CATFISHING: CRIME DE FALSA IDENTIDADE?

CATFISHING: FAKE IDENTITY CRIME?

Anaflavia Cera Daltro de Castro*

Margareth Vetis Zaganelli**

SUMÁRIO: Introdução. 1 Catfishing. 2 Insegurança Jurídica Acerca de Crimes Digitais. 3 Catfishing nas legislações brasileira e estrangeira. 4 Falsa Identidade. 5 Caráter Subsidiário do Crime. 6 Meios de Coibicão. Conclusão.

RESUMO: O presente artigo possui como escopo a análise do *catfishing*, termo americano utilizado para descrever o ato de criação de um perfil falso em redes sociais ou em sites de relacionamento, com a intenção de enganar outras pessoas emocionalmente, que pode ter várias motivações, como vingança, solidão, curiosidade ou até mesmo tédio. Primeiramente, o trabalho evidencia como essa é uma prática crescente no Brasil e no mundo. A seguir, aborda a falha da legislação brasileira em lidar com crimes digitais. Em seguida, compara a tipificação penal da conduta na legislação brasileira em relação à legislação estrangeira. Por fim, examina a possibilidade de enquadramento da prática do *catfishing* na conduta tipificada no artigo 307 do Código Penal brasileiro, crime de falsa identidade. Por meio de metodologia qualitativa de natureza exploratória, de levantamento bibliográfico e à luz da legislação sobre crimes digitais e do PL nº 7.758/2014, o trabalho busca ressaltar a necessidade de tutela das vítimas da prática em comento.

Palavras-chave: falsa identidade. catfishing. redes sociais. crime digital.

ABSTRACT: The following article analyzes catfishing, american term that describes the act of creating a fake profile on social media and on online relationship websites, one of the many coups that there are in the virtual world. Firstly, the paper highlights how catfishing has been growing in Brazil and around the world, a phenomenon in which a person creates one or more virtual fake identities to fool other users emotionally and that can have various motivations: vengeance, solitude, curiosity or even boredom. Then, examines foreign laws and compares them to the current brazilian juridical order. Then, the article approaches if it is possible to frame this act under the

*Graduanda em Direito pela Universidade Federal do Espírito Santo (UFES).

"Doutora em Direito pela Universidade Federal de Minas Gerais (UFMG). Mestre em Educação pela Universidade Federal do Espírito Santo (UFES). Estágios de Pósdoutorado na Università degli Studi di Milano-Bicocca (UNIMIB), na Alma Mater Studiorum Università di Bologna (UNIBO) e na Università degli Studi Del Sannio (UNISANNIO). Professora Titular de Direito Penal e Processual Penal e de Teoria do Direito da Universidade Federal do Espírito Santo (UFES). Docente Permanente do Programa de Pós-Graduação em Gestão Pública da Universidade Federal do Espírito Santo (UFES). Membro da Associação Argentina de Bioética Jurídica. Coordenadora do Bioethik - Grupo de Estudos e Pesquisas em Bioética (UFES), do Grupo de Estudos e Pesquisas MIGRARE: Migrações, Fronteiras e Direitos Humanos (UFES) e do Grupo de Estudos e Pesquisas "Direito & Ficção".

Artigo recebido em 16/01/2020 e aceito em 30/08/2021.

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

typified conduct of article 307 of Brazilian's Penal Code, the fake identity crime. Through qualitative exploratory nature, bibliographic survey and under the digital crimes legislation and the Project of Law n. 7758/2014, the work seeks to highlight the necessity of protection from catfishing victims.

Keywords: fake identity. catfishing. social media. digital crime.

INTRODUÇÃO

Ocatfishing, ato analisado no presente estudo, corresponde à criação de perfis falsos em mídias sociais, que possuem como objetivo ludibriar os internautas e seduzi-los a entrar em um relacionamento. Os relatórios disponibilizados por redes sociais como o Facebook e o Twitter mostram a grande quantidade de perfis inidôneos que permeiam o ambiente virtual.

Apesar dos recentes avanços na área, crimes digitais ainda não são suficientemente regrados no Brasil. A internet e os meios eletrônicos estão em constante avanço e precisam de regulação por meio de uma legislação com nomenclaturas abertas, para que seja possível abranger eventual desenvolvimento e não precisem ser constantemente atualizadas.

Atualmente, o Brasil conta com a Lei 12.965/2014 (Marco Civil da Internet), a Lei 12.735/2012 (Azeredo) e a Lei 12.737/2012 (Carolina Dieckmann), as quais são insuficientes, visto que tratam de poucos crimes e usam termos incapazes de abarcar o desenvolvimento tecnológico. Ademais, o país não é signatário de nenhum tratado internacional acerca do assunto, sendo que a Convenção de Budapeste, acordo mais eficiente na área, está em vigor desde 2004.

O Projeto de Lei nº 7.558/2014 propõe mudanças no artigo 307 do Código Penal, o qual trata do crime de falsa identidade, de modo que a possibilidade de operação do crime pela internet ou por outros meios eletrônicos seja especificada.

Considerando a falta de regulamentação exata e a grande periculosidade do *catfishing*, é essencial que a tutela ocorra por meios que já existem, como o crime de falsa identidade. Desse modo, é essencial demonstrar como o PL nº 7.758 pode ser utilizado para viabilizar a tutela do *catfishing* dentro do atual sistema normativo brasileiro.

1 CATFISHING

Catfishing é um termo americano utilizado para descrever o ato de criar uma identidade falsa ou roubar a de outra pessoa para enganar indivíduos online e os seduzir a entrar em um relacionamento. Isso

normalmente ocorre por meio da criação de perfis não autênticos em mídias sociais e em sites de relacionamento.

Essa palavra surgiu com o documentário *Catfish*, lançado em 2010 e produzido por Henry Joost e Ariel Schulman, o qual conta a história de Yaniv Schulman, vítima de *catfishing*. O jovem conhece virtualmente e começa a se relacionar com uma suposta menina de 19 anos e com sua família, mas desconfia que está sendo enganado e viaja com seu irmão Ariel para descobrir a verdade. Quando chega ao seu destino, Yaniv descobre que sua namorada era, na verdade, uma mulher adulta e que as fotos utilizadas em suas redes sociais eram de uma modelo canadense.

Após o sucesso do filme, os irmãos Schulman, protagonistas e produtores, começaram a receber centenas de relatos pessoais descrevendo situações parecidas por meio de e-mails. Yaniv conta que, apesar de suas expectativas, as pessoas pediam conselhos de como agir e contavam sobre como estavam desconfiando de seus relacionamentos virtuais. O êxito do filme fez com que o canal MTV iniciasse uma série de TV, na qual Yaniv Schulman e Max Joseph ajudam os participantes a descobrir se seus namoros e parceiros são reais ou não.

Segundo dados da Organização das Nações Unidas (2017), no seu relatório da Conferência das Nações Unidas Sobre Comércio e Desenvolvimento (UNCTAD), o Brasil é o quarto país mundial com maior número absoluto de usuários na internet. Logo, fica claro que há um enorme contingente de acesso à rede, dados preocupantes quando somados à proporção de perfis falsos em relação aos verdadeiros encontradas nos relatos de empresas como o Twitter e o Facebook.

De acordo com os relatórios do Twitter de 2013 (D'ONFRO, 2013), 5% de todos os seus usuários eram contas falsas, isso representa 10.75 milhões das 215 milhões de contas "ativas" na rede. Além disso, o Facebook estima que 91 milhões de seus perfis ativos em 2018 tenham sido falsos (NICAS, 2019). As estatísticas mostram que as redes sociais são ambientes perigosos, visto que a quantidade de contas não autênticas é gigantesca.

Contudo, as empresas possuem políticas de proteção dos seus usuários, por meio da coibição da criação desses perfis e da exclusão dos que já existem. O Facebook descreve no *Newsroom* (SCHULTZ, 2019), seu canal oficial, algumas das ferramentas utilizadas para evitar a proliferação de perfis *fakes*. A primeira delas é a análise de antigos perfis que tenham sido identificados como falsos e maldosos para que haja a junção de suas

características principais, logo, novos perfis que se encaixem nesses padrões são bloqueados. Em seguida, o Facebook impede IPs que tenham criado muitas contas em um curto período de tempo de se inscreverem novamente no site. Por fim, sua solução repressiva é tirar do ar perfis que tenham sido identificados pela própria empresa ou denunciados por usuários.

Essas soluções, todavia, não são totalmente eficazes. O jornalista Jack Nicas do The New York Times fez, em 2019, uma reportagem comparando os dados que o próprio Facebook libera e analisando também suas experiências pessoais, o que o levou à conclusão de que as informações da empresa são incompatíveis entre si e com a realidade.

Por exemplo, como demonstrado anteriormente, a rede social declarou uma estimativa de 91 milhões de perfis falsos ativos em 2018. Entretanto, dentro de sua própria plataforma de transparência, segundo os dados do The New York Times, expôs que 754 milhões de contas falsas haviam sido retiradas do ar no mesmo ano, número muito maior do que o anterior.

Ademais, a rede social alega em suas mídias oficiais que excluiu 90% das contas falsas criadas minutos após o seu registro e que identifica por si só 99% das que já estão ativas, o que demonstra que as denúncias dos usuários seriam apenas uma ferramenta subsidiária (SCHULTZ, 2019). Todavia, Jack Nicas conta em sua matéria como criou 11 perfis exatamente iguais no Facebook e 10 no Instagram, empresa da qual Mark Zuckerberg também é dono. Os resultados foram que, no intervalo de 5 dias, nenhuma conta foi retirada do ar na primeira rede antes que o próprio jornalista as denunciasse e apenas metade foi excluída na segunda.

Os dados de redes sociais, todavia, não são os únicos a serem analisados. A Federal Trade Comission (FTC), agência governamental americana, fez um levantamento de dados sobre os casos de *catfishing* em 2018. O documento Consumer Sentinel Work Data Book demonstrou que os episódios reportados ao FTC entre 2015 e 2018 subiram de 8,5 mil para 21 mil.

Os casos de *catfishing* são cada vez mais frequentes e podem deixar graves danos às vítimas. Quando eles ocorrem, duas pessoas são as principais afetadas: quem tem suas fotos utilizadas e quem é enganado. No presente artigo trataremos da relação entre o *catfish*, a vítima que se relaciona virtualmente com ele e a sociedade, visto que o direito penal tem como principal objetivo a defesa do interesse social e a manutenção da ordem.

A primeira vez que o termo foi utilizado dentro de um processo judicial nos Estados Unidos foi no caso de Manti Te'o, jogador de futebol americano da Universidade de Notre Dame, localizada no estado Indiana. Horas antes de um jogo contra a Universidade de Michigan, Te'o recebeu uma mensagem que informava sobre o falecimento de sua avó e de sua namorada virtual, Lennay Kekua, o que abalou o seu estado emocional.

O caso ocorreu em 2012, mas apenas em 2013 a verdade foi revelada: Manti havia sido enganado e sua namorada Lennay foi inventada por Ronaiah Tuiasosopo, jovem de 22 anos que estava apaixonado por Te'o.

Outro caso que ficou famoso na Grã-Bretanha foi o de Ruth Palmer. Em 2015, a jovem descobriu que suas fotos estavam sendo utilizadas por outra pessoa – a qual se denominava Leah Palmer – em perfis falsos no Instagram, no Facebook, no Twitter e no Tinder desde 2012.

Dentre as postagens dos perfis falsos, havia fotos de Ruth Palmer e seu marido, Benjamin Graves, que o descreviam como o ex-namorado psicótico de Leah Palmer e relatavam que ele perseguia Leah. Ademais, os perfis eram utilizados para seduzir companheiros online, de forma que uma das vítimas chegou a terminar um relacionamento da vida real para namorar Leah Palmer.

Além disso, foram criados vários perfis fingindo serem da família e dos amigos de Ruth, os quais interagiam com ela online para dar um ar mais real à página falsa de Leah, mas que a polícia desconfia que fossem administrados pela mesma pessoa.

O caso de Ruth não teve resolução, a jovem denunciou os perfis para as redes sociais, mas, após serem excluídos, foram recuperados quase imediatamente. Além disso, a polícia não conseguiu enquadrar a conduta em nenhum crime. Dessa maneira, a vítima continuou sem tutela.

Esses são apenas alguns dos vários casos onde pessoas são enganadas diariamente e seduzidas a acreditar em um relacionamento com uma pessoa inexistente, os danos psicológicos e emocionais causados por uma relação assim são imensuráveis e devem ser evitados.

A partir dos dados e casos analisados, é perceptível que as políticas de proteção das redes sociais não são suficientemente confiáveis, tampouco seguras. Logo, é fundamental que o Estado intervenha para cumprir seu objetivo de tutelar direitos e pessoas.

2 INSEGURANÇA JURÍDICA ACERCA DE CRIMES DIGITAIS

Segundo a Organização para a Cooperação e Desenvolvimento Econômico da Organização das Nações Unidas, crime de computador é "qualquer comportamento ilegal, aético, ou não autorizado envolvendo processamento automático de dados e/ou transmissão de dados" (BORTOT, 2017, p. 4). Assim, devem ser condutas típicas, antijurídicas e culpáveis, praticadas por meio de sistema informático.

O direito é um produto cultural e uma ferramenta de solução de conflitos que deve estar em consonância com a sociedade a qual regula. Logo, deve se atualizar de acordo com as mudanças sociais. Todavia, essa não é a realidade prática encontrada quando se analisa a relação do direito e da internet.

A tecnologia está em constante evolução, trazendo muitas consequências práticas ao cotidiano da população brasileira. Por isso, foi criado e está em avanço o direito digital, o qual representa um desenvolvimento em relação ao direito em si, mas que, no Brasil, ainda não é suficiente para abarcar todos os conflitos.

No presente artigo, trataremos principalmente sobre crimes digitais e sua falta de regulação no ordenamento jurídico brasileiro. É fundamental ressaltar que estes são, em sua maioria, crimes já previstos na ordem brasileira, mas que são colocados em prática por meio de uma nova ferramenta: a internet. Dessa maneira, via de regra, não é necessária a criação de leis novas, mas sim a adaptação de leis já existentes para que abranjam o novo modo de operação dos mesmos crimes.

As principais legislações brasileiras acerca da informática são o Marco Civil da Internet (Lei 12.695/2014), a Lei Carolina Dieckmann (Lei 12.737/2012) e a Lei Azeredo (Lei 12.735/2012). Contudo, essas leis não são suficientes para abordar grande parte das situações fáticas que necessitam de tutela atualmente. Isso se dá, primeiramente, pelo fato de que os conflitos abordados em tais textos normativos são limitados, sendo insuficientes perante ao desenvolvimento tecnológico, que acontece de maneira rápida, gerando cada vez mais situações que necessitam de tutela.

Em seguida, deve-se entender que a linguagem utilizada em sua redação não é abrangente o suficiente, ela trata de dispositivos que são atuais no momento da promulgação da lei, mas que podem se tornar obsoletos e inutilizados em um curto período de tempo. Logo, seria

necessário que houvesse uma constante atualização dos termos para que a realidade continuasse a ser eficientemente protegida.

Por fim, o maior problema é que esses dispositivos são nacionais. Dessa forma, são limitados por princípios como o da territorialidade e nacionalidade, já que a lei brasileira, via de regra, não pode ser aplicada fora de seu território.

Nesse sentido, insta frisar que os crimes digitais, frequentemente, são cometidos de maneira a gerar repercussões internacionais, sendo essencial a assinatura do Brasil em tratados internacionais, cuja área de atuação não se limite à extensão territorial de apenas um país.

A Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, é um tratado internacional de direito penal e de direito processual penal que foi adotada na Sessão 109 do Comitê de Ministros do Conselho da Europa, em 2001.

O documento possui quatro capítulos, os quais tratam de terminologias, medidas a serem tomadas em nível nacional e cooperação internacional entre os países signatários. Apesar de não tratar especificamente do *catfishing*, esse tratado é atualmente o mais completo no que tange à crimes virtuais, visto que utiliza nomenclaturas abertas, as quais se adaptam ao desenvolvimento tecnológico sem demandar constantes mudanças na redação do documento.

Outrossim, a Convenção de Budapeste permite que seus os países signatários cooperem entre si, por exemplo, por meio da concessão de acesso rápido a provas eletrônicas que estejam sob jurisdição de outro país.

Atualmente, a Convenção conta com mais de 60 signatários, dentre os quais o Brasil ainda não está incluso. Contudo, após esforços do Ministério Público Federal (MPF), do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública, o Brasil foi convidado pelo Comitê de Ministros do Conselho da Europa para aderir à Convenção.

Em junho de 2019, o MPF se reuniu na Câmara dos Deputados para debater sobre a assinatura do Brasil na Convenção de Budapeste, em encontro promovido pela Comissão de Segurança Pública e Combate ao Crime Organizado, no qual a Procuradora regional da República Neide Mara Cavalcanti Cardoso de Oliveira, coordenadora do Grupo de Apoio sobre Criminalidade Cibernética, apresentou sua proposta.

A Procuradora divulgou dados do órgão sobre as dificuldades na persecução de crimes digitais, as quais se materializam na falta de legislação nacional e internacional acerca do assunto e na baixa capacitação dos agentes que lidam com tais problemas.

Além disso, Neide Mara Cavalcanti Cardoso de Oliveira defendeu a criação de um ambiente virtual mais seguro por meio da implementação de algumas mudanças, como melhor capacitação dos agentes públicos, criação de grupos especializados no Ministério Público Federal, Estadual e nas polícias e a assinatura do Brasil no tratado em questão.

Segundo informações do sítio eletrônico do Governo Federal (2019), após os incentivos do Ministério Público Federal, o Governo brasileiro manifestou seu interesse em aderir à Convenção com base em pareceres técnicos da Polícia Federal (PF) e do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional.

Assim, em dezembro de 2019, o Comitê de Ministros do Conselho da Europa convidou o Brasil para integrar o grupo dos não-membros do Conselho da Europa que assinam e ratificam a Convenção (GOVERNO FEDERAL, 2019).

Ato contínuo, o Presidente da República Jair Bolsonaro, por meio da Mensagem nº 412 de 22 de julho de 2020, encaminhou o texto da Convenção sobre o Crime Cibernético ao Congresso Nacional, com objetivo de adesão brasileira ao instrumento (2020).

Dessa forma, a aprovação do texto da Convenção está sob discussão no Projeto de Decreto Legislativo de Acordos, Tratados ou Atos Internacionais nº 255/2021. O regime de tramitação do PDL é de urgência, de acordo com o que foi solicitado pelo Ministério Público Federal por meio do Ofício nº 736/2020.

Destarte, percebe-se que o ordenamento jurídico está em processo de desenvolvimento para que os crimes cibernéticos sejam devidamente tutelados, de forma que a Convenção de Budapeste servirá como um forte instrumento de coibição de tais práticas, principalmente se utilizado em conjunção com as legislações brasileiras atualmente existentes.

3 CATFISHING NAS LEGISLAÇÕES BRASILEIRA E ESTRANGEIRA

A prática do *catfishing* é extremamente perigosa e já teve sua importância reconhecida em outros países, como os Estados Unidos, sendo que estados como Texas, California e Oklahoma criaram leis específicas para tratar do assunto.

Em fevereiro de 2009, a House Bill 2003 foi apresentada para a Câmara de Representação dos Estados Unidos, a casa "mais baixa" do Congresso (sendo o Senado a casa mais alta). Os representantes Joaquin Castro, Brian McCall e Robin Duke Orr do Texas pretendiam alterar o capítulo 33 do Código Penal texano, adicionando a seção 33.07, a qual transforma em crime de terceiro grau o ato de utilizar o nome ou a imagem de outra pessoa em um site de interação comercial ou social e em uma infração de menor potencial ofensivo de classe A o ato de mandar mensagens eletrônicas a partir de uma conta que utilize as informações de outro cidadão.

Ademais, vale citar que a redação da House Bill especifica sites de interação comercial ou social como qualquer rede, negócio ou organização online que opera através de um site e permite usuários a se registrarem e estabelecerem relações pessoais com outros internautas através de mensagens instantâneas. Logo, redes sociais e sites de relacionamento estão inclusos na área de atuação da lei.

O projeto foi aceito e passou a valer em junho de 2009.

Ademais, em fevereiro de 2010, o Senador Joe Simitian apresentou a Senate Bill 1.411 ao estado da Califórnia, o que equivale a um Projeto de Lei no Brasil, a qual pretendia alterar a seção 528.5 do Código Penal californiano. A Senate Bill passou a classificar como uma infração de menor potencial ofensivo o ato de criação de um perfil online, no qual uma pessoa mente sua identidade com a intenção de ferir, intimidar, ameaçar ou defraudar. Além disso, a vítima de tenha sofrido danos ou perdas poderia abrir uma ação civil contra qualquer um que viole tal lei. A Senate Bill entrou em vigor em primeiro de janeiro de 2011, estabelecendo a pena para tal crime como multa de U\$1000,00 e/ou detenção de até um ano.

Por fim, em 2016, os legisladores John Paul Jordan e David Holt do Oklahoma apresentaram a House Bill 3024, conhecida como Catfishing Liability Act of 2016, a qual foi aprovada em maio de 2016 e passou a valer em novembro do mesmo ano. Ela é conhecida como a lei mais forte dos Estados Unidos no que tange ao *catfishing*, definindo especificamente termos como fotografia e rede social, bem como citando os tipos de danos a serem causados para que a lei se aplique e como esta deve ser aplicada.

4 FALSA IDENTIDADE

Como demonstrado, o Brasil não tem legislação específica acerca do *catfishing*, mesmo que haja necessidade de tutela por parte do Estado.

Logo, é fundamental que as leis brasileiras já existentes sejam adaptadas para que abarquem tal situação. Com esse intento, é possível perceber que a prática em análise pode ser enquadrada sob o crime de falsa identidade.

É de extrema necessidade entender as classificações deste crime para compreender completamente sua semelhança com o *catfishing* e porque um pode ser utilizado para criminalizar o outro.

O crime de falsa identidade está elencado no artigo 307 do Código Penal de 1940:

Art. 307 – Atribuir-se ou 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.

Nele, há a tipificação da ação de imputar características falsas a si ou a outrem, haja vista que elas permitem a identificação do indivíduo e sua distinção de outros, buscando proteger o bem jurídico da fé pública.

Ademais, deve-se especificar o que a doutrina entende como identidade, visto que esse é o núcleo do crime que está em análise. Esta equivale ao conjunto de atributos individuais de cada ser humano, que servem para identificá-lo e distingui-lo dos demais. Por exemplo, há o nome, idade, profissão, sexo, estado civil, filiação, entre outros. Vale ressaltar que endereço e telefone não entram nos aspectos que caracterizam o crime.

Assim, o crime se materializa quando alguém mente sobre esses caracteres, de modo a causar dano a outrem.

Nesse sentido, é possível perceber que o ato de criação de um perfil falso na internet, seja utilizando informações de outras pessoas ou dados inteiramente inventados, corresponde a criar uma falsa identidade.

Quanto ao bem materialmente tutelado, há desentendimento doutrinário. Rogério Greco (2017) acredita que não há bem material em tutela, enquanto Guilherme Nucci (2018) defende que esse bem é a identidade em si.

Sob outro prisma, é fundamental classificar o crime de falsa identidade quanto aos seus elementos penais: eleé, via de regra, crime comum, formal, doloso, comissivo, instantâneo, unissubjetivo e unissubsistente.

Dizer que a falsa identidade configura crime comum significa dizer que ele não exige nenhuma qualidade especial do sujeito ativo, ou seja, pode ser cometido por qualquer cidadão. No mesmo diapasão, vale citar que o sujeito passivo da situação será o Estado, já que o crime é primeiramente contra a fé pública, e, secundariamente, contra a pessoa prejudicada.

Ademais, o tipo penal analisado configura crime formal ou de consumação antecipada. Isso significa dizer que é irrelevante se o resultado almejado por meio da ação foi atingido ou não. Logo, se o agente atribui a si mesmo falsa identidade com a intenção atingir objetivo específico, mas não o atinge, o crime ainda se configura.

Além disso, deve sempre ser em forma dolosa, não há falsa identidade culposa. Dessa forma, o agente deve querer o resultado, enquadrando-se em dolo direto, ou assumir o risco de produzi-lo, de maneira a ter dolo eventual.

Outrossim, o delito em questão ocorre de forma comissiva, ele pressupõe um comportamento positivo do agente, o qual consiste em fazer o que a lei proíbe: atribuir a si ou a terceiro falsa identidade, de modo a causar dano.

Todavia, há discussão doutrinária acerca do assunto. Enquanto Rogerio Sanches (2017) acredita que não há, em hipótese alguma, a forma omissiva do crime, mas Guilherme Nucci (2018) discorda. Nucci defende a existência do crime de modo omissivo impróprio ou omissivo por comissão, quando o agente possui o dever jurídico de evitar o resultado.

Outrossim, o tipo jurídico analisado é instantâneo, ou seja, a ofensa à vítima é imediata, não há possibilidade de que a ação se prolongue no tempo, já que o crime é considerado como cometido logo quando a ação prevista no artigo é colocada em prática.

Além disso, é crime unissubjetivo. Isso significa dizer que não precisa de mais de um agente para que seja cometido, apesar de ser possível o concurso eventual de agentes. Por fim, é unissubsistente, realizado em ato único, sendo impossível o fracionamento da conduta.

5 CARÁTER SUBSIDIÁRIO DO CRIME

O *catfishing*, por proporcionar que a pessoa se esconda atrás de uma identidade que não é a sua, frequentemente é utilizado como meio para a execução de outros crimes, como fraude ou estelionato. É comum que a vítima seja seduzida a entrar em um relacionamento virtual e comece a confiar no seu parceiro, que logo passa a pedir dinheiro e presentes ou tenta aplicar golpes.

Esses golpes funcionam através de histórias que o *catfish* usa para pedir ajuda financeira, contando que ele precisa de dinheiro para viajar e conhecer o namorado ou que um membro de sua família está doente.

Contudo, quando esses casos acontecem, eles não podem mais ser enquadrados sob o crime de falsa identidade, já que este é subsidiário. O princípio da subsidiariedade serve para solucionar aparentes conflitos entre normas, ou seja, quando dada conduta recai ou parece recair sob a incidência de mais de um tipo legal de crime, embora apenas um possa ser aplicado, devido ao princípio *ne bis in idem*, o qual proíbe a dupla valoração da mesma ação.

Segundo os ensinamentos de Paulo Queiroz (2018) a subsidiariedade em tipos penais deve ser aplicada quando a lei descreve vários graus de intervenção aos mesmos bens jurídicos, buscando protegêlos da maneira mais completa possível. Dessa forma, a norma subsidiária só pode ser aplicada quando não couber o enquadramento na norma principal e mais grave.

É importante citar que o caráter subsidiário da lei pode ser expresso, quando a lei deixa explícito que a norma só deve ser aplicada se o fato não constitui crime mais grave - por exemplo no caso do artigo 132 do Código Penal de 1940 - ou pode ser tácito, quando a subsidiariedade depender da interpretação dos tipos penais em questão.

Dizer que o crime de falsa identidade possui caráter subsidiário significa dizer que ele não se configura caso haja, por exemplo, vantagem econômica por parte do agente, já que a ação recairia em outros crimes mais graves, como o estelionato.

Dessa maneira, caso outro delito tenha sido cometido ao mesmo tempo, a falsa identidade seria consumida pelo mais grave, já que apareceria apenas como meio ou instrumento para a realização do crime de real intenção do agente.

Para fins de ilustração, há o artigo 328 do Código Penal de 1940, que versa sobre a usurpação de função pública: se o agente se utiliza de falsa identidade para cometer a ação descrita, ele é imputado segundo o artigo 328, não o 307.

Da mesma forma, caso a intenção visada pelo agente não seja atingida, o enquadramento ainda recai sobre o artigo 307. Logo, se o polo ativo da relação comete o crime de falsa identidade almejando vantagens econômicas e não as alcança, ainda há a tipificação neste.

6 MEIOS DE COIBIÇÃO

Como demonstrado, a legislação brasileira não é suficiente para proteger os usuários da internet de crimes digitais. Dessa forma, é necessária a atualização de leis já existentes para que os conflitos do mundo tecnológico atual sejam abarcados.

Nesse viés, em 2014 foi apresentado o Projeto de Lei nº 7.758 pelo Deputado estadual Nelson Marchezan Júnior (PSDB-RS), o qual pretende alterar o artigo 307 do Código Penal para a seguinte redação:

Art. 307. 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:

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

Uma das justificativas que o Deputado utilizou na redação do seu Projeto de Lei foi a lei californiana anteriormente mencionada, a qual fez muito sucesso entre os criminalistas brasileiros. Entre eles, há o especialista em direito penal empresarial David Rechulski, o qual diz que em 2008 o Brasil teve um milhão de denúncias de crimes praticados em âmbito digital, sendo que a falsa identidade era utilizada como meio em muitos deles.

A proposta do PL nº 7.758 foi apresentada em julho de 2014 e aprovada pela Comissão de Constituição e Justiça e de Cidadania em agosto de 2015. Entretanto, o Relator Deputado Bentinho Gomes (PSDB-PE) alterou o texto original, aumentando a pena em 1/6 a ½ para caso o crime seja pela internet ou por outro meio eletrônico.

Segundo ele, "pouco importa o *modus operandi*. Se pela internet ou não, o delito se perfaz quando alguém atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem". Entretanto, o aumento na pena era necessário porque a internet tornou-se um lugar propício para a prática de crimes, além de facilitar que estes sejam colocados em prática.

Agora, a proposta se encontra pronta para pauta no Plenário, onde será analisada. Caso ela seja aprovada, será encaminhada para o Senado Federal e, posteriormente, para a Presidência da República.

O Projeto de Lei sob análise, apesar de não citar especificamente o *catfishing*, é uma forma de fazer com que a legislação brasileira abarque

tal ato, já que esta prática nada mais é do que uma forma de cometer o crime de falsa identidade utilizando meios tecnológicos.

Insta frisar que, apesar de já ter havido um avanço no direito brasileiro no que tange aos crimes digitais, nenhuma das novas leis abrange especificamente o crime de falsa identidade.

Por exemplo, há a Lei nº 14.155, que foi publicada em maio de 2021 e alterou o Código Penal, tornando mais graves os crimes de violação de dispositivo informático, furto e estelionato que sejam cometidos de forma eletrônica ou pela internet. Outrossim, ela modificou o Código de Processo Penal para definir a competência para o julgamento dependendo das modalidades de estelionato.

Essas modificações certamente representam uma evolução do direito brasileiro no que tange à tipificação de crimes cometidos pela internet. É possível perceber que o legislador se atentou à necessidade de tutelar tais situações, com base na facilitação da execução de crimes que surge dos meios eletrônicos.

Nesse sentido, a promulgação de tal lei demonstra uma preocupação da legislação brasileira em se atualizar e acompanhar as mudanças tecnológicas. Isso porque o uso de expressões como "dispositivo informático" e "forma eletrônica" transparece um cuidado na utilização de palavras abrangentes, que não exijam atualizações constantes.

Contudo, apesar de haver um desenvolvimento, o crime de falsa identidade cometido pela internet continua sem tipificação específica, de forma que as vítimas de certas atividades lesivas permanecem desamparadas.

Dessa maneira, o PL nº 7.758 representa um avanço importante para o ordenamento jurídico brasileiro.

Todavia, é fundamental analisar o objetivo do Projeto de Lei sob comento a partir do prisma das funções da pena, de forma a compreender sua utilidade na inibição do *catfishing* e da falsa identidade cometida por meios virtuais.

Para Claus Roxin, a pena seria um instrumento de prevenção subsidiária, tanto especial como geral (1993, p. 35 *apud* QUEIROZ, 2018, p. 428). Dessa forma, em sua perspectiva geral, a pena se justificaria pelo seu objetivo de proteger bens jurídicos relevantes para a sociedade. Por outro lado, em seu panorama individual, a pena consistiria na ressocialização do condenado.

O jurista ressalta, ainda, que a pena deve ser limitada pela culpabilidade do condenado, haja vista que a atividade punitiva estatal não

deve extrapolar os limites constitucionais, aplicando-se a pena na medida necessária para coibir a atividade que ofendeu o bem jurídico protegido.

Assim, o intento da tipificação de uma atitude tida como lesiva a um bem jurídico é a sua proteção e a inibição de eventuais ações que venham a repetir o ato danoso, por meio da ressocialização do condenado.

Nesse sentido, o PL nº 7.758 traz inovações que estão em consonância com as finalidades da pena. Isso porque ele pretende incluir na descrição do crime a possibilidade da utilização de meios eletrônicos ou da rede mundial de computadores, de modo a especificar o tipo penal, bem como elevar a pena nas situações em que esses meios são utilizados.

Logo, busca-se demonstrar para a sociedade a gravidade da utilização da internet para a prática de atos ilegais, o que conflui com o objetivo da pena de proteger bens jurídicos relevantes. A tipificação de uma atitude demonstra a sua expressividade para o Estado, realçando e difundindo a pertinência de proteger o bem jurídico. Consequentemente, sua salvaguarda é facilitada.

Ademais, o aumento da pena nos casos em que a falsa identidade é cometida por meio da internet colabora para esse realce, já que salienta o perigo advindo das referidas situações.

Sob outro viés, a perspectiva da prevenção individual se torna mais tangível a partir do momento da execução da pena, já que há a concretização da previsão legal e, por consequência, de sua intenção originadora.

Caso o Projeto de Lei com a alteração do Relator Deputado Bentinho Gomes (PSDB-PE) seja aprovado, a pena do crime de falsa identidade quando cometido por meios eletrônicos será de detenção por, no máximo, um ano e quatro meses ou multa.

Dessa forma, de acordo com o art. 44 do Código Penal, é possível que haja a substituição da pena privativa de liberdade por penas restritivas de direito, visto que a pena aplicada seria inferior a quatro anos. Vale ressaltar que os outros requisitos para a substituição também devem ser cumpridos. Por exemplo, não pode haver violência ou grave ameaça à pessoa.

Nesse caso, penas como prestações pecuniárias, perdas de bens e valores, limitações em fins de semana, prestação de serviço à comunidade ou a entidades públicas e interdições temporárias de direitos podem ser aplicadas em alternativa à detenção.

Essas possibilidades previstas pelo Código Penal seriam mais eficientes na persecução da prevenção individual, haja vista que mais úteis para obter a ressocialização do condenado.

Nesse sentido, a prestação de serviço à comunidade ou a entidades públicas, por exemplo, é um forte instrumento para a ressocialização. É possível inserir o indivíduo em atividades relacionadas à importância de se respeitar a identidade alheia, demonstrando os riscos lesivos de utilizar fotos de outra pessoa para criar perfis falsos em redes sociais.

Além disso, também é concebível a sua introdução em ambientes de recuperação psicológica, objetivando expô-lo ao contato com cenários de recuperação das vítimas do *catfishing*.

Portanto, é possível concluir que as alterações pretendidas pelo PL nº 7.758 permitem o alcance dos objetivos e finalidades da pena, porque ressaltam a importância de proteger o bem jurídico, facilitando esse processo, bem como permitem a aplicação de penas justas e necessárias, que são capazes de ressocializar o condenado e inibir condutas idênticas posteriores.

CONCLUSÃO

O presente trabalho teve como escopo a análise do *catfishing* (criação de perfis falsos em redes sociais) e de sua relação com crime de falsa identidade, de modo que haja uma tutela eficiente de crimes digitais e a defesa da fé pública.

Foi demonstrado que o Brasil não possui um direito digital bem desenvolvido e suficiente para resolver os conflitos que surgem diariamente. Assim, algumas soluções seriam a assinatura do país à Convenção de Budapeste, tratado internacional mais eficiente atualmente acerca do tema, bem como a aceitação do Projeto de Lei nº 7.558/2014, que especifica a possibilidade de ocorrência do crime de falsa identidade no âmbito digital, além de prever o aumento da pena para quando isso ocorra.

Além disso, visto que crimes digitais são apenas o novo modo de operação de um crime já existente e que a legislação não pode ser alterada constantemente para acompanhar a evolução da tecnologia, não é plausível a criação de novas leis para tratar destes. Logo, as leis antigas devem ser atualizadas de modo abrangente, para que sejam capazes de tutelar os novos acontecimentos.

A solução apresentada para o problema do *catfishing* é o enquadramento dessa prática no artigo 307 do Código Penal, que trata do crime de falsa identidade, já que esta é justamente a apropriação que

alguém faz da identidade do outro para causar dano a outrem, por via de meios eletrônicos.

REFERÊNCIAS

BLAZKA, Matthew. SMITH, Kenny D. SMITH, Lauren Reichart. Follow me, what's the harm? Considerations of Catfishing and Utilizing Fake Personas on Social Media. **Journal of Legal Aspects of Sport**. Nova Iorque, 2017 n. 27, v. 1, p. 32-45. Disponível em: file:///C:/ Users/Usu%C3%A1rio/Downloads/27JLegalAspectsSport32.pdf. Acesso em: 5 nov. 2019.

BLUE, Violet. **Analysis: California's Online Impersonation Law, Effective January 1.** ZDNET, 30 dez. 2010. Disponível em: https://www.zdnet.com/article/analysis-californias-online-impersonation-law-effective-january-1/?tag=mantle_skin;content. Acesso em: 14 jan. 2020.

BORTOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com base nas Legislações Brasileira e Internacional. **VirtuaJus**, Belo Horizonte, n. 2, v. 2, 2017. Disponível em: file:///C:/Users/Usu%C3%A1rio/Downloads/15745-Texto%20 do%20artigo-56007-2-10-20180808.pdf. Acesso em: 5 nov. 2019.

BRASIL. Congresso Nacional. **Projeto de Lei nº 7.558/2014**, versão final. Acrescenta dispositivo ao art. 307 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 — Código Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1263593&filename=PL+7758/2014. Acesso em: 19 nov. 2019.

BRASIL. Despachos do Presidente da República. **Diário Oficial da União**, Brasília, DF, 24 jul. 2020. Disponível em: https://www.in.gov.br/web/dou/-/despachos-do-presidente-da-republica-268441788. Acesso em: 2 ago. 2021.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. **Diário Oficial da União**, Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 8 nov. 2019.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Diário Oficial da União**, Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 8 nov. 2019.

- BRASIL. Lei nº 12.965, de 23 de abril de 2014. **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: 8 nov. 2019.
- BRASIL. Lei nº 14.155, de 27 de maio de 2021. **Diário Oficial da União**, Brasília, DF, 27 mai. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 3 jul. 2021.
- CALIFORNIA. **California's Penal Code**, de 1872. Disponível em: https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode =PEN&tocTitle=+Penal+Code+-+PEN. Acesso em: 14 jan. 2020.
- CALIFORNIA. Senate Bill 1411, de 19 de fevereiro de 2010. Disponível em: http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200920100SB1411. Acesso em: 16 jan. 2020.
- CONSELHO DA EUROPA. Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime. Budapeste, 08 nov. 2019. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Acesso em: 8 nov. 2019.
- CONSUMIDOR MODERNO. **Você Sabe O Que É Catfishing?** São Paulo, 27 mar. 2019. Disponível em: https://www.consumidormoderno.com.br/2019/03/27/voce-sabe-catfishing/. Acesso em: 13 jan. 2020.
- CONVENÇÃO de Budapeste sobre crimes cibernéticos = **BUDAPEST** Convention on Cybercrime. 23 nov. 2001. Disponível em: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest /7 conv budapest en.pdf. Acesso em: 8 nov. 2019.
- CUNHA, Rogerio Sanches. **Manual de Direito Penal Parte Especial**. 8. ed. Salvador: Editora Juspodivm, 2016.
- D'ONFRO', Jillian. **Twitter Admits 5% Of Its 'Users' Are Fake**. Business Insider, 03 out. 2013. Disponível em: https://www.businessinsider.com/5-of-twitter-monthly-active-users-are-fake-2013-10. Acesso em: 7 nov. 2019.
- ESPN. **Hoaxer was in love with Manti Te'o.** Indiana, 31 jan. 2013. Disponível em: https://www.espn.com/college-football/story/_/id/8900688/ronaiah-tuiasosopo-says-was-love-manti-teo. Acesso em: 8 nov. 2019.

FEDERAL TRADE COMISSION. **Consumer Sentinel Nework Data Book 2017**. Washington, 2018. Disponível em: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf. Acesso em: 13 jan. 2020.

GOVERNO FEDERAL. Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Brasília, 11 dez. 2019. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 2 ago. 2021.

GRECO, Rogerio. **Código Penal Comentado**. 11. ed. Rio de Janeiro: Editora Impetus, 2017.

KLEINMAN, Zoe. **Who's That Girl: The Curious Case of Leah Palmer**. BBC News., 5 mar. 2015. Disponível em: https://www.bbc.com/news/technology-31710738. Acesso em: 13 jan. 2020.

MINISTÉRIO PÚBLICO FEDERAL. **MPF defende adesão do Brasil à Convenção de Budapeste em audiência pública na Câmara**. Brasília, 06 jun. 2019. Disponível em: http://www.mpf.mp. br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-de-budapeste-em-audiencia-publica-na-camara. Acesso em: 8 nov. 2019.

MINISTÉRIO PÚBLICO FEDERAL. **MPF pede celeridade ao Congresso na ratificação do Brasil como parte da Convenção de Budapeste**. Brasília, 04 ago. 2020. Disponível em: http://www.mpf.mp. br/pgr/noticias-pgr/mpf-pede-celeridade-ao-congresso-na-ratificacao-do-brasil-como-parte-da-convencao-de-budapeste. Acesso em: 2 ago. 2021.

MINISTÉRIO PÚBLICO FEDERAL. **Ofício nº 736/2020- SUPCAP/ SEJUD/PGR**. Brasília, 30 jun. 2020. Disponível em: http://www.mpf.mp. br/pgr/documentos/Oficio736DaviAlcolumbre.pdf. Acesso em: 2 ago. 2021.

NAÇÕES UNIDAS BRASIL. **Brasil é o quarto país com mais usuários de Internet do mundo, diz relatório da ONU**. Rio de Janeiro, 04 out. 2017. Disponível em: https://nacoesunidas.org/brasil-e-o-quarto-pais-com-mais-usuarios-de-internet-do-mundo-diz-relatorio-da-onu/. Acesso em: 8 nov. 2019.

NICAS, Jack. **Does Facebook Really Know How Many Fake Accounts It Has?** The New York Times, 30 jan. 2019. Disponível em: https://www.nytimes.com/2019/01/30/technology/facebook-fake-accounts.html. Acesso em: 7 nov. 2019.

NOBRE, Noeli. **CCJ Aprova Pena Maior Para Crime de Falsa Identidade Praticado Pela Internet**. Câmara dos Deputados, 04 nov. 2015. Disponível em: https://www.camara.leg.br/noticias/466024-ccj-aprova-pena-maior-para-crime-de-falsa-identidade-praticado-pela-internet/. Acesso em: 19 nov. 2019.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 18. ed. Rio de Janeiro: Editora Forense, 2018.

OKLAHOMA. House Bill 3024, de 01 de fevereiro de 2016. Disponível em: https://openstates.org/ok/bills/2015-2016/HB3024/. Acesso em: 16 jan. 2020.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5. ed. São Paulo: Saraiva, 2013.

QUEIROZ, Paulo. **Direito Penal: Parte Geral**. 13. ed. Salvador: Editora Juspodivm, 2018.

SCHULTZ, Alex. **How Does Facebook Measure Fake Accounts?** Facebook Newsroom, 23 mai. 2019. Disponível em: https://newsroom. fb.com/news/2019/05/fake-accounts/. Acesso em: 7 nov. 2019.

TEXAS. Código Penal do Texas, de 1856. Disponível em: https://statutes.capitol.texas.gov/?link=PE. Acesso em: 16 jan. 2020.

TEXAS. House Bill 2003, de 27 de fevereiro de 2009. Disponível em: https://capitol.texas.gov/billlookup/History.aspx?LegSess=81R&Bill=HB2003. Acesso em: 26 jan. 2020.

USA TODAY. **Manti Te'o's 'Catfish' story is a common one.** Virginia, 18 jan. 2013. Disponível em: https://www.usatoday.com/story/sports/ncaaf/2013/01/17/manti-teos-catfish-story-common/1566438/. Acesso em: 7 nov. 2019.

YOUNG, Mike. Online Harassment: New Texas Internet Law Goes Into Effect. Mike Young Law, 16 dez. 2009. Disponível em: https://mikeyounglaw.com/online-harassment-texas-internet-law/. Acesso em: 14 jan. 2020.