10.05.2021

[89] AGUIARI, Vinicius. Lei contra perfil falso entra em vigor nos EUA. *Exame.* 02 jan. 2011. Disponível em: <https://exame.com/tecnologia/lei-contra-perfil-falso-entra-em-vigor-nos-eua/> Acesso em: 10.05.2021

CONCLUSÃO

Diante de todo o estudo apresentado, a primeira conclusão a que chegamos é de que não é possível mais dissociar a vida no mundo físico da vida no mundo virtual. As relações sociais entre as pessoas são impactadas diretamente pelo o que acontece no meio digital.

A grande diferença é que no meio virtual, é possível o anonimato. Essa caraterística influencia em como as pessoas se comportam, vez que ao beneficiarem a si mesmas, em detrimento de alguém, o constrangimento moral da sociedade não acontecerá, fazendo com que muitas delas cometam atos ilícitos ou imorais.

Assim, os perfis falsos são ferramentas de anonimato de usuários que praticam diversos crimes no meio virtual, como estelionato, extorsão, assédio, discursos de ódio etc.

Porém, é importante salientar que nem todo perfil falso é criado com a intenção de cometimento de crime. Muitas pessoas criam perfis falsos para divulgarem ideias, piadas e assuntos que não ofendem outras pessoas.

Tendo havido cometimento de crime e dano a alguém, deve-se haver também investigação e a punição do infrator. Porém, uma censura prévia criminalizando a criação de perfis falsos pode implicar em uma supressão à liberdade no meio digital.

Portanto, a punição deve ser proporcional ao dano causado. Seja no âmbito civil ou penal.

No âmbito civil, como vimos, é completamente cabível o pedido de indenização por danos morais e/ou materiais, bem como, o responsável pelo dano é quem deve arcar com esse custo. Porém, pela dificuldade de localização do usuário infrator, o provedor é quem deve ser responsabilizado, em que pese a discussão doutrinária, pois é o único capaz de criar ferramentas de inibição de tais práticas, bem como de localizar um perfil em uma rede social.

Haja vista que o provedor é um prestador de serviço, deve prezar sempre pelo bom funcionamento da ferramenta que oferta, nos termos no Código de Defesa do

Consumidor. Não seria justo deixar que o consumidor arque com prejuízos que não deu causa, quando sua única intenção era de utilizar um serviço ofertado no mercado.

Já no âmbito penal, vislumbra-se que não há Lei no sentido de criminalização de perfis falsos em redes sociais. Em que pese haver projeto de lei, bem como lei internacional nesse sentido.

Conforme já dito, uma criminalização da criação de perfil falso em rede social, sem prever uma finalidade, pode ser prejudicial para a própria rede, tendo em vista a censura prévia.

Porém, o usuário que se utiliza desse meio para uma finalidade obscura pode e deve ser penalizado. Sugerimos que haja tipificação desse tipo de conduta, nos crimes de falsa identidade (quando o perfil copia dados de alguém e obtém vantagem se passando por outra pessoa) ou falsidade ideológica (quando insere dados mentirosos em seu perfil, mas não necessariamente os copia de alguém) em concurso de crime cometido através desse perfil, já que, pela falta de uma norma que enquadre expressamente essa conduta ao tipo penal, os tribunais têm entendido pelo conflito aparente de normas e, consequentemente, aplicado o princípio da concussão.

Diante de todo exposto, é importante ressaltar que qualquer medida penal deve ser tomada em *ultima ratio*, sendo a educação o melhor meio para se alcançar a diminuição do cometimento de crimes.

É importante que haja uma cooperação a nível nacional e internacional de conscientização sobre a utilização dos meios eletrônicos, a começar do ensino básico até a população mais velha. Pois a internet é um meio democrático de uso e que proporciona uma ideia de liberdade muito ampla. Mas, assim como no meio físico, não se pode ter liberdade absoluta no mesmo ambiente em que há sociedade e civilização.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIARI, Vinicius. Lei contra perfil falso entra em vigor nos EUA. *Exame*. 02 jan. 2011. Disponível em: <https://exame.com/tecnologia/lei-contra-perfil-falso-entra-em-vigor-nos-eua/> Acesso em: 10.05.2021.

AMIKY, Luciana Gerbovic. *Stalking*. 2014. Dissertação (Mestrado em Direito) – Pontífica Universidade Católica de São Paulo, São Paulo, 2014.

ANDREUCCI, Ricardo Antonio. *Manual de direito penal*: de acordo com a Lei n. 13.869, de 2019, Lei de Abuso de Autoridade. 14. São Paulo Saraiva 2019 1 recurso online ISBN 9788553616329.

ARROYO, Danilo Wohnrath. *A criação de perfil falso nas redes sociais Facebook e Twitter*: motivações e tipos. Araranguá. 2019. Disponível em: <https://repositorio.ufsc.br/handle/123456789/203028> Acesso em 01.12.2020.

BAPTISTA, Hugo Filipe Fontainhas. *Identificação de perfis falsos nas redes sociais.* 2019. Projeto (Mestrado em Cibersegurança e Informática Forense) – Instituto Politécnico de Leiria, Leiria, 2019. Disponível em: < https://iconline.ipleiria.pt/bitstream/10400.8/4550/1/Identificacao_de_perfis_falsos_nas_redes_sociais_2170086.pdf> Acesso em: 07.05.2021.

BRASIL. DECRETO-LEI Nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 07 dez. 1940. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em 14.03.2021.

BRASIL. LEI Nº 8.0878, de 11 de setembro de 1990. Código de Defesa do Consumidor. Diário Oficial da União, Brasília, DF, 11 set. 1990. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 10.05.2021

BRASIL. LEI Nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 23 abr. 2014. Disponível em <

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 10.05.2021.

CAIADO, Felipe; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: Ministério Público Federal. *Crimes Cibernéticos.* Brasília: 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018. Disponível em: < https://memorial.mpf.mp.br/ce/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos> Acesso em: 07.05.2021.

CAMELO, Fábio Assunção Berlim. *Detecção Automática de Discursos de Ódio em Comentários de Jornais Online*. Dissertação (Bacharelado em Ciências da Computação) – Universidade Federal Fluminense, Rio de Janeiro, 2017. Disponível em: < https://app.uff.br/riuff/bitstream/1/5753/1/tcc-fabio-assuncao-berlim-camelo.pdf> Acesso em: 07/05/2021.

CASTRO, Paulo Alexandre de. *Rede complexa e criticalidade auto-organizada: modelos e aplicações.* 2007. Tese (Doutorado em Física Básica) – Universidade de São Paulo, São Paulo, 2007. Disponível em: <https://www.teses.usp.br/teses/disponiveis/76/76131/tde-14012008-165356/pt-br.php> Acesso em: 05.04.2021.

CLEMENTE, Ricardo Gomes. *Uma Arquitetura Para Processamento De Eventos De Log Em Tempo Real*. 10 dez. 2008. Tese (Banco de dados) Puc-Rio - Pontifícia Universidade Católica do Rio De Janeiro, Rio de Janeiro, 2008. P. 15. Disponível em: < https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=especifico&nrSeq=12571@1>. Acesso em 10.05.2021.

CONFESSORE, Nicholas; DANCE, Gabriel; HARRIS, Richard. The Follower Factory. *The New York Times.* New York, 7 jan. 2018. Disponível em: < https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html> Acesso em: 07.05.2021.

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

Disponível em: <https://www.camara.leg.br/noticias/451303-camara-lanca-enquete-sobre-uso-de-perfil-falso-na-internet/> Acesso em: 10.05.2021.

DUARTE, Marcella. O que é stalking? Prática comum na web agora é crime que prevê prisão. *Tilt*, São Paulo, 01 abr. 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/04/01/curte-stalkear-pratica-agora-e-crime-e-pode-dar-tres-anos-de-prisao.htm>. Acesso em: 09.04.2021.

DOMINGOS, Fernanda Teixeira Souza (coordenação). *Crimes Cibernéticos*: coletânea de artigos. Brasília: MPF, 2018.

FACEBOOK. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/facebook/> Acesso em: 07.04.2021.

FERREIRA, Gonçalo Costa. *Redes Sociais de Informação*: uma história e um estudo de caso. 2011. Dissertação (Mestrado em Ciência da Informação) - Escola da Comunicações e Artes da Universidade de São Paulo, São Paulo, 2011. Disponível em: <https://www.scielo.br/pdf/pci/v16n3/13.pdf> Acesso em: 05.04.2021.

FIDALGO, Adriano Augusto (Ed.). Cibernética Jurídica: Estudos sobre Direito Digital. Paraíba: eduepb, 2020.

FONTANA, Eliane; COSER, Thomas Felipe. Perfil Falso Na Rede E O Anonimato: Uma Visão (Polêmica) À Luz Do Marco Civil Da Internet. In: SEMINÁRIO INTERNACIONAL: DEMANDAS SOCIAIS E POLÍTICAS NA SOCIEDADE CONTEMPORÂNEA, VIII Mostra de trabalhos jurídicos científicos, 2015. Rio Grande do Sul: Universidade de Santa Cruz do Sul, 2015. Disponível em: < https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13174/2387> Acesso em: 18.10.2020.

GOGONI, Ronaldo. Qual foi a primeira rede social criada na internet?. *Tecnoblog*. São Paulo, 2020. Disponível em: <https://tecnoblog.net/author/ronaldogogoni/> Acesso em: 06.04.2021.

GONÇALVES, Victor Hugo Pereira. *Marco civil da internet comentado*. 1ª ed. São Paulo: Atlas, 2017.

GRIZOTTI, Giovani. Golpistas usam perfis falsos nas redes sociais para extorquir dinheiro de vítimas no RS. *G1*. Rio Grande do Sul, 23 set. 2019. Disponível em: <https://g1.globo.com/rs/rio-grande-do-sul/noticia/2019/09/23/golpista-usam-perfis-falsos-nas-redes-sociais-para-extorquir-dinheiro-de-vitimas-no-rs.ghtml> Acesso em: 07.05.2021.

HARARI, Yuval Noah. *Sapiens:* uma breve história da humanidade. Tradução de Janaína Marcoantonio. Porto Algre: L&M Editores, 2020.

INSTAGRAM. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/instagram/> Acesso em: 07.04.2021

JESUS, Damásio Evangelista de. *Direito penal 1:* parte geral. 37ª ed. São Paulo: Saraiva. 2020.

JESUS, Damasio Evangelista de; OLIVEIRA, Jose Antonio M Milagre de*. Manual de crimes informáticos***.** 1ª ed. São Paulo: Saraiva. 2015.

LEONARDI, Marcel. *Internet:* elementos fundamentais. in Responsabilidade Civil na Internet e nos demais meios de comunicação, coordenado por Regina Beatriz Tavares da Silva e Manoel J. Pereira dos Santos. 2. ed. São Paulo: Saraiva, 2012.

LÉVY, Pierre. *As tecnologias da inteligência*: o futuro do pensamento na era da informática. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1993.

LINKEDIN. *CanaTech.* Disponível em: <https://canaltech.com.br/empresa/linkedin/#:~:text=O%20LinkedIn%20foi%20lan%C3%A7ado%20por,..de%20usu%C3%A1rios%20em%20200%20pa%C3%ADses.> Acesso em: 07.04.2021.

MARTINS, Victor. Investigação digital: procedimentos para rastreamento de IP, *SajAdv*, Minas Gerais, 03 dez. 2018. Disponível em: <https://blog.sajadv.com.br/investigacao-digital-ip/> Acesso em: 10.05.2021.

MAZZOLA, Marcello Adriano. *I nuovi danni.* Padova: Dott. Antonio Milini, 2008.

MELOY, J. Reid. *The psychology of stalking.* San Diego: Elsevier Science, 1998.

MILITÃO, Eduardo; REBELLO, Aiuri. Rede de fake news com robôs pró-bolsonaro mantém 80% das contas ativas. *UOL*. Brasília, 19 set. 2019. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2019/09/19/fake-news-pro-bolsonaro-whatsapp-eleicoes-robos-disparo-em-massa.htm> Acesso em: 07.05.2021.

NORONHA, Edgard Magalhães. *Direito Penal.* 17 ed., vol. 4. São Paulo: Rideel, 1980.

NUCCI, Guilherme de Souza. *Manual do Direito Penal*. 7ª ed. São Paulo. Revista dos Tribunais, 2011.

OLIVEIRA, Neide M.C. Cardoso de; MORGADO, Marcia. Projeto “Ministério Público Pela Educação Digital Nas Escolas”. In: Ministério Público Federal. Crimes Cibernéticos. Brasília: 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018. Disponível em: < https://memorial.mpf.mp.br/ce/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos> Acesso em: 10.05.2021

OLIVEIRA, Neide M. C. Cardoso; GOÉS, Silvana Batini (ed.). *FAKE NEWS e COMO INVESTIGAR.* Rio de Janeiro: Ministério Público Federal, 2018. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/orientacoes/documentos/11-texto-sobre-fake-news-gacc.pdf> Acesso em: 09.04.2021.

OLIVO, CK. *Avaliação de características para detecção de phishing de email.* Dissertação(mestrado), Pontifícia Universidade Católica do Paraná, Curitiba, 2010. P. 1. Disponível em: < https://www.ppgia.pucpr.br/pt/arquivos/mestrado/dissertacoes/2010/cleber_kiel_olivo_-_final.pdf> Acesso em: 07.05.2021.

PAZ, Nathália. O que é falsidade ideológica? Identidade, *IdBlog*, São Paulo, 2020. Disponível em: <https://blog.idwall.co/o-que-e-falsidade-ideologica/#:~:text=A%20falsidade%20ideol%C3%B3gica%2C%20como%20falado,pessoa%20se%20passa%20por%20outra.> Acesso em 07.04.2021.

PENAL CODE -PEN. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=13.&part=1.&chapter=8.&article=> Acesso em: 10.05.2021.

PINHEIRO, Patrícia Peck*. Direito Digital*. São Paulo: Saraiva, 2016.

QUEM MATOU O ORKUT. Direção e Produção: *Canal Meteoro Brasil*. Curitiba. 2021. Disponível em: <https://www.youtube.com/watch?v=joat8DME_UI> Acesso em: 06.04.2021.

REVISTA DA FACULDADE DE DIREITO DE SÃO PAUO: Regulação tecnológica e jurídica das redes sociais (*social networks).* São Paulo: Universidade de São Paulo, v. 100, jan/dez 2005.

SANTOS, Chistiano Jorge; GARCIA, Cristina Victor. A Criminalização Da lgbtfobia Pelo Supremo Tribunal Federal do Brasil. *Revista Direito UFMS.* Mato Grosso do Sul, v. 5, n.2, 2019. Disponível: <https://periodicos.ufms.br/index.php/revdir/article/view/9845> Acesso em: 07.05.2021.

SILVA, Melissa Garcia Blagitz de Abreu e. *The Microsoft Ireland Case and Access to ata: An International Perspective*.Trabalho apresentado durante o curso de Mestrado em Direito na Universidade de Chicago nos Estados Unidos da América na matéria Computer Crime ministrada pelo Professor William Ridgway. 2016.

SILVA, Rosane Leal et al. Discurso de ódio em redes sociais*:* jurisprudência brasileira. *Revista Direito GV*, São Paulo, v. 14, 2011. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/23964/22729> Acesso em: 09.04.2021.

STF. Recurso Extraordinário: 1.037.396. Relator: Ministro Dias Toffoli. Data de Julgamento: 10/03/2020. JusBrasil, 2020. Disponível em: < https://www.jusbrasil.com.br/processos/151812037/processo-n-1037396-do-stf> Acesso em: 10.05.2021.

SUSPEITOS DO ROUBO DAS FOTOS DE CAROLINA DIECKMANN SÃO DESCOBERTOS. *G1*. Rio de Janeiro, 13 mai. 2012. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html> Acesso em: 07.05.2021.

TEIXEIRA, Eduardo Ariel de Souza. *Estudo Ergonômico da Interface De Produtos Web Focados Na Transmissão De Alta Velocidade*. 2004. Dissertação. Pontifícia Universidade Católica Do Rio De Janeiro, Rio de Janeiro, 2004. Disponível em: <https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=resultado&nrSeq=5090@1> Acesso em: 19.02.2021

TJ-MG - Apelação Cível: 10000180966970001. Relator: Desembargador Marcos Lincoln. Data de Julgamento: 09/10/2018. JusBrasil, 2018. Disponível em: < https://tj-mg.jusbrasil.com.br/jurisprudencia/916414050/apelacao-civel-ac-10000180966970001-mg/inteiro-teor-916414096> Acesso em: 10.05.2021.

TJ-MG – Apelação Criminal: 10480110105404001, Relator: Desembargador Agostinho Gomes de Azevedo, Data de Julgamento: 20/08/2015. JusBrasil, 2015. Disponível em: <https://tj-mg.jusbrasil.com.br/jurisprudencia/225500906/apelacao-criminal-apr-10480110105404001-mg> Acesso em: 10.05.2021.

TJ-SC - APELAÇÃO CRIMINAL: 00134605420148240023 Capital 0013460-54.2014.8.24.0023, Relator: Norival Acácio Engel, Data de Julgamento: 26/11/2019, Segunda Câmara Criminal. JusBrasil, 2019. Disponível em: <https://tj-sc.jusbrasil.com.br/jurisprudencia/794762222/apelacao-criminal-apr-13460542014824 0023-capital-0013460-5420148240023/inteiro-teor-794762227> Acesso em: 10.05.2021.

TRF-3.Apelação Criminal: 00045947020164036113 SP, Relator: Desembargador Federal José Lunardelli, Data de Julgamento: 12/03/2019. Décima primeira turma. JusBrasil, 2019. Disponível em: < https://trf-3.jusbrasil.com.br/jurisprudencia/910083085/apelacao-criminal-ap-45947020164036113-sp>. Acesso em: 10.05.2021.

TRF-1. Habeas Corpus: 76.689/PB. Relator: Desembargador Hilton Queiroz, Data de julgamento: 28 nov. 2011, JusBrasil, 2011. Disponível em: < https://trf-1.jusbrasil.com.br/jurisprudencia/2315156/habeas-corpus-hc-29296-go-20010100029296-8> Acesso em: 10.05.2021.

TOMAÉL, Maria Inês; MARTELETO, Regina Maria. *Redes sociais: posições dos atores no fluxo da informação*. Encontros Bibli: Revista eletrônica De Biblioteconomia E Ciência Da informação, 2006. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2006v11nesp1p75> Acesso em: 05.04.2021.

TWITTER. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/twitter/#:~:text=O%20Twitter%20foi%20fundado%20em,conte%C3%BAdos%20escritos%2C%20fotografias%20e%20v%C3%ADdeos./> Acesso em: 07.04.2021

WARDLE, Claire. Fake news. It's complicated. *First Draft*, New York, 16 fev. 2017. Disponível em: < https://firstdraftnews.org/latest/fake-news-complicated/> Acesso em: 07.06.2021.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes Cibernéticos*. Ameaças e Procedimentos de Investigação. Rio de Janeiro. Brasport, 2012.

WHATSAPP. *CanalTech.* Disponível em: <https://canaltech.com.br/empresa/whatsapp/#:~:text=O%20WhatsApp%20foi%20fundado%20em,Brian%20Acton%20e%20Jan%20Koum.&text=Focado%20em%20sua%20miss%C3%A3o%20de,em%20mais%20de%20180%20pa%C3%ADses.> Acesso em: 07.04.2021.

ANEXOS

ANEXO I

COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA

PROJETO DE LEI Nº 7.758, DE 2014

Acrescenta dispositivo ao art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal.

Autor: Deputado NELSON MARCHEZAN JUNIOR

Relator: Deputado FÁBIO TRAD

I - RELATÓRIO

Vem à análise da Comissão de Constituição e Justiça e de Cidadania o Projeto de Lei nº 7.758, de 2014, de autoria do ilustre Deputado Nelson Marchezan Junior, que altera o crime de falsidade ideológica, previsto no art. 307 do Código Penal (Decreto-lei nº 2.848, de 7 de dezembro de 1940), para incluir a modalidade eletrônica ou digital do delito, pelo uso de perfis falsos na internet, punível com detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

A matéria foi distribuída unicamente à Comissão de Constituição e Justiça e de Cidadania, nos termos do art. 24, I combinado com o art. 54, I do Regimento Interno da Câmara dos Deputados, para tramitar em regime ordinário, devendo ser submetida à apreciação do Plenário.

Transcorreu em branco o prazo para oferecimento de emendas ao PL 7758/14 na CCJC.

É o relatório.

II - VOTO DO RELATOR

Compete à Comissão de Constituição e Justiça e de Cidadania manifestar-se quanto aos aspectos de constitucionalidade, juridicidade e técnica legislativa, e sobre o mérito da proposição, nos termos regimentais.

O PL 7758/14 está formalmente em harmonia com a Constituição Federal de 1988. O projeto de lei dispõe sobre direito penal, tópico da competência legislativa privativa da União, nos termos do art. 22, *caput* e inciso I; sendo a iniciativa legítima, conforme o art. 48, *caput*; e adequada, pelo teor do art. 61, *caput*.

A técnica legislativa empregada merece reparos, por estar em desacordo com a Lei Complementar nº 95, de 1998, com as alterações introduzidas pela Lei Complementar nº 107, de 2001.

A ementa não faz referência ao cerne do projeto, apenas à alteração na legislação penal – *"acrescenta dispositivo ao art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal"*. O artigo inaugural tem o defeito oposto, indica o objetivo do projeto – *"tipifica penalmente o uso de falsa identidade na rede mundial de computadores"* – sem mencionar que para tanto altera a legislação em vigor.

O *caput* do art. 2º do PL 7758/14 indica que *"o art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte parágrafo único"*, porém o texto legal indicado é de substituição do *caput* do art. 307 do Código Penal. Verifica-se ainda a ausência das iniciais maiúsculas NR entre parênteses para sinalizar a modificação de dispositivos legais vigentes; bem como da cláusula de vigência.

A hipótese parece ser de inclusão de um art. 307-A no Código Penal, de modo a que se preserve o tipo penal de falsidade ideológica, previsto no art. 307, e que se tipifique, não por parágrafo único, mas por novo dispositivo (art. 307-A), a conduta criminosa prevista.

No mérito, tem-se que o ilustre Deputado Nelson Marchezan Junior toma a iniciativa de transpor para o ordenamento jurídico pátrio o crime de *"e-personation"* ou usurpação de identidade ou perfil

eletrônico, o que corresponderia a algo como **e-surpação** de perfil, em português. A conduta faz parte da nova criminalidade virtual e é descrita como:

> *Atribuir-se ou atribuir a terceiro falsa identidade, inclusive por meio da rede mundial de computadores ou qualquer outro meio eletrônico, com o objetivo de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio.*

Como justificativa, o autor indica a importância de se complementar o quadro jurídico brasileiro sobre delitos informáticos, ou crimes eletrônicos, composto pelas Leis nº 12.735, de 2012, e nº 12.737, de 2012, vez que o crime de uso de perfil falso na internet não está alcançado pelas normas vigentes.

O tema já está regulado em parte pela Lei nº 12.737, de 30 de novembro de 2012 – também conhecida como Lei Carolina Dieckmann, em razão da notoriedade do furto de informações do telefone celular da atriz, entre as quais fotografias íntimas, que foram amplamente divulgadas pelos meios de comunicação, causando constrangimento e perplexidade à vítima e a todos que se comoveram com sua exposição.

Dentre outras providências, a Lei Carolina Dieckmann incluiu no Código Penal o crime de invasão de dispositivo informático, no art. 154-A, próximo ao crime de violação do segredo profissional, previsto no art. 154 do CP.

A Lei nº 12.735, de 30 de novembro de 2012, conhecida como Lei Azeredo, em reconhecimento ao trabalho de Eduardo de Azeredo, relator no Senado e na Câmara das proposições que deram origem à norma legal, trata da estruturação dos órgãos da polícia judiciária para combater a ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Com efeito, ainda não existe dispositivo legal que puna, no Brasil, o uso de perfil falso na internet, do modo proposto pelo PL 7758/14. Para tanto, o Deputado Nelson Marchezan Junior recorreu ao *“legal transplant”* ou transplante de normas, instituto de direito comparado, por reconhecer a

importância de se trazer para o direito brasileiro regra semelhante ao art. 528.5 do Código Penal da Califórnia, nos Estados Unidos, que tem o seguinte teor[1]:

> *528.5.(a) Notwithstanding any other provision of law, any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense punishable pursuant to subdivision (d).*
>
> *(b) For purposes of this section, an impersonation is credible if another person would reasonably believe, or did reasonably believe, that the defendant was or is the person who was impersonated.*
>
> *(c) For purposes of this section, "electronic means" shall include opening an e-mail account or an account or profile on a social networking Internet Web site in another person's name.*
>
> *(d) A violation of subdivision (a) is punishable by a fine not exceeding one thousand dollars ($1,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.*
>
> *(e) In addition to any other civil remedy available, a person who suffers damage or loss by reason of a violation of subdivision (a) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief pursuant to paragraphs (1), (2), (4), and (5) of subdivision (e) and subdivision (g) of Section 502.*
>
> *(f) This section shall not preclude prosecution under any other law.*

O novo tipo penal foi introduzido no Código Penal californiano em 2011, após aprovação de projeto de lei que alterava o crime de falsa representação, previsto desde 1872.

Uma tradução livre do dispositivo da legislação estrangeira (art. 528.5 do Código Penal da Califórnia) tem o seguinte teor:

> *528.5. (a) Mantidas todas as demais provisões legais, qualquer pessoa que sabidamente e sem consentimento imita com credibilidade outra pessoa*

[1] ESTADO DA CALIFÓRNIA. **Penal Code**. State of California: Official California Legislative Information, 2011. Fonte: Legislative Counsel. Disponível em: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>. Acesso em 4 set. 2014.

> *específica através de ou em um sítio da rede eletrônica de computadores, ou por outros meios eletrônicos, com intenção de ferir, intimidar, ameaçar ou defraudar outra pessoa é culpada de um delito de ordem pública punível de acordo com o subitem (d).*
>
> *(b) Para os fins deste dispositivo, uma imitação tem credibilidade se outra pessoa, em sã consciência, acreditar, ou tiver acreditado, que o acusado era ou é a pessoa imitada.*
>
> *(c) Para os fins deste dispositivo, o termo "meios eletrônicos" deve abranger a abertura de uma conta de correio eletrônico [e-mail] ou uma conta ou perfil em rede social em um sítio da rede eletrônica de computadores em nome de outra pessoa.*
>
> *(d) A violação do disposto no subitem (a) é punível com multa de até mil dólares ($ 1.000), ou detenção em uma prisão municipal por até um (1) ano, ou ambas.*
>
> *(e) Sem prejuízo de outras medidas de responsabilização civil disponíveis, a pessoa que sofrer dano ou prejuízo em razão da violação do disposto no subitem (a) pode mover ações cíveis contra o autor do delito para compensação ou reparação de danos, entre outras medidas cautelares e tutelas antecipatórias previstas nos parágrafos 1, 2, 4 e 5 dos itens (e) e (g) do artigo 502.*
>
> *(f) O disposto nesta seção não impede a persecução criminal com base em outra norma legal.*

Comparando-se os dispositivos, vê-se que o autor do PL 7758/14 foi feliz ao transpor as regras da legislação californiana para o nosso Código Penal. O novo dispositivo considera crime:

> *Atribuir-se ou atribuir a terceiro falsa identidade, inclusive por meio da rede mundial de computadores ou qualquer outro meio eletrônico, com o objetivo de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio.*

A sanção penal prevista – detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave – está lançada de forma proporcional em relação ao crime de falsidade ideológica e aos demais delitos informáticos tipificados no Brasil.

A pergunta que se pode fazer é se esse seria o caminho para punir a delinquência digital. Alguns estudiosos, especialmente dos Estados Unidos, país que está na gênese da inovação legislativa em tema de

política criminal digital, no mundo, têm advertido sobre a possibilidade de rápida obsolescência dessas normas penais.

O principal argumento para que se evite a introdução de tipos penais eletrônicos é que se tratam dos mesmos delitos já previstos nos códigos penais tradicionais, com o diferencial de serem cometidos no meio ambiente digital[2].

A velocidade com que evoluem os dispositivos e programas informáticos seria, portanto, incompatível com a necessária estabilidade e solidez do direito penal. Essas críticas são feitas inclusive à legislação comparada[3] na qual se inspira o PL 7758/14.

Além disso, pode-se argumentar que já existe a ferramenta de verificação de autenticidade de perfil eletrônico, um recurso muito utilizado por personalidades políticas e do meio artístico, vítimas preferenciais da e-surpação de perfil. A questão é que esse recurso é privado, pago, portanto, e nem todas as vítimas são celebridades públicas; ou seja, o poder público deve ser capaz de proteger todos os jurisdicionados dos ataques de cibercriminosos.

Para isso está a postos o Poder Legislativo no século XXI, para lidar com a realidade "líquida", em constante transformação, no entender do sociólogo Zygmunt Bauman[4]. O desafio dos novos legisladores é, em grande parte, saber selecionar, dentre as proposições em trâmite, aquelas que são relevantes, ainda que possam ser efêmeras, das que são meramente casuísticas e passageiras, não estando destinadas a compor o corpo jurídico penal.

Mesmo admitindo a possibilidade de ver a legislação penal brasileira sobre ciberdelinquência caducar precocemente, em razão das vertiginosas mudanças no campo da tecnologia da informação, tem-se como fundamental a inclusão no Código Penal de novo dispositivo que tipifique como crime e puna a conduta de uso de perfil falso na internet com o objetivo de

---

[2] CONTE Christiany Pegorari; FIORILLO, Celso Antonio Pacheco. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

[3] RAMASASTRY, Anita. California's E-personation Statute: a recent New Jersey case shows why new laws aren't really needed to address fake Facebook profiles and the like. In: **Verdict Legal Analysis and Commentary from Justia**, November 22, 2011. Fonte: Justia. Disponível em: <http://verdict.justia.com/2011/11/22/dealing-with-e-personation>. Acesso em 4 set. 2014.

[4] BAUMAN, Zygmunt. **Legisladores e intérpretes**: sobre modernidade, pós-modernidade e intelectuais. Rio de Janeiro: Zahar, 2010.

prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio.

Essa é medida que se impõe para dar ao jurisdicionado meios de conter mais um fenômeno da criminalidade digital, a **e-surpação** de perfil, que tem vitimado os cidadãos de bem que, inevitavelmente, precisam se identificar e criar perfis e contas em redes sociais e em sítios da rede mundial de computadores, e que têm sua identidade usurpada com fins escusos.

Diante do exposto, votamos pela constitucionalidade, juridicidade, adequada técnica legislativa; e, no mérito, pela aprovação do Projeto de Lei nº 7.758, de 2014, nos termos do Substitutivo apresentado.

Sala da Comissão, em de de 2014.

Deputado FÁBIO TRAD
Relator

COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA

SUBSTITUTIVO AO PROJETO DE LEI Nº 7.758, DE 2014

Dispõe sobre o crime de usurpação de identidade ou perfil eletrônico, ou uso de falsa identidade na rede mundial de computadores, ao acrescentar o art. 307-A ao Decreto-lei nº 2.848, de 7 de dezembro de 1940 – Código Penal.

O Congresso Nacional decreta:

Art. 1º Esta lei acrescenta o art. 307-A ao Código Penal, para tipificar e punir a conduta de usurpação de identidade ou perfil eletrônico, ou uso de falsa identidade na rede mundial de computadores.

Art. 2º O Decreto-lei nº 2.848, de 7 de dezembro de 1940 – Código Penal passa a vigorar acrescido do seguinte artigo 307-A.

Art. 307-A. Atribuir-se ou atribuir a terceiro falsa identidade, por meio da rede mundial de computadores ou qualquer outro meio eletrônico, com o objetivo de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio.

Pena – detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. (NR)

Art. 3º Esta lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação.

Sala da Comissão, em de de 2014.

Deputado FÁBIO TRAD
Relator

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, STÉPHANIE MARTINEZ DUARTE

Aluno(a), regularmente matriculado(a), no Curso de Direito, na disciplina do TCC da 10ª etapa, matrícula nº 31619770, Período Noturno, Turma U,

tendo realizado o TCC com o título: PERFIS FALSOS EM REDES SOCIAIS CONTEMPORÂNEAS: Uma análise quanto às responsabilidades Penal e Civil.

sob a orientação do(a) professor(a): Profa. Dra. Maria Patricia Vanzolini Figueiredo

declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 19 de maio de 2021.

Stephanie Martinez Duarte

Assinatura do discente