A ILEGALIDADE DA APLICAÇÃO DO PRINCÍPIO DA ANALOGIA NOS CRIMES VIRTUAIS

Marrison Luciano Silva*[1]

Rafaela Yumi Oliveira e Silva Aoyama**[2]

RESUMO

O presente trabalho tem por finalidade analisar se o uso da Lei Penal vigente para punir condutas ilícitas em ambiente cibernético fere ou não o princípio da legalidade. Entendemos que, com o expressivo avanço tecnológico na última década, os crimes cometidos na internet têm-se proliferado, gerando uma necessidade cada vez maior de discutir sobre o tema, uma vez que a legislação pátria ainda se mostra ineficiente no que tange aos delitos informáticos. Embora tenha havido esforço nos últimos anos, através da promulgação de leis, assinatura de tratados sobre o tema e criação de delegacias especializadas em apurar tais ilícitos, a norma penal brasileira não é ainda capaz de abarcar todas as modalidades de crimes cibernéticos e tutelar de forma adequada e coerente os recentes bens digitais. Esse estudo verificou que o nosso Código Penal não prevê sanção para quem comete crimes de dano ou apropriação indébita que atinjam os bens digitais mais recentes, como as cryptomoedas, por exemplo. Assim, a apuração, tipificação e punição de tais crimes permanecem uma incógnita no ordenamento jurídico pátrio, muitas das vezes, fica a cargo do aplicador legal a tarefa de buscar soluções na integração ou interpretação da norma. Diante disso, essa análise procurou demonstrar que recorrer aos mecanismos da interpretação extensiva e analogia para se moldar os cybercrimes aos delitos já tipificados no Código Penal não é a decisão mais correta, visto que a tentativa, nada mais é, do que tornar criminosa uma conduta que, embora notadamente ilícita, não possui lei anterior que a defina como crime. Isso significa ferir o princípio da legalidade e a vedação da analogia danosa ao réu em sede de Direito Penal, o que de longe não é a melhor saída para sanar a questão em debate, mas sim, a reformulação eficaz da Norma Penal Brasileira.

PALAVRAS-CHAVE: Direito Penal; Crimes Virtuais; Interpretação Extensiva Analógica; Analogia; Princípio da Legalidade.

* Graduando em Direito – Centro Universitário UNA – marrison.silva@hotmail.com

**Graduanda em Direito – Centro Universitário UNA – rafaelaaoyama@gmail.com

INTRODUÇÃO

Com o rápido avanço da internet e seu constante estágio de mutação e evolução, faz-se pertinente o questionamento se o Direito Penal, criado pelo Decreto-Lei nº 2.848, de 07 de dezembro de 1940, ainda que atualizado repetidas vezes, é suficiente para contemplar as novas modalidades de ilícitos informáticos, que crescem e se espalham na mesma velocidade dos veículos que os torna possíveis.

A norma criminal brasileira é incapaz de acompanhar as complexidades trazidas pelos crimes surgidos com o advento tecnológico, restando ao julgador recorrer aos métodos de interpretação e integração, quais sejam a interpretação extensiva e analogia. Bem sabemos que o instituto da analogia encontra algumas barreiras em sede de Direito Penal, mas sem dúvidas, que em face de tantas modalidades delituosas, é necessário adequar, à medida do possível, a legislação pátria existente, para que não se incorra em grave impunidade.

Alguns tipos penais facilitam o processo interpretativo, acatando, sem discussões, os novos cybercrimes. É o que acontece com o crime de furto, como podemos perceber na Lei nº 2.848 (BRASIL, 1940):

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.

No parágrafo terceiro da norma, temos que se equipara ao objeto tutelado (bem móvel) a energia elétrica, que é bem incorpóreo e intangível, equiparando-se a esta qualquer outra que tenha valor econômico, ou seja, a internet. Com isso em mente, fica autorizado o uso da interpretação extensiva para permitir que um perfil de rede social também seja objeto de furto, já que o mesmo é também um bem digital incorpóreo assim como a energia elétrica ou a internet.

A grande dificuldade surge quando o tipo penal não facilita essa interpretação. É sob a ótica desses casos específicos, que passaremos a analisar a utilização dos institutos da analogia e interpretação extensiva para conter no bojo da lei os delitos

cibernéticos, pois, nesses casos, haveria um conflito intransponível com o princípio constitucional da legalidade, não sendo essa, a solução mais adequada para mitigar o impasse legislativo originado pelos delitos informáticos.

A pesquisa demonstra relevância na medida em que procura comprovar a violação do princípio da legalidade na aplicação da analogia, e em alguns casos, da interpretação extensiva, nos crimes virtuais. O tema apresenta controvérsia doutrinária, uma vez que parte da doutrina entende ser possível utilizar as formas de interpretação da lei ao aplicar a Lei Penal nos crimes cibernéticos, enquanto outra vertente afirma que a aplicação da Lei Penal nos crimes virtuais é uma simples analogia *in malam partem*, visto que, não existe legislação específica que normatiza as condutas ilícitas no ciberespaço.

À vista disso, este artigo busca comprovar a ilegalidade da aplicação da analogia nos crimes cibernéticos, que é o que ocorre quando o aplicador legal se utiliza da interpretação extensiva em casos específicos que extrapolam o conceito trazido pela norma, gerando a problemática de, ao tentar punir o ciberdelito a todo custo, acaba legislando em malefício do réu.

A pesquisa terá caráter bibliográfico, já que se trata de um tema estritamente teórico. Foram consultadas as legislações penal, constitucional e civil brasileira, assim como a vasta biografia sobre o tema a partir de: artigos publicados em periódicos, matérias jornalísticas, doutrina nacional e estrangeira, entendimentos jurisprudenciais etc.

1 OS CRIMES DIGITAIS

O advento da tecnologia causou grandes impactos nas relações humanas, deixando-as mais dinâmicas, instantâneas e facilitando a vida do indivíduo. Entretanto, essa explosão tecnológica foi a responsável pelo surgimento de uma nova modalidade de atos ilícitos, os chamados "crimes digitais", que são aqueles cometidos dentro do ciberespaço, através de *gadgets*, redes de relacionamentos, aplicativos, sites, e-mails e afins.

Segundo os pesquisadores Damásio de Jesus e José Antônio Milagre, delitos informáticos são:

> o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo direito penal. (JESUS; MILAGRE, 2016. p. 9)

Esclarece-nos também o renomado doutrinador Rossini:

> O conceito de 'delito informático' poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade. (ROSSINI, 2004, p. 109)

O rápido avanço tecnológico, somado ao caos pandêmico enfrentado recentemente, contribuiu para o crescimento exponencial desses ataques cibernéticos no Brasil, chegando à marca de aproximadamente 2,6 bilhões no período de janeiro a junho de 2020, de acordo com a ferramenta que coleta e analisa incidentes de segurança cibernética em todo o mundo, Fortinet Threat Intelligence Insider Latin America.

Ao levarmos em consideração que a internet é um dos maiores expoentes da globalização, e que as interações realizadas em ambiente virtual podem, muitas das vezes, ser de caráter transnacional, entendemos a necessidade de se avaliar, com maior cautela, como se dará a punição dos cada vez menos raros, crimes cibernéticos. Nessa "aldeia global", onde bilhões de pessoas se conectam e transacionam a todo instante e não prevalece à soberania de Estado algum, a norma penal brasileira, que encontra suas barreiras territoriais, poderá muito facilmente estar aquém de tutelar sozinha toda a infinidade de novas possibilidades que surgem com o avanço da internet a cada dia.

Analisando a aplicação da Lei Penal às atividades ilícitas desenvolvidas no ciberespaço, é de se esperar que surjam questões de divergência em relação à aplicação da lei, uma vez que o Código Penal Brasileiro foi adotado em 1940 e é impossível que naquela época o legislador tivesse em mente crimes relacionados ao universo digital. Portanto, é razoável supor a impossibilidade da legislação penal pátria em abarcar a complexidade das interações online e a dificuldade de aplicar aos seus desdobramentos delituosos as leis penais vigentes.

Diante disso, é necessário também analisar a postura que cabe ao aplicador legal, que se vê obrigado a fugir de sua competência originária para legislar diante das situações dos crimes cometidos no âmbito informático, sob pena de macular o princípio da efetividade da jurisdição.

1.1 Os Crimes Digitais no Código Penal Brasileiro

Partindo do entendimento de que os crimes digitais constituem uma nova espécie de delitos, faz-se necessária a análise de seu cabimento perante o Direito Criminal brasileiro, em razão do consagrado princípio da estrita legalidade, aludido no artigo 5º, XXXIX da Magna Carta e repetido no artigo 1º do Código Penal. Tal princípio define que somente existe crime mediante uma lei anterior que o tipifique, clara e precisamente, como tal.

Com base nesse raciocínio, podemos inferir que alguns dos delitos cometidos em ambiente cibernético se adequam aos já tipificados, como é o caso dos crimes contra a honra, previstos nos artigos 138, 139 e 140 do Código Penal. Sobre estes, explica Guilherme de Souza Nucci:

> [...] o direito garante e protege a honra, visto que, sem ela, os homens estariam desguarnecidos de amor-próprio, tornando-se vítimas frágeis dos comportamentos desregrados e desonestos, passíveis de romper qualquer tipo de tranquilidade social. (NUCCI, 2017, p. 499).

Se uma pessoa sofre injúria, é caluniada ou difamada no meio virtual, a ação penal é cabível, uma vez que nenhum desses crimes necessita ser praticado de forma verbal, e pode muito bem o agente praticá-los através de troca de mensagens de texto, exposição em sites, redes sociais, blogs e conexos. Importante frisar que, nos moldes do art. 138, § 1º “Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga” (Brasil, 1940), aqueles que compartilharem e ajudarem a espalhar a falsa imputação, sabendo se tratar de uma inverdade, também respondem pelo ilícito.

Embora exista uma dificuldade em rastrear a origem da ofensa, e mais ainda daqueles que a propagam, os tribunais têm utilizado o disposto no art. 141, III do CP para enquadrar as ofensas cometidas no meio informático, uma vez que dispõe que

os crimes contra a honra cometidos na presença de várias pessoas, ou por meio que facilite sua divulgação, estarão sujeitos a um aumento da pena acima de um terço.

Na tentativa de facilitar a definição e consequente tipificação dos delitos virtuais, no ano de 2012 foi promulgada a Lei Nº 12.737, conhecida como Lei Carolina Dieckmann, visto sua participação na defesa da causa por haver passado por uma desagradável situação no ano anterior à promulgação da Lei, onde teve seu computador invadido por um criminoso virtual (cracker), que divulgou conteúdos de foro íntimo da atriz. Vejamos:

> Art.154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 2012)

A citada Lei altera o Código Penal, acrescentando, entre outros, o art. 154-A "invasão de dispositivo informático", tipificando a conduta popularmente conhecida como "*hackear*", que significa burlar os meios de segurança presentes em dispositivos, sites, aplicativos etc. para ter acesso à conta, dados e informações pessoais de outrem. Segundo o próprio artigo, o dolo consiste em praticar a conduta com o fim de "adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

Embora se tenha estabelecido os contornos do que seriam as condutas típicas dos neonatos crimes cibernéticos, apenas o artigo supracitado é incapaz de abarcar toda a variedade e complexidade dos delitos virtuais, ainda mais quando levamos em consideração que a rápida inovação é um dos maiores atributos da teia informática, surgindo diariamente novas maneiras e oportunidades de se obter vantagens ilícitas através dos meios digitais, e tornando ainda mais difícil o rastreio e enquadramento de tais ações delituosas.

1.2 Impossibilidade do Crime de Dano e Apropriação Indébita para a Tutela dos Bens Digitais

Para além dos delitos cibernéticos supracitados, em que parece não haver discordância entre as correntes doutrinárias quanto sua adequação aos tipos penais já existentes na legislação pátria, cabe agora analisar aqueles em que há, não apenas divergências quanto à tipificação, mas também questionamentos quanto à constitucionalidade de sua utilização pautada em interpretação analógica e extensiva.

A grande dificuldade em enquadrar os crimes de natureza cibernética nesses tipos penais deve-se principalmente ao fato de que o objeto da proteção jurídica se constitui em bens móveis e imóveis, em contrapartida, os recém-chegados, bens digitais, são aviltados nos delitos informáticos. Na lição do professor Bruno Zampier sobre bens digitais:

> Seriam bens incorpóreos, os quais são progressivamente inseridos na internet por um usuário, consistindo em informações de caráter pessoal que trazem alguma utilidade àquele, tenha ou não conteúdo econômico. Não há, até o presente momento, qualquer conceito legal no Brasil em relação a estes bens. (ZAMPIER, 2021, pp. 63-64)

Assim, podemos definir na categoria de bens digitais as contas e perfis em sites de relacionamento como *Instagram* e *Facebook*, o conteúdo em vídeo postado em sites como *YouTube*, os *blogs*, milhas aéreas, pontos de cartão de crédito e as criptomoedas.

Partindo dessa breve definição, comecemos pela análise do crime de dano, previsto no art. 163 do CP, *in verbis* "Destruir, inutilizar ou deteriorar coisa alheia". No entendimento de Túlio Lima Vianna:

> o crime de dano previsto no art. 163 do Código Penal Brasileiro é perfeitamente aplicável à tutela dos dados informáticos, sendo completamente prescindível a criação de um novo tipo penal para tal fim. Trata-se de interpretação extensiva da palavra "coisa", elemento objetivo do tipo penal. (VIANA, 2003, p. 492).

Ora, mais adiante cumpriremos esclarecer o significado do conceito de interpretação extensiva, mas por enquanto, é urgente analisar o porquê de não estarmos de acordo com a interpretação do renomado jurista. Não podemos, de forma alguma, supor que o legislador tivesse pensado em tutelar um "bem digital", portanto, incorpóreo, quando utilizou-se do substantivo "coisa" como objeto do tipo penal sob análise. Como simplificadamente leciona Fernando Capez a respeito do crime de dano: "O artigo em tela, entretanto, cuida propriamente do dano físico, ou seja, daquele que recai diretamente sobre a coisa, causando nestas modificações de ordem material." (CAPEZ, 2012, p. 531)

Trata-se de crime patrimonial, cujo objeto jurídico a ser tutelado é a posse e propriedade de coisas móveis e imóveis, não se incluindo bens de natureza virtual. Entendemos, portanto, ser forçosa a utilização de interpretação extensiva, sob risco de se incorrer em grave atentado ao princípio da reserva legal. Por mais que seja possível "destruir", digitalmente falando, 30 mil milhas do cartão de crédito, ou uma conta no *Instagram*, isso não configura crime de dano. À vítima, resta recorrer à indenização civil pelo prejuízo sofrido, mas a julgar pelo ocorrido, o dolo do agente e à importância social que possuem esses bens digitais hoje, fica inegável que a questão também mereça a tutela do Direito Penal.

Similar raciocínio podemos aplicar ao delito previsto no art. 168 do Código Penal, *in verbis* "Apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção", onde o objeto se trata especificamente de coisa (material) móvel. Aqui também, pelos mesmos motivos acima citados, concluímos impossível supor que o legislador entenderia por "coisa móvel" uma criptomoeda, um vídeo hospedado em uma plataforma de vendas etc.

O canal do famoso y*outuber* brasileiro, Whinderson Nunes, fatura milhões de reais pela quantidade de acessos no site, assim como suas contas nas redes sociais,

que seguramente são administradas por uma equipe com a incumbência de geri-las. Se por acaso, um dos membros dessa equipe passa a utilizar a conta para obter vantagens pessoais, agindo como se dono fosse, não podemos estender a esse caso a tutela sobre o delito de apropriação indébita, mas talvez, e a depender das circunstâncias, furto.

Analisando bens digitais como as criptomoedas, as milhas de cartão de crédito, os canais no *YouTube*, os perfis em redes sociais que são monetizados, estamos claramente diante de bens de relevância sociocultural que carecem ser amparados, protegidos pela norma penal brasileira, mas cujo resguardo é ainda bastante limitado, uma vez que o ataque direto a tais bens não encontra respaldo adequado no Código Penal. Ora, por que não se utilizar dos tipos já existentes para referenciar os novos cibercrimes? Por causa da enorme diferença existente entre interpretação extensiva e de analogia, e a vedação desta em sede de direito criminal. É sob essa ótica que passaremos a analisar a perspectiva dos delitos informáticos no Brasil hoje.

2 INSTITUTOS DA ANALOGIA E INTERPRETAÇÃO EXTENSIVA

Primeiramente, cumpre destacar a importância da interpretação da Lei Penal, que visa sempre à busca pela vontade da Lei, e não a vontade do legislador. Como esclarece Dirley da Cunha Junior (2008), interpretação é:

> A atividade prática de revelar/atribuir o sentido e o alcance das disposições normativas, com finalidade de aplicá-las a situações concretas, pois interpretar é determinar o conteúdo e significado dos textos visando solucionar o caso concreto. Não se interpreta em vão, ou por diletantismo, mas para resolver os problemas jurídicos concretos. (CUNHA JUNIOR, 2008, p. 186).

Dessa forma, entendemos que a intenção do aplicador legal deve seguir sempre no sentido de solucionar o problema de cada caso concreto, mas quando estamos diante de crimes na esfera virtual, surge à necessidade de tutelar o direito lesado ante a inexistência de uma lei penal que especifique os delitos dessa espécie. Daí nascem as interpretações dos tipos penais para que sejam moldados aos

cibercrimes, o que acaba por gerar um problema de outra natureza, qual seja, constitucional.

Diante disso, na tentativa de buscarmos solução para o problema exposto, é substancial analisar a diferença entre a forma de interpretação extensiva e o instituto da analogia no direito penal brasileiro.

Em relação ao instituto da interpretação extensiva, vejamos o que diz o jurista Paulo Nader:

> Na interpretação extensiva o caso é previsto pela lei diretamente, apenas com insuficiência verbal, já que a mens legis revela um alcance maior para o enunciado. A má redação do texto é uma das causas que podem levar à não correspondência entre as palavras da lei e o seu espírito. Nesse caso não se pode falar em lacuna. Existe apenas uma impropriedade de linguagem. (NADER, 2014, p. 193).

A respeito do tema, existe uma grande discussão doutrinária quanto sua aplicação em sede de Direito Penal, uma vez que se não lhe forem definidos os contornos, ela se transforma em analogia (sabidamente vedada), e é a posição que defendemos em relação ao que acontece quanto aos crimes digitais. Para tornar mais claro esse pensamento, vejamos o que aludem Francisco Muñoz Conde e Mercedes García Arán:

> Se entendido por interpretação extensiva, o que inclui no termo legal o número máximo de significados permitidos pelo seu significado literal, mas sem excedê-lo, pode ser considerado respeitoso do princípio da legalidade e muito aceitável. Por outro lado, se a interpretação ampliar o significado da norma além dos possíveis significados do termo legal, está permitindo a sua aplicação a suposições não contidas no preceito e, portanto, incorrendo em analogia proibida. (CONDE; ARÁN, 2010, p. 127):

Aqui, faz-se necessário esclarecer que o grande risco no uso de tal método interpretativo é “forçar” de tal maneira o significado do texto normativo a ponto de se ferir o princípio da legalidade, acrescentando ao fato típico elementos que não podem ser oriundos de sua essência, praticando-se a analogia *in malam partem.* É o que ocorre, a nosso ver, quando se tenta imputar crime de dano a quem “deteriorou” duzentos *Bitcoins*. Dito isso, esclarecemos que não enxergamos problema no uso da interpretação extensiva no bojo do Direito Penal, apenas coadunamos com a doutrina majoritária que defende seu uso restrito a casos bastante pontuais, o que, a nosso ver, exclui os delitos informáticos, uma vez que sua correspondência ao Código Penal

significa sempre a tentativa de imputar a alguém um fato que por si só não está tipificado.

Para elucidar melhor esse posicionamento, o professor Guilherme de Souza Nucci nos fornece um bom exemplo em que a interpretação extensiva é utilizada em benefício do réu:

> No caso do art. 176 [outras fraudes], pune-se a conduta de quem 'tomar refeição em restaurante […] sem dispor de recursos para efetuar o pagamento', ampliando-se o conteúdo do termo 'restaurante' para abranger, também, boates, bares, pensões, entre outros estabelecimentos similares. Evita-se, com isso, que o sujeito faça uma refeição em uma pensão, sem dispor de recursos para pagar, sendo punido por estelionato, cuja pena é mais elevada. (NUCCI, 2014, p. 35)

Caminhando agora para o entendimento do conceito de analogia, é importante destacar que ela não se confunde como forma de interpretação da norma, ocorrendo apenas uma mera integração desta. Na visão de Paulo Nader, ela é um recurso que permite aplicar uma norma legal a um caso não previsto por essa lei, contemplando, assim, um número maior de situações cotidianas sem a necessidade de se pormenorizar a legislação:

> A aplicação da analogia legal decorre necessariamente da existência de lacunas da lei. É uma técnica a ser empregada somente quando a ordem jurídica não oferece uma regra específica para determinada matéria de fato. Normalmente essas lacunas surgem em razão do desencontro cronológico entre o avanço social e a correspondente criação de novas regras disciplinadoras. [...] Outras vezes, aparecem em virtude do excesso de abstratividade da norma jurídica que, pretendendo alcançar elevado número de casos, deixa de contemplar diversas situações que, não se acomodando nos esquemas legais, passam a reclamar autonomia e tratamento próprio. (NADER, 2014, p. 191).

Importante também salientar que os conceitos de analogia e interpretação analógica não se confundem. Esta é uma das formas de interpretação da lei, aquela, não. Embora sejam conceitos distintos, a interpretação analógica recebe da doutrina o mesmo tratamento do instituto da analogia, como bem esclarece Rogério Greco:

> Em matéria penal, por força do princípio da reserva, não é permitido, por semelhança, tipificar fatos que se localizam fora do raio de incidência da norma, elevando-os à categoria de delitos. No que tange às normas incriminadoras, as lacunas, porventura existentes, devem ser consideradas como expressões da vontade negativa da lei. E, por isso, incabível se torna o processo da interpretação analógica. Nestas hipóteses, portanto, não se

> promove a integração da norma (analogia) ao caso por ela não abrangido. (GRECO, 2004, p. 92)

O entendimento pacificado pela doutrina é de que a analogia constitui aberração quando se posiciona em malefício do réu (analogia *in malam partem*), seguindo a lição do professor Guilherme Nucci:

> Entretanto, se noutros campos do Direito a analogia é perfeitamente aplicável, no cenário do Direito Penal ela precisa ser cuidadosamente avaliada, sob pena de ferir o princípio constitucional da legalidade (não há crime sem lei que o defina; não há pena sem lei que a comine). Assim sendo, não se admite a analogia in malam partem, isto é, para prejudicar o réu (NUCCI, 2019, p. 77).

Desta forma, não há que se cogitar o uso da analogia para aplicação da norma penal nos delitos cibernéticos.

2.1 A Impossibilidade da Aplicação da Interpretação Extensiva e da Analogia nos Crimes Digitais

Na lição de Tércio Sampaio Ferraz Junior (2018) a diferenciação entre interpretação extensiva e analogia se faz bastante lógica:

> O cuidado especial com a interpretação extensiva provoca uma distinção entre esta e a interpretação por analogia. A doutrina afirma que a primeira se limita a incluir no conteúdo da norma um sentido que já estava lá, apenas não havia sido explicitado pelo legislador. Já na segunda, o intérprete toma de uma norma e aplica-a um caso para o qual não havia preceito nenhum, pressupondo uma semelhança entre os casos. Por exemplo, se a norma pune o lenocínio, o intérprete dirá que sob a rubrica deste símbolo está também a exploração de motéis em que se tolera a presença de casais, dos quais não se pergunta se são ou não casados ou se estão lá apenas por motivos libidinosos. (FERRAZ JUNIOR, 2018, p. 323)

Contrapondo os dois conceitos, temos que a interpretação extensiva pressupõe a existência de uma lei, que por um defeito textual não abarcaria o caso concreto. Em contrapartida, a analogia depende da inexistência total da lei, existindo uma ausência da norma, utilizando-se então o paradigma de um caso semelhante para solucionar o problema.

Ora, superficialmente pensamos que a melhor solução seria a aplicação da analogia nos crimes virtuais, visto que bastaria ao aplicador legal observar as semelhanças entre o que a lei tipifica com as nuances do delito cibernético - se os pontos do cartão foram “destruídos”, se a conta do *Instagram* foi “furtada” por um dos co-produtores etc. A grande questão é que já sabemos ser vedado o uso da analogia para efeito de enquadramento em figuras delituosas, em penas ou como fator de agravamento destas, e por isso, usa-se o argumento de ser a interpretação extensiva a saída para resolver a questão dos crimes digitais face ao direito criminal pátrio.

Restou comprovado que a interpretação extensiva, quando extrapola os limites do que está determinado na norma com o intuito de enquadrar uma conduta a uma lei penal preexistente, viola o princípio da legalidade, se tornando uma espécie de analogia em malefício ao réu. Além do mais, quando se trata dos delitos informáticos comparados a certos tipos penais, como o crime de dano e apropriação indébita que citamos, se torna incabível estender aos objetos jurídicos tutelados os novos bens digitais, como milhas e pontos de cartão de crédito, perfis monetizados no *Instagram* e *Facebook*, canais milionários no *YouTube*, criptomoedas e afins.

De acordo com Nunes (2015, p. 18) “o fato é que a legislação pertinente não acompanhou de forma proporcional a evolução na forma de cometimento dos crimes, deixando assim as chamadas “brechas” na lei que favorecem o infrator”. De fato, não se pode desejar que quem cometa crimes através do meio informático permaneça impune, mas também não se deve admitir nem que a interpretação da norma ultrapasse seu sentido e fira princípios constitucionais e nem que a norma penal permaneça inerte. Desta feita, acreditamos ser a reformulação do sistema normativo criminal a chave para solucionar os empasses identificados ao longo desta análise, e não compactuamos com o uso da interpretação extensiva para abarcar os novos delitos digitais no seio do nosso Direito Penal.

CONCLUSÃO

Em face de todo o exposto, concluímos que, embora aparente ser cabível o uso da interpretação extensiva (uma vez vedada à analogia maléfica) em Direito Penal

para punir os crimes virtuais, corre-se um sério risco de interpretar a norma para além do que ela pretende abarcar, transformando-se assim o modo interpretativo em analogia para prejuízo do réu, como ocorre nos crimes de dano e apropriação indébita, que analisamos.

Ora, nessa circunstância, a interpretação extensiva deverá ser considerada tão danosa quanto o é a analogia *in malam partem*, não devendo ser utilizada para forçar uma adequação da lei ao ilícito informático praticado.

Cumpre salientar que entendemos a importância de se resguardar criminalmente os bens digitais, uma vez que se constituem em bens de cunho patrimonial, inclusive, e de enorme relevância sociocultural, merecendo toda guarnição advinda da Lei. Não defendemos a posição de que deva permanecer impune quem danifica, obstrui, se apropria de perfis em sites de relacionamentos, infoprodutos, conteúdo digital e *Bitcoins*. Pelo contrário, concluímos ser de suma importância a garantia desses bens para a sociedade contemporânea, que faz-se urgente a reformulação da Lei Penal, para que possa de maneira adequada e eficaz punir os cibercriminosos, e preservar o direito informático.

THE ILLEGALITY OF THE APPLICATION OF THE ANALOGY PRINCIPLE IN VIRTUAL CRIMES

ABSTRACT

The purpose of this paper is to analyze whether or not the use of the current Criminal Law to punish illegal conduct in a cyber environment violates the principle of legality. With the expressive technological advance in the last decade, crimes committed on the internet have proliferated, generating an ever greater need to shed light on the topic, since the domestic legislation is still inefficient with regard to computer-related crimes. Although efforts have been made in recent years, through the enactment of laws, the signing of treaties on the subject and the creation of police stations specialized in investigating such crimes, the Brazilian criminal law is not yet able to cover all types of cyber crimes and to protect them in a recent digital goods. As verified in the study, our Penal Code does not provide for sanctions for those who commit crimes of misappropriation or damage that affect the most recent digital assets, such as cryptocurrencies, for example. Thus, the investigation, classification and punishment of such crimes remains unknown in the national legal system, and the legal enforcer is often in charge of seeking solutions in the integration or interpretation of the rule. In view of this, the analysis seeks to demonstrate that resorting to the mechanisms of extensive interpretation and analogy to shape cybercrimes to crimes already typified in the Penal Code is not a more correct decision, since the attempt is nothing more than making a conduct criminal, which, although notably illicit, it does not have a previous law that defines it as a crime. This means hurting the principle of legality and prohibiting the harmful analogy to the defendant in the context of Criminal Law, which by far is not the best way to resolve the issue under discussion, but rather the effective reformulation of the Brazilian Penal Rule.

Key words: Criminal Law; Virtual Crimes; Analog Extensive Interpretation; Analogy; Principle of Legality.

REFERÊNCIAS

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro 1940. Código Penal Brasileiro. **Portal da Legislação do Governo Federal**. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 13 Mar. 2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Portal da Legislação do Governo Federal**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 27 Mar. 2021.

CAPEZ, **Curso de Direito Penal: parte geral.** 15. ed. São Paulo: Saraiva, 2012.

CONDE, Francisco Muñoz; ARÁN, Mercedes García. **Derecho penal**: parte general. 8. ed. Valencia: Tirant lo Blanch, 2010.

CUNHA JÚNIOR, Dirley da. **Curso de direito constitucional**. Salvador: Juspodivm, 2008.

FERRAZ JUNIOR, Tercio Sampaio. **Introdução ao estudo do direito**. 10. ed. São Paulo: Atlas, 2018.

GRECO, Rogério. **Curso de direito penal** – Parte Geral. 4. ed. Rio de Janeiro: Impetus, 2004.

JESUS, Damásio de. MILAGRE, Celso Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

NADER, Paulo. **Introdução ao estudo do direito.** 36. ed. Rio de Janeiro: Forense, 2014.

NUCCI, Guilherme de Souza. **Código penal comentado**. 14. ed. Rio de Janeiro: Forense, 2014.

NUNES, Massio Barbosa. **Crimes Virtuais: uma análise acerca de alguns de seus aspectos.** Fortaleza, Faculdade Cearense, 2015.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

VIANNA, Túlio Lima. Do delito de dano e de sua aplicação ao Direito Penal Informático. **Revista dos Tribunais**. São Paulo, ano 92, n. 807, p. 486-492, jan 2003.

ZAMPIER, Bruno. **Bens digitais**. 2. ed. Indaiatuba: Foco, 2021.