CRIMES CIBERNÉTICOS: ATIPICIDADE DOS DELITOS

Keniche Guimarães Matsuyama[1]
João Ademar de Andrade Lima[2]

RESUMO: O presente texto visa a discorrer sobre o instituto do crimes cibernéticos, analisando-os enquanto tipificação para novos comportamentos e a utilização da analogia em dadas situações. Parte-se do conceito hodiernamente adotado para crime cibernético, explicitando suas principais classificações. Ademais, explora a importância do princípio da legalidade para o Direito Penal, correlacionando sua base principiológica à temática dos crimes cometidos em ambiente cibernético.

Por fim, diante do pensamento doutrinário majoritário a respeito da vedação do emprego da analogia *in malam partem* no Direito Penal, aponta para a não criminalização de certas condutas, mediante o emprego do recurso da integração.

Palavras-chave: Crimes Cibernéticos; Atipicidade; Analogia.

1. INTRODUÇÃO

Longe de esgotar a discussão acerca do tema em análise, busca-se com este esboço tecer breves comentários sobre o surgimento de novas condutas criminosas, ora conceituadas de crimes cibernéticos, diante da maciça utilização da informática no dia-a-dia da sociedade moderna, abordando-se a problemática da aplicação do Código Penal para tais novas infrações, analisando-se a tipificação desses comportamentos e a utilização da analogia em dadas situações.

Inicialmente articula-se de forma pragmática o conceito hodiernamente adotado para crime cibernético, explicitando suas principais classificações.

Em seguida, explora-se a importância do princípio da legalidade para o Direito Penal, correlacionando tal princípio com a temática dos crimes cibernéticos, de que trata este estudo acadêmico.

[1] Bacharelando em Direito (7º período) na UNIFACISA.
[2] Orientador. Professor de Direito Digital na UNIFACISA.

Por fim, diante do pensamento doutrinário majoritário a respeito da vedação do emprego da analogia *in malam partem* no Direito Penal, aponta-se para a não criminalização dos, *stricto sensu*, crimes cibernéticos, mediante o emprego de tal recurso de integração.

2. CONCEITO DE CRIME CIBERNÉTICO

Inicialmente, faz-se necessário esclarecer que, doutrinariamente, não há consenso sobre a terminologia adequada para se conceituar crime cibernético, vislumbrando-se o emprego de diversos termos para caracterizá-lo como: crimes digitais, crimes eletrônicos, crimes informáticos, e-crimes, crimes virtuais, dentre outros.

Nessa perspectiva, assevera Patrícia Santos da Silva:

> [...]que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (DA SILVA, 2015, p.39).

Para efeito desse estudo, adotaremos o conceito de crime cibernético, por entender-se como termo suficientemente abrangente, abarcando diversas condutas delitivas que se utilizam ou que se voltam contra dispositivos e recursos computacionais.

De maneira objetiva, pode-se conceituar crimes cibernéticos como sendo condutas ilegais que se efetivam mediante a utilização de dispositivos informáticos, conectados ou não a rede mundial de computadores, bem como as ações criminosas contra equipamentos tecnológicos, sistemas de informação ou banco de dados. Nesse sentido assevera Aldemario Araujo Castro:

> [...] são denominados de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados). (CASTRO, 2003, p.1).

Em suma, qualquer ação ilegal, que utiliza-se de recursos tecnológicos como meio para a prática delituosa ou voltada contra computadores, sistemas e dados não autorizados, pode ser caracterizado como crime cibernético.

3. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Com fins didáticos, os doutrinadores acabam sistematizando o conhecimento, adotando classificações para determinados temas. Nesse sentido, os estudiosos propõem diversas classificações normativas para as condutas delitivas ora denominadas de crimes cibernéticos.

Dentre as variadas classificações adotadas na literatura para esses crimes, destacam-se duas. Uma que faz referência a crimes cibernéticos puros, mistos e comuns. E uma outra que classifica tais infrações como próprios e impróprios.

3.1 CRIMES CIBERNÉTICOS PUROS, MISTOS E COMUNS

O crime cibernético puro está relacionado a comportamentos ilícitos que objetivam especificamente a atacar sistema computacional e seus componentes, seja o *hardware*[3] ou o *software*[4], abarcando ainda os dados e os sistemas em si. Nessa modalidade, a investida do agente tem por objetivo atingir o equipamento físico, o sistema informático e as informações dos bancos de dados. Nessa modalidade, exemplificativamente, temos a invasão de servidores e *sites*.

Já o crime cibernético misto, a ação criminosa está essencialmente condicionada ao uso da Internet para que o intento delituoso possa se efetivar, conquanto o infrator vise bem jurídico distinto do informático. O agente não dirige sua conduta ao sistema computacional ou a seus componentes, mas o uso da tecnologia é ferramenta primordial para a concretude da ação delinquente. Como exemplo, cita-se a retirada ilícita de valores monetários de contas bancárias via *homebanking*.

Por último tem-se a conduta do agente que se vale da rede mundial de computadores tão somente como instrumento para efetivação de um crime já devidamente tipificado no Código Penal, caracterizando a modalidade de crime cibernético comum. Os crimes contra a

[3] Palavra usada para definir a parte física de um equipamento. Além do computador formado por placas, discos e microprocessadores, incluem-se nesta definição as impressoras, os monitores de vídeo, os scanners, o mouse, entre outros. É a parte de um sistema de computador que pode ser vista ou tocada. (SILVA JÚNIOR, 2009, p.23).

[4] Programas que dão função aos computadores. Os programas são escritos em linguagem de programação e comandam todo o funcionamento do computador. Software é a parte lógica do computador, que nos permite administrar, operar, manter e usar o equipamento. (SILVA JÚNIOR, 2009, p.23).

honra que no passado se materializavam-se por outros meios, hoje pode se concretizar através da utilização da Internet, sobretudo por meio das redes sociais.

3.2 CRIMES CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS

Segundo preleciona Anderson Soares Furtado Oliveira, crime cibernético próprio é aquele que:

> [...] só pode ser cometido no ciberespaço, ou seja, necessariamente, deve ser realizado no ambiente do ciberespaço, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional. Ademais, tanto a ação quanto o resultado da conduta ilícita consumam-se no ciberespaço. (OLIVEIRA, 2009, p.33).

Acredita-se que o cerne da discussão sobre a aplicação da norma penal aos crimes cibernéticos está mais fortemente relacionado aos crimes cibernéticos próprios.

Essas condutas, ora intituladas como crimes cibernéticos próprios, caracterizam-se pela sua autonomia e distinção das infrações positivadas no Código Penal. Daí a dificuldade, ou até mesmo, a impossibilidade de se criminalizar tais ações, por falta de tipificação legal, uma vez que o ordenamento penal brasileiro pauta-se pela estrita legalidade, não punindo infrações não previstas em lei.

No que diz respeito aos crimes cibernéticos impróprios, assevera Aires José Rover:

> São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta para a perpetração de crime comum, tipificável na lei penal. Dessa forma, o sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. (ROVER, 2009, p.3).

Tratando-se dos crimes cibernéticos impróprios, considera-se possível a aplicação da norma penal para essas condutas, onde o agente se vale de recursos informáticos como mero instrumento para a prática de delitos já tipificados no Código Penal.

Ressalta-se, porém, que essa aplicação não se dá de forma sumária, devendo a conduta se amoldar à descrição do tipo penal, analisando-se o caso concreto, a fim de que não se incorra no emprego da analogia *in malam partem*, instituto rechaçado pelas disposições penais pátria.

4. PRINCÍPIO DA LEGALIDADE

O princípio da legalidade é, sem dúvida, um dos mais importantes para o Direito Penal. Serve como alicerce, como base de sustentação para a aplicação concreta da lei penal. Está positivado no art. 5º, inciso XXXIX da Constituição Federal, que diz: Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Similarmente está expresso no art. 1º do Código Penal, sem substancial diferenciação com relação ao disposto na Carta Magna. Nessa esteira preleciona Rogério Greco:

> É o princípio da legalidade, sem dúvida alguma, o mais importante do Direito Penal. Conforme se extrai do art. 1º do Código Penal, bem como do inciso XXXIX do art. 5º da Constituição Federal, não se fala na existência de crime se não houver uma lei definindo-o como tal. A lei é a única fonte do Direito Penal quando se quer proibir ou impor condutas sob a ameaça de sanção. Tudo o que não for expressamente proibido é lícito em Direito Penal. (GRECO, 2015, p.144).

No ordenamento jurídico brasileiro, não se concebe que um fato seja considerado como crime sem que exista lei anterior que descreva tal conduta como delituosa.

A lei, em sentido estrito, é a única fonte capaz de proibir ou impor comportamentos sob a ameaça de cominar sanções, constituindo uma verdadeira limitação ao poder do Estado de interferir na esfera de liberdades dos indivíduos. Nesse sentido assevera Cleber Masson sobre o princípio da legalidade:

> Preceitua, basicamente, a exclusividade da lei para a criação de delitos (e contravenções penais) e cominação de penas, possuindo indiscutível dimensão democrática, pois revela a aceitação pelo povo, representado pelo Congresso Nacional, da opção legislativa no âmbito criminal. De fato, não há crime sem lei que o defina, nem pena sem cominação legal (nullum crimen nulla poena sine lege). (MASSON, 2015, p.82).

O epicentro da discussão sobre os crimes cibernéticos está assentado nesse princípio basilar do Direito Penal (princípio da legalidade). Como punir possíveis infratores desses crimes diante da ausência de lei descrevendo tal conduta como criminosa? O Estado-Juiz pode aplicar sanções para comportamentos não tipificados em lei? É nesse diapasão que se discute a atipicidade dessas condutas e a consequente isenção de punição desses indivíduos.

Nesse contexto normativo, o *jus puniendi* do Estado está vinculado ao que preceitua a lei, não podendo aplicar sanções ao arrepio de sua vontade, sendo imprescindível que haja expressamente previsão normativa para tal.

5. ANALOGIA *IN MALAM PARTEM*

O instituto da analogia, caracteriza-se pela integração do ordenamento jurídico com a intenção de suprir lacunas na lei. Fundamenta-se no brocardo *ubi eadem ratio, ibi eadem jus*, ou seja, onde há a mesma razão, aplica-se o mesmo dispositivo de lei.

Nas precisas lições de Rogério Sanches Cunha:

> [...] a analogia consiste no complexo de meios dos quais se vale o intérprete para suprir a lacuna (o vazio) do direito positivo e integrá-lo com elementos buscados no próprio direito. Nesta ótica, seu fundamento é sempre a inexistência de uma disposição precisa de lei que alcance o caso concreto. (CUNHA, 2015, p.64).

Como uma das espécies do mecanismo integrativo supracitado, tem-se a analogia *in malam partem*, que "é aquela pela qual aplica-se ao caso omisso uma lei maléfica ao réu, disciplinadora de caso semelhante." (MASSON, 2015, p.181).

A crítica mais incisiva a punição aos ditos crimes cibernéticos, está alicerçada na impossibilidade de se utilizar no Direito Penal da analogia para prejudicar o réu. A doutrina é quase que uníssona no que diz respeito a proibição do operador do Direito se valer da analogia *in malam partem*.

Sobre essa questão, assevera Guilherme de Souza Nucci:

> [...] 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). Nesse caso, não se admite a analogia *in malam partem*, isto é, para prejudicar o réu. (NUCCI, 2014, p.36).

Nesse mesmo sentido preleciona, novamente, Cleber Masson:

> Não se pode pretender a aplicação da analogia para abarcar hipótese não mencionada no dispositivo legal (analogia in malam partem). Deve-se adotar o fundamento constitucional do princípio da estrita legalidade na esfera penal. (MASSON, 2015, p.181).

Corroborando o pensamento dos doutrinadores acima citados, afirma Rogério Sanches Cunha:

> Em síntese, com espeque no princípio da legalidade, o emprego da analogia no Direito Penal somente é permitido a favor do réu, jamais em seu prejuízo, seja criando tipos incriminadores, seja agravando as penas dos que já existem. (CUNHA, 2015, p.64).

Nesse contexto, vislumbra-se o impedimento da aplicação do Código Penal a determinadas condutas especificadas como crimes cibernéticos, sobretudo os denominados próprios, por falta de tipificação legal e pela impraticabilidade do intérprete se valer da analogia *in malam partem* na aplicação do Direito Penal.

6. CRIMES CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS TIPIFICADOS

Trazendo-se uma amostra de alguns crimes cibernéticos que se amoldam às tipificações do Código Penal, pode-se citar o crime de homicídio elencado no artigo 121. Tal infração é passível de ser praticada mediante a utilização de um sistema informático pelo agente. Nesse caso o infrator emprega tal recurso computacional como mera ferramenta para consumar o delito, caracterizando-se um crime cibernético impróprio.

Exemplificando o cometimento de um crime cibernético impróprio no delito de homicídio, aduz Andréa de Fátima Araújo Cavalcante: "Seria o caso em que um *cracker*[5] invade a rede de computadores de um hospital e muda as prescrições médicas relativas a um determinado paciente, substituindo os remédios ou alterando as dosagens, com o *animus necandi*." (CAVALCANTE, 2011, p. 55).

Outra modalidade de delito tipificado no código incriminador que se adequa aos chamados crimes cibernéticos impróprios, diz respeito aos crimes que tem por objetivo tutelar o bem jurídico honra. Calúnia, difamação e injúria, crimes contra a honra elencados respectivamente nos artigos 138, 139 e 140 do Código Penal, são infrações que ganharam maior amplitude, através da utilização de ferramentas informáticas como as mídias sociais, blogs, sites, aplicativos de comunicação, dentre outros, que facilitam e dinamizam o cometimento desses ilícitos.

Com relação aos crimes cibernéticos próprios, aqueles que necessariamente precisam ser cometidos no ambiente do ciberespaço, destaca-se o artigo 313 A e 313 B, incluídos no Código Penal pela Lei nº 9.983/03:

---

[5] [...]termo utilizado para identificar aqueles indivíduos que também possuem um conhecimento elevado relacionado à tecnologia, mas que não a utilizam de maneira positiva, são os que invadem sistemas e promovem ações com a intenção de prejudicar os outros, como desfigurar páginas da Internet ou promover a invasão de PCs (Computadores Pessoais) de usuários leigos.

> Inserção de dados falsos em sistema de informações
>
> Art. 313A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
>
> Modificação ou alteração não autorizada de sistema de informações
>
> Art. 313B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.

Os dois artigos supracitados correspondem a uma nova tendência do ordenamento jurídico brasileiro, no sentido de abarcar condutas praticadas no ambiente virtual, socialmente reprováveis, merecedoras do *jus puniendi* Estatal, que ainda não estejam descritas no Código Penal.

Recentemente, nova legislação com o intuito de punir especificamente crimes cibernéticos, foi inserida no ordenamento jurídico pátrio.

Trata-se da Lei 12.737/2012, que dispõe sobre a tipificação criminal de delitos informáticos, regramento este que ficou conhecido como “Lei Carolina Dieckmann”, atriz da Rede Globo de Televisão. A artista teve seu computador de uso privado invadido, o que acabou ocasionando a divulgação indevida de suas fotos íntimas na internet.

Este episódio com a atriz Global, foi o fato catalizador para a rápida ação legislativa, que culminou com a referida lei, inovando a legislação penal brasileira com modernas disposições acerca de condutas ilícitas de invasão a meios informáticos.

A lei de delitos informáticos, acrescentou os artigos 154-A e 154-B no Código Penal. Importante se faz a transcrição literal da *novatio legis* incriminadora:

> Invasão de dispositivo informático
>
> 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.
>
> Ação penal
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou

> indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

A mencionada lei também realizou alterações nos artigos 266 e 298, ambos do mesmo diploma penalista, punindo como crimes cibernéticos as condutas de tais dispositivos.

Com constantes inovações tecnológicas e atividades cotidianas cada vez mais atreladas à dispositivos informáticos, não pode o direito ficar aquém dessas transformações sociais, sobretudo quando tais avanços acarretam o surgimento de novos ilícitos. Diante disso, é louvável a atividade legislativa voltava à punir comportamentos lesivos à sociedade moderna, como é o caso da Lei 12.737/2012.

7. CONSIDERAÇÕES FINAIS

A contemporaneidade que engendra o mundo cibernético é, já ponderada por diversos autores, em distintos arrazoados filosóficos ou especulativos, a materialização de um mundo tanto quanto atípico, porque não dizer fantástico, quanto surpreendentemente familiar, cujas reproduções de comportamento tão só constituem a corriqueira prática de se fazer a nós, sociedade, meros agentes realizadores, no sentido próprio de tornar-se real, realizar, por práticas tão comuns quanto quaisquer outras advindas do mundo dito “concreto”, não virtualizado.

Ao Direito, fenômeno necessariamente social, fulcrado em fatores culturais, indissociáveis dos hábitos humanos, resta a missão, por vezes inglória, de corresponder sincronicamente às demandas que esta mesma base social por ele chama, como quem se vê conclamado por fatores materiais à assunção de elementos jurídicos positivos, eficazes ao desmonte da insegurança que os hiatos normativos geram a quem necessite.

Para o Direito Penal, uma missão ainda mais espinhosa: tipificar situações novas, nomeados crimes cibernéticos, pautadas num cibermundo cuja variância de mérito beira o casuísmo. Como fazê-lo? Não ousamos pronunciar a resposta. Como dito alhures, parte-se da análise do tipo para a utilização analógica em dadas situações, jamais esquecendo o princípio da legalidade para o Direito Penal, em coadunância à própria temática dos crimes cibernéticos e em respeito à vedação da analogia *in malam partem*, para apontar-se à não criminalização dos crimes cibernéticos, mediante o emprego de tal recurso de integração.

Nestes termos, enseja, como se depreende, o início de uma discussão da qual ousamos acreditar, com o fito de contribuir às letras acadêmicas do Direito Penal Cibernético, para o que convidamos o leitor à reflexão, sem, notadamente, pretensões de esgotamento.

REFERÊNCIAS

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf>. Acesso em 15 de setembro de 2016.

CAVALCANTE, Andréa de Fátima Araújo. A atipicidade dos Crimes cibernéticos no Brasil e a impunidade: uma análise crítica. <Disponível em: http://repositorio.favip.edu.br:8080/bitstream/123456789/866/1/Monografia+Andrea+de+F%C3%A1tima+Ara%C3%BAjo+Cavalcante.pdf>. Acesso em 13de setembro de 2016.

CUNHA, Rogério Sanches. **Manual de Direito Penal – Parte Geral.** 3ª ed. Salvador: JusPodivm, 2015.

DA SILVA, Patrícia Santos. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais.** Brasília: Vestnik, 2015.

GRECO, Rogério. **Curso de Direito Penal.** 17. ed. Rio de Janeiro: Impetus, 2015.

MASSON, Cleber. **Direito penal esquematizado – Parte geral – vol. 1.** 9.ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2015.

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

OLIVEIRA, Anderson Soares Furtado. **Crime por Meios Eletrônicos.** Brasília: Universidade Gama Filho, 2009.

SILVA JÚNIOR, Edson Nascimento. **Introdução à computação.** Manaus: Universidade Federal do Amazonas, CETAM, 2009.

ROVER, Aires José. Crimes de informática. <Disponível em: http://www.infojur.ufsc.br/aires/arquivos/CRIMES%20DE%20INFORMATICA%20public.pdf>. Acesso em 10 de setembro de 2016.