



Escola da Magistratura do Estado do Rio de Janeiro

A evolução no combate aos crimes virtuais

Maria Paula Castro de Almeida

Rio de Janeiro
2015

MARIA PAULA CASTRO DE ALMEIDA

A evolução no combate aos crimes virtuais

Artigo Científico apresentado como exigência de conclusão de Curso de Pós-Graduação *Lato Sensu* da Escola de Magistratura do Estado do Rio de Janeiro.
Professores Orientadores:
Mônica Areal
Néli Luiza C. Fetzner
Nelson C. Tavares Junior

Rio de Janeiro
2015

EVOLUÇÃO NO COMBATE AOS CRIMES VIRTUAIS

Maria Paula Castro de Almeida

Graduado pela Pontifícia Universidade Católica do Rio de Janeiro. Advogada.

Resumo: A sociedade e suas relações estão em constante evolução e, como consequência, o Direito deve acompanhar as mudanças para que não existam relações jurídicas desprotegidas pelo ordenamento jurídico. O uso da internet nas últimas décadas apresentou um crescimento enorme, tornando cada vez mais comuns as interações entre pessoas através do mundo virtual. Com essas novas formas de se relacionar no ambiente cibernético tornaram-se mais comuns as práticas de crimes perpetrados nesse ambiente e tornou-se urgente a regulamentação dessas práticas criminosas, através de leis sobre o tema. A essência desse trabalho é abordar as características principais dos crimes virtuais e fazer uma análise da legislação atual acerca do tema, que surgiu como forma de combate a essas novas práticas.

Palavras-chave: Direito Penal. Internet. Crimes Virtuais

Sumário: Introdução. 1. O surgimento do Direito da Informática. 2. Crimes Virtuais: espécies e sujeitos 2. Lei penal no espaço e lugar do crime. 3. Legislação vigente. Conclusão. Referências.

INTRODUÇÃO

O Trabalho apresentado tem como objetivo abordar o tema dos crimes virtuais, fazendo breves considerações sobre o Direito da Informática e analisando as espécies desses crimes e algumas de suas características para então apresentar as Leis vigentes na atualidade acerca do tema.

A internet surgiu no contexto da Guerra Fria e, com objetivos essencialmente militares, era usada como forma de comunicação entre as forças armadas, caso os outros meios de comunicação fossem danificados ou interrompidos pelos inimigos. Com o passar do tempo foi sendo utilizada com outros objetivos, como a comunicação entre pessoas. Foi então na década de 90 que houve uma explosão da internet e essa passou a ser utilizada pelos mais diversos segmentos sociais e com os mais diferentes objetivos o que tornou nos dias atuais, tarefa difícil imaginar um mundo sem a internet.

Infelizmente não só de pessoas de boa índole vive a rede mundial de computadores. Com esse avanço na utilização da internet foram tornando-se comuns os crimes virtuais. Isso aconteceu porque o Direito não teve como acompanhar as mudanças da sociedade em tempo real, muito menos como acompanhar o surgimento quase que diário de novas tecnologias. Então com o *boom* da internet houve também a ampliação na prática dos crimes nesse ambiente e do número de pessoas prejudicadas por eles.

Durante quase 20 anos de internet, o Brasil não possuía qualquer lei específica que regulamentasse o tema, permitindo que a ação de criminosos fosse mais fácil e se propagasse em grande velocidade.

Foi nesse cenário, no qual se verificava o crescimento e a impunidade dos crimes virtuais, que surgiram em 2012, a Lei n. 12.735 e a Lei n. 12.737 que, entre outras coisas, tornaram crime a invasão de aparelhos eletrônicos para obtenção de dados particulares e promoveram alterações do Código Penal, que então passou a tipificar alguns crimes virtuais.

Esse trabalho científico busca, seguindo a metodologia do tipo bibliográfica e histórica, parcialmente exploratória, em um primeiro momento, fazer algumas considerações necessárias ao entendimento do assunto, demonstrando a importância do Direito acompanhar as mudanças que ocorrem na sociedade.

Em um segundo momento, busca-se fazer uma análise das espécies de crimes virtuais que são encontrados no ordenamento jurídico brasileiro, bem como apresentar seus sujeitos.

Em seguida, pretende-se continuar a análise, através da compreensão do local em que os crimes virtuais consideram-se ocorridos, apresentando alguns dos princípios do Direito Penal bem como a teoria que nosso Código Penal adotou para determinar se a lei penal brasileira será aplicada em determinado caso.

Ao final, pretende o trabalho, analisar a legislação vigente no Brasil sobre o tema, fazendo uma análise de cada uma das modificações que a Lei n. 12.735/12 e a Lei n. 12.737/12 trouxeram para o ordenamento jurídico.

1. O SURGIMENTO DO DIREITO DA INFORMÁTICA

A sociedade sofreu grandes transformações nos últimos anos, entre elas o enorme crescimento no número de usuários da rede mundial de computadores, mais comumente conhecida como internet. Segundo dados fornecidos pelo IBGE¹, do ano de 2009 ao ano de 2013 o número de usuários passou de 35 milhões para 85 milhões aproximadamente, o que significa dizer que em apenas 5 anos, o número de pessoas conectadas à rede, mais que duplicou.

Com essas transformações na sociedade é que vão surgindo novos ramos do Direito, que buscam se adaptar às mudanças e à novas realidades, não permitindo que relações corriqueiras fiquem desprotegidas pelo ordenamento jurídico. Assim surgiu o Direito da Informática, da necessidade de serem reguladas as relações entre as pessoas no mundo virtual, incluindo-se nessa regulamentação o combate aos crimes cometidos nessa esfera.

A influência da informática aconteceu em vários ramos do Direito. Os contratos eletrônicos passaram a fazer parte do cotidiano, modificando especialmente as relações de compra e venda do Direito Civil e do Direito do Consumidor, que agora podiam ser feitas pelo computador. Surgiram também os serviços de compra coletiva, permitindo a compra de produtos e serviços com grandes descontos, através da rede.

¹ ESTATÍSTICAS de usuários de internet, Domínios e Hosts no Brasil. Disponível em <<http://www.teleco.com.br/internet.asp>>. Acesso em 06 jun. 2015.

No campo do Direito Processual Civil surgiram o processo eletrônico² e os primeiros Juizados virtuais, por exemplo. No Direito Penal e Processual Penal também houve mudanças, sendo a mais importante para esse trabalho, o surgimento de leis específicas sobre os crimes virtuais.

Até 2012, como fora mencionado anteriormente, não havia qualquer regulação para infrações perpetradas no ambiente virtual, tornando essas cada vez mais comuns. Os computadores e a rede passaram a ser nova forma para a consecução de crimes que já existiam no ordenamento jurídico brasileiro.

Por esses motivos, surgiu para o Direito a importante tarefa de regular as relações entre os indivíduos no espaço cibernético. Para que seja possível essa regulação, faz-se necessária a identificação dos tipos de crimes que podem ser praticados pela via de computadores, para que a Lei possa regulá-los, evitando assim que se propaguem infinitamente e continuem gerando danos muitas vezes irreparáveis.

2. CRIMES VIRTUAIS: ESPÉCIES E SUJEITOS

Como visto anteriormente, foi nesse cenário de avanços tecnológicos na área da informática, que surgiram os denominados crimes cibernéticos, crimes de informática, crimes tecnológicos, crimes virtuais, crimes digitais; todos sinônimos.

Crime, em seu aspecto formal, na definição de Rogério Greco³, é “aquela conduta que viola os bens jurídicos mais importantes”, que “atenta e colide frontalmente contra a lei penal editada pelo Estado”. Em uma definição analítica, segundo ensina Guilherme de Souza

² A Lei n. 11.419/06 alterou o Código de Processo Civil regulamentando a informatização do processo judicial.

³ GRECO, Rogério. *Curso de Direito Penal: parte geral*. 15. ed. Rio de Janeiro: Impetus, 2013, p 142.

Nucci⁴, crime seria “toda conduta típica, antijurídica e culpável”. Para esse autor, fato típico seria todo comportamento humano, positivo ou negativo, que provoca um resultado e é previsto como infração penal. Fato antijurídico seria o fato que contraria o ordenamento jurídico. E, por fim, fato culpável, seria a reprovação da ordem jurídica a esse fato típico e antijurídico.

Certo é que da mesma forma que existe a criminalidade tradicional, no mundo físico, existe a criminalidade no mundo cibernético, que pode assumir diferentes formas e métodos diferentes, de acordo com o objetivo e habilidades do criminoso.

Assim, deve-se bucar uma definição para melhor compreensão do tema e muito embora seja o conceito de crime virtual seja conceito com divergência na doutrina, pode-se dizer, segundo a definição de Carla Rodrigues Araújo de Castro⁵ que:

Crime virtual é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Inclui-se nesse conceito os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador.

Portanto, os crimes da internet subdividem-se em crimes contra o computador e crimes por meio do computador, ou segundo a doutrina ensina, os crimes digitais podem ser classificados em próprios e impróprios.

Os crimes próprios, também chamados de crimes puros são aqueles que só podem ser praticados na informática, ou seja, a execução e a consumação ocorrem nesse meio. Tratam-se de tipos novos em que o bem jurídico tutelado é a informática. São aqueles em que o sujeito se utiliza necessariamente do computador, que é usado como objeto e meio para execução do crime.

Nesse raciocínio se posiciona Damásio de Jesus⁶:

⁴ NUCCI, Guilherme de Souza. *Código Penal Comentado*. 14 ed. Rio de Janeiro: Forense, 2014, p 101.

⁵ ARAÚJO DE CASTRO, Carla Rodrigues apud REDIVO, Rafella; MONTEIRO, Gabriela Loosli. O Direito frente à era da informática. Disponível em <<http://www.egov.ufsc.br/portal/sites/default/files/1411-2489-1-pb.pdf>>. Acesso em 06 jun. 2015.

Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade de dados, da máquina e periféricos) é o objeto jurídico tutelado.

Nessa categoria de crimes está a invasão de dados armazenados em computador com o intuito de modificar, alterar, inserir dados falsos e também aqueles que atingem, diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos. Alguns exemplos são a violação de e-mail e o dano em arquivos causado pelo envio de vírus.

Os crimes virtuais impróprios, por sua vez, são aqueles que já estão tipificados pelo Direito Penal mas que são cometidos com a utilização do computador e da rede, ou seja, a máquina em si é utilizada como instrumento para a realização das condutas ilícitas. São, portanto, aqueles já tipificados que violam bens já protegidos pela legislação brasileira, podendo ser praticados de qualquer forma, sendo o computador só mais um meio/instrumento de execução dessa conduta.

Assim, corrobora Damásio⁷:

[...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens não-computacionais ou diversos da informática.

Diante do exposto e para fins de didática, é importante definir alguns dos crimes impróprios mais praticados em nosso ordenamento jurídico. Primeiramente, os crimes contra a honra, quais sejam, calúnia, difamação e injúria, que dizem respeito à reputação da vítima e estão previstos respectivamente nos artigos 138, 139 e 140 do Código Penal⁸. Podem ocorrer nas redes sociais, nas páginas de internet, por exemplo, se alguém divulgar informações falsas

⁶ DAMÁSIO DE JESUS apud ARAS, Vladimir. *Crimes de informática: Uma nova criminalidade*. Disponível em <<http://jus.com.br/artigos/2250/crimes-de-informatica>>. Acesso em 5 jul. 2014.

⁷ Ibid.

⁸ Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 5 jul. 2014.

que acusem alguém de fato definido como criminoso, fatos que prejudiquem a reputação de outra pessoa, ou ainda ofendam a dignidade do outro.

Em segundo lugar, os crimes contra a liberdade individual, tais quais a ameaça, a violação de correspondências, a divulgação de segredos. A ameaça está prevista no art. 147 do Código Penal e consiste em escrever ou mostrar uma imagem que ameace alguém, avisando que a pessoa será vítima de algum mal ainda que seja em tom de piada ou brincadeira.

São frequentes também casos de discriminação, quando alguém escreve uma mensagem ou publica uma imagem que seja preconceituosa em relação a raça, cor, etnia, religião ou origem de outra pessoa. Várias páginas da rede social facebook são excluídas diariamente em razão de denúncias feitas pelos próprios usuários, de que tais páginas abrigam conteúdo discriminatório.

Verifica-se ainda, inúmeros casos de estelionato, crime contra o patrimônio, previsto no artigo 171 do Código Penal, que na maioria das vezes, ocorre quando o criminoso engana a vítima para conseguir uma vantagem financeira. Pode acontecer em sites de leilões, por exemplo, se o vendedor enganar o comprador recebendo o dinheiro da transação sem entregar a mercadoria. Pode acontecer também quando alguém vende um produto pela internet e não o entrega.

Uma vez feita a definição dos crimes cibernéticos, em próprios e impróprios, cabe fazer uma análise sobre os sujeitos ativo e passivo da relação. Os crimes virtuais são crimes comuns, aquele que segundo Cezar Roberto Bitencourt⁹ “pode ser praticado por qualquer pessoa, não exige qualquer qualidade especial, seja do sujeito ativo, seja do sujeito passivo do crime”.

⁹BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte geral*. 17. ed. São Paulo: Saraiva, 2012, p.108.

O sujeito ativo, que é o autor da infração penal, poderá ser tanto pessoa física, como pessoa jurídica, assim como entidade pública ou privada titular do bem jurídico tutelado. O sujeito passivo, que é pessoa ou ente que sofre as consequências da infração penal, poderá ser pessoa física ou jurídica, esta última porque pode, por exemplo, ter seus bens desviados, seu patrimônio deteriorado ou mesmo ter informações sigilosas violadas.

Tão importante quanto a classificação dos crimes informáticos e da análise de seus sujeitos é saber aplicar a lei penal no espaço, isto é, determinar em qual local o crime ocorreu, para que se possa assim, determinar se a lei penal brasileira se aplicará ao caso. Nos ensinamentos de Cezar Roberto Bitencourt¹⁰ “a lei penal, em decorrência do princípio de soberania, vige em todo o território de um Estado politicamente organizado”, todavia, comporta algumas exceções como será explicado em seguida.

2. LEI PENAL NO ESPAÇO E LUGAR DO CRIME

Com o surgimento da Internet e, com ela, do espaço cibernético, a concepção clássica de território modificou-se, já que esta permitiu uma interação num espaço em que não há limites físicos e exatamente por possuir tal característica é que trouxe maiores dificuldades para o legislador no sentido de definir o lugar do crime.

Diante disto, o conceito de lugar do crime precisou adaptar-se a nova realidade já que com o surgimento do mundo virtual a noção de espaço deixou de ser aquela relacionada ao espaço físico. Nesse sentido, um delito virtual pode ser cometido facilmente entre diversos países, uma vez que na internet não há fronteiras.

Chega-se então a uma questão de suma importância, descobrir o lugar no qual foi cometido o crime para que se possa determinar se o Brasil tem jurisdição para seu julgamento.

¹⁰ Ibid., p. 88.

A doutrina aponta cinco princípios a respeito da aplicação da lei penal no espaço, sendo eles, segundo Mirabete¹¹: da territorialidade; da nacionalidade; da proteção; da competência universal e da representação. Se torna necessária uma breve análise de cada um destes princípios.

O princípio da territorialidade é decorrente da soberania do Estado, que tem jurisdição sobre as pessoas que se encontram em seu território e prevê a aplicação da lei penal nacional ao fato praticado no território do próprio país.

O princípio da nacionalidade, por sua vez, está previsto no art 7º, inc II, “b” do Código Penal e não leva em consideração o local em que ocorreu o delito e sim a origem do agente que praticou tal delito, o Estado no exercício de sua soberania pode exigir que seu cidadão, mesmo que se encontre em país estrangeiro tenha determinado comportamento.

Pelo princípio da proteção, também chamado de princípio de defesa ou da competência real, não se consideram nem o local em que ocorreu o crime nem a nacionalidade do agente que o praticou, e sim se o bem jurídico atingido é nacional.

Já o princípio da competência universal, não considera quaisquer das condições dos anteriormente mencionados, não leva em conta o local do crime, a nacionalidade do agente ou sequer o bem jurídico que foi violado, bastando apenas que o indivíduo encontre-se em território nacional.

Por fim, o princípio da representação, é a aplicação do princípio da nacionalidade, mas não do agente ou da vítima, e sim do transporte em que ocorreu o crime. O legislador autoriza a aplicação da lei penal estrangeira quando frente a delito cometido em aeronave ou embarcação privada, desde de que não este tenha sido perseguido pelo judiciário detentor da competência originária, por deficiência legislativa ou desinteresse punitivo.

¹¹ MIRABETE, Julio Fabrinni. *Manual de Direito Penal*. 23 ed. São Paulo: Atlas, 2006, p 56.

Para a aplicação da regra da territorialidade é necessário, que se esclareça o lugar do crime, que de acordo com a doutrina penalista e a previsão do art 6º do Código Penal, corresponde ao local em que o crime tiver sido praticado ou àquele local em que tenha ocorrido o resultado. Portanto, nosso Código Penal, adotou a teoria da ubiquidade, pela qual se entende como lugar do crime, tanto o local da conduta como o do resultado.

Assim, através da aplicação o princípios supramencionados e da teoria da ubiquidade, terá eficácia a lei penal brasileira quando o crime tem início em território estrangeiro e se consuma no Brasil, e também quando os atos executórios do crime são praticados em nosso território mas o resultado se produz em país estrangeiro.

Feita essa análise, saindo do plano teórico e ingressando no plano prático, deve-se passar a compreensão das leis que existem em nosso ordenamento jurídico no tocante aos crimes virtuais.

3. LEGISLAÇÃO VIGENTE

No Direito Penal, assim como em todos os ramos do Direito, é imperiosa a aplicação do princípio da legalidade, que é cláusula pétrea insculpida no art. 5º, inciso XXXIX da Constituição da República Federativa do Brasil¹² e traz a seguinte redação: “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Isso quer dizer que, para que possa haver punição dos crimes praticados no meio digital, deve antes haver previsão legal nesse sentido.

O Brasil nunca demonstrou fortes iniciativas no tocante aos crimes virtuais, deixando o tema sem qualquer previsão e completamente desprotegido por muitos anos, sem leis

¹² BRASIL, Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 5 jul. 2014.

específicas que tratassem dos delitos que estavam crescendo desenfreadamente. Foi apenas no ano de 2012 que foram aprovadas duas Leis específicas em relação ao tema e que trouxeram algumas inovações importantes para o Direito da Informática.

A primeira delas foi a Lei 12.735/12¹³ que passou a tipificar condutas realizadas mediante o uso de sistema eletrônico, digitais ou similares, que fossem praticadas contra sistemas informatizados e similares. Todavia, tal lei foi vetada quase que em sua totalidade pela presidente da República, Dilma Rousseff, restando a essa norma somente instituir que órgãos da polícia judiciária, as polícias civis dos Estados e do DF deverão estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado¹⁴.

Além disso, a Lei 12.735/12 conservou seu art 5º, que alterou o inciso II do §3º do art. 20 da Lei 7.716/89¹⁵. A lei alterada, que define os crimes de preconceito de raça ou de cor passou a trazer previsão expressa de que o juiz poderá determinar a cessação das transmissões eletrônicas.

Já a Lei 12. 737/12¹⁶, trouxe a tipificação criminal de delitos informáticos e alterou o Código Penal em dois dos seus artigos. Foi apelidada de Lei Carolina Dieckmann pois o projeto de lei (PL 35/12) foi elaborado à época em que as fotos íntimas da atriz foram divulgadas na internet.

Cabe analisar cada uma das mudanças trazidas por esta lei.

¹³ Lei n.º 12.735 de 30 de novembro de 2012, que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 16 mar. 2015.

¹⁴ DILMA sanciona lei dos crimes cibernéticos. Disponível em <<http://www12.senado.leg.br/noticias/materias/2012/03/presidente-dilma-sanciona-leis-dos-crimes-ciberneticos>>. Acesso em 23 abr. 2015.

¹⁵ Lei n.º 7.716 de 5 de janeiro de 1989, que define os crimes resultantes de preconceito de raça ou de cor. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L7716compilado.htm>. Acesso em: 16 mar. 2014.

¹⁶ Lei n.º 12.737 de 30 de novembro de 2012, que traz a tipificação criminal de delitos informáticos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Acesso em: 16 mar. 2015.

Inicialmente, a Lei 12.737/12, em seu artigo 2º, acrescentou ao Código Penal Brasileiro, dentro dos crimes contra a liberdade individual, dois artigos, 154A e 154B, trazendo as condutas que fazem parte do tipo bem como suas sanções e por fim a ação penal utilizada para tais casos.

A conduta prevista no *caput* do art 154A¹⁷ traz como núcleo do tipo o verbo invadir, que significa violar, transgredir, entrar à força em algum lugar. O objeto a conduta, é o dispositivo informático e esse deve ser pertencente a outra pessoa. A expressão instalar vulnerabilidade traz a conduta o indivíduo de obter vantagem ilícita tornando o dispositivo informático acessível à violação¹⁸. A pena prevista é a de detenção de 3 (três) meses a 1 (um ano) para quem incorrer nessas condutas.

O §1º do artigo citado trouxe algumas condutas que foram equiparadas àquelas do *caput*, com o objetivo de punir os atos preparatórios do crime, através da punição daqueles que facilitam a invasão, produzindo, oferecendo, distribuindo, vendendo ou difundindo dispositivo informático que permita o cometimento do crime mencionado no parágrafo anterior. Com essa previsão a intenção do legislador foi punir os indivíduos que estavam indiretamente relacionados ao crime.

O §2º do art. 154A, tratou de proteger o patrimônio da pessoa lesada nas formas do *caput*, trazendo causa de aumento de pena, de um sexto a um terço, para as condutas que gerem prejuízo econômico para a vítima.

O §3º trouxe uma forma de qualificação pelo resultado: “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”, a pena passa a ser de reclusão de 6 (seis) meses a 2 (dois) anos pois

¹⁷ O art. 154A do Código Penal tem a seguinte redação: “invadir dispositivo 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 de informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”.

¹⁸ NUCCI, op.cit., p. 812.

assim está também tutelando e tratando de forma mais severa os casos que repercutam na vida profissional do lesado.

O §4º tratou também de causa de aumento de pena mas apenas no tocante ao parágrafo anterior. Isto é, será aumentada a pena, de um a dois terços, caso os dados sigilosos protegido no §3º sejam repassados a terceiros e de um terço a metade, no §5º, caso a invasão seja cometida contra os chefes dos Poderes Legislativo, Executivo e Judiciário, o que representa maior gravidade da infração.

Portanto, após a análise do art. 154A, e segundo as considerações de Guilherme de Souza Nucci¹⁹, concluímos que os bens jurídicos tutelados são privacidade, o sigilo de dados e informações contidos em dispositivos informáticos de qualquer natureza e a propriedade material ou imaterial. Tanto o sujeito ativo quanto o sujeito passivo desse crime, podem ser pessoa física ou jurídica, não se exigindo nenhuma qualidade especial daquele que o comete, configurando crime comum. E, o elemento subjetivo do tipo é o dolo, não se punindo a forma culposa.

O artigo 145B, por sua vez, tratou das ações penais para os delitos cibernéticos. Tais delitos deverão ser processados mediante representação, na forma do art. 39 do Código de Processo Penal. A representação é a manifestação de vontade daquele que foi ofendido quanto a instauração da ação penal. Já nos casos em que houver questões de segurança nacional, ou seja, quando forem cometidos delitos 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 ação penal terá natureza pública incondicionada em razão da maior gravidade do ato cometido.

Fora todas as inovações trazidas pelo artigo 2º da Lei 12.737/12, seu artigo 3º trouxe ainda outras modificações ao Código Penal, acrescentando parágrafos aos artigos 266 e 298.

¹⁹ Ibid., p 811-813.

O art. 266 tipifica o crime de perturbação ou interrupção de serviços ligados à comunicação, tais quais: serviço telegráfico, radiotelegráfico ou telefônico estabelecendo a pena de 1 (um) ano a 3 (três) anos e multa para quem cometer o crime. A Lei 12.737/12 ao incluir o §1º a esse artigo ampliou a previsão do caput, aumentando o alcance da norma para os serviços telemáticos e de informação de utilidade pública.

Por fim, o parágrafo único, incluído no artigo 298, que tipifica o crime de falsificação de documento particular, equiparou o cartão de crédito e de débito a documento particular.

Essas foram, todas as mudanças proporcionadas pelas leis expostas, concluindo-se que houve inovações ao cenário jurídico penal brasileiro, que durante muitos anos deixou desprotegidas as relações no mundo virtual, em especial os crimes nesse âmbito mas que atualmente vem tentando combater tais delitos, mesmo que ainda haja poucas leis a respeito do tema.

CONCLUSÃO

Através do estudo das características principais dos crimes de informática, tais como suas espécies, sujeitos e lugar do crime, bem como da legislação especificamente aplicada, o trabalho cumpriu com seu objetivo, qual seja o de compreender o contexto jurídico dos crimes cibernéticos no ordenamento jurídico brasileiro. Após a exposição do tema e da análise de seus institutos, faz-se necessária a realização de algumas reflexões.

O Brasil, durante décadas desde o surgimento da internet deixou desprotegidas as relações que ocorriam entre os indivíduos nesse meio, facilitando a ploriferação de crimes e a impunidade dos criminosos.

Em 2012 foram criadas leis específicas sobre o tema mas que não se mostraram suficientes para combater os crimes virtuais uma vez que a cada dia que passa surgem novas formas de violação de direitos individuais através da rede mundial de computadores. A criminalidade digital dá grandes passos e a legislação não a acompanha.

É nítido, no entanto, que a Lei 12.737/2012 e a Lei 12.375/12 trouxeram grandes inovações ao cenário jurídico penal-informático, permitindo que alguns problemas mais recorrentes, como os crimes contra a honra, entre outros, fossem parcialmente controlados e punidos, através de tipificação.

É necessário, contudo, observar que a não só com Leis se impede o cometimento de crimes no ambiente virtual, já que como visto é impossível que o Direito acompanhe a evolução das tecnologias e o nascimento de outras condutas lesivas.

Diante disto, além de ser extremamente importante que o legislador esteja sempre trabalhando para editar novas normas jurídicas acerca do tema e atualizando as existentes, é necessário que aja em conjunto especialmente com os órgãos com poderes investigatórios, Ministério Público e Polícias, para que haja efetiva prevenção e combate dos crimes digitais, afinal, não adianta ter uma lei a respeito de um tema se esta não for efetivamente colocada em prática.

REFERÊNCIAS

ARAÚJO DE CASTRO, Carla Rodrigues apud REDIVO, Rafella; MONTEIRO, Gabriela Loosli. O Direito frente à era da informática. Disponível em <<http://www.egov.ufsc.br/portal/sites/default/files/1411-2489-1-pb.pdf>>. Acesso em 06 jun. 2015.

BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte geral*. 17. ed. São Paulo: Saraiva, 2012.

BRASIL, Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 5 jul. 2014.

_____, Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/De12848compilado.htm>. Acesso em: 5 jul. 2014.

_____, Lei n.º 7.716 de 5 de janeiro de 1989, que define os crimes resultantes de preconceito de raça ou de cor. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L7716compilado.htm>. Acesso em: 16 mar. 2015.

_____, Lei n.º 12.735 de 30 de novembro de 2012, que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 16 mar. 2015.

_____, Lei n.º 12.737 de 30 de novembro de 2012, que traz a tipificação criminal de delitos informáticos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 16 mar. 2015.

DAMÁSIO DE JESUS apud ARAS, Vladimir. *Crimes de informática: Uma nova criminalidade*. Disponível em <<http://jus.com.br/artigos/2250/crimes-de-informatica>>. Acesso em 5 jul. 2014.

DILMA sanciona lei dos crimes cibernéticos. Disponível em <<http://www12.senado.leg.br/noticias/materias/2012/03/presidente-dilma-sanciona-leis-dos-crimes-ciberneticos>>. Acesso em 23 abr. 2015.

ESTATÍSTICAS de usuários de internet, Domínios e Hosts no Brasil. Disponível em <<http://www.teleco.com.br/internet.asp>>. Acesso em 06 jun. 2015.

GRECO, Rogério. *Curso de Direito Penal: parte geral*. 15. ed. Rio de Janeiro: Impetus, 2013.

JESUS, Damásio Evangelista de. *Código Penal anotado*. 22. ed. atual. São Paulo: Saraiva, 2014.

MIRABETE, Julio Fabrinni. *Manual de Direito Penal*. 23 ed. São Paulo: Atlas, 2006.

NUCCI, Guilherme de Souza. *Código Penal Comentado*. 14. ed. Rio de Janeiro: Forense, 2014.