UNIVERSIDADE LUTERANA DO BRASIL – ULBRA

CAMPUS GRAVATAÍ

JEAN PABLO BARBOSA VELLOZO

CRIMES INFORMÁTICOS E CRIMINALIDADE CONTEMPORÂNEA

Gravataí

2015

JEAN PABLO BARBOSA VELLOZO

CRIMES INFORMÁTICOS E CRIMINALIDADE CONTEMPORÂNEA

Monografia apresentada como requisito para a obtenção do grau de Bacharel em Direito da Faculdade de Direito da Universidade Luterana do Brasil.

Orientador: Leonel Carivali

Gravataí

2015

RESUMO

O presente trabalho tem por objetivo demonstrar a maneira com que a internet se tornou parte da vida das pessoas e de que forma se tornou também uma arma na mão dos criminosos. Analisar o conceito dos crimes informáticos e a sua ingerência no âmbito do Direito Penal. Citar exemplos de crimes informáticos, alguns crimes já previstos no Código Penal, entretanto, sendo a internet e os dispositivos informáticos um meio para o seu cometimento e, sendo assim, dividindo-os em crimes informáticos próprios e impróprios. Analisar questões processuais inerentes a esse novo tipo de crime e as suas respectivas peculiaridades. Apresentar diferentes visões doutrinárias quanto ao seu conceito e a necessidade de legislação específica. Apresentar diferentes interpretações à Lei 12.737 de 2012 e as suas fragilidades. Elencar propostas legislativas que tem o intuito de regular atitudes na internet e nos meios eletrônicos, demonstrar seus pontos fortes, quando realmente trazem inovações no sentido de equiparar o direito à modernização da sociedade, bem como suas carências e limitações.

Palavras-chave: crimes informáticos; direito penal; internet; dispositivos eletrônicos; processo penal;

ABSTRACT

This study aims to demonstrate the way in which the internet has become part of people's lives and how they became also a weapon in the hands of criminals. To analyze the concept of computer crimes and their interference in the criminal law. Give examples of computer crimes, some crimes already provided for in the Penal Code, however, the internet and computer devices being a means for its commission and, therefore, dividing them into proper and improper computer crimes. Examine procedural issues related to this new type of crime and their respective peculiarities. Have different doctrinal views about its concept and the need for specific legislation. Have different interpretations of Law 12,737 of 2012 and its weaknesses. To list legislative proposals which aims to regulate attitudes on the Internet and in electronic media, to demonstrate their strengths when really bring innovations in order to equate the right to modernization of society as well as its shortcomings and limitations.

Keywords: computer crimes; tort law; internet; electronic devices; criminal proceedings;

Sumário

1. Introdução

A internet, outrora uma ferramenta de comunicação militar, evoluiu de maneira global. Hoje, inclusive, é indispensável para determinadas atividades e transformou, por meio de suas facilidades, a vida cotidiana. Muitas das atividades humanas foram englobadas pela automatização em vários setores de produção. A evolução exacerbada da internet e dos computadores culminou no surgimento de um universo paralelo e instantâneo: o cyber espaço. Essa facilidade e agilidade trazida por esse novo universo fez com que as redes computacionais se tornassem meio de efetivação de negócios envolvendo valores cada vez maiores. Não só valores monetários, a informação se tornou a verdadeira riqueza. Porém, essa troca ininterrupta de informação atrai também a criminalidade, pois, a ausência de uma regulamentação e o falso anonimato proporcionado pela grande rede de computadores trouxe consequências negativas.

Dessa forma, inúmeros delitos surgem e se propagam neste novo universo. Surge, também, a necessidade de uma regulamentação e controle das atividades, pois a internet se torna tanto o instrumento, quanto o alvo dos agentes criminosos. Crimes já conhecidos como furto, fraude, estelionato são cometidos diariamente na internet e de maneira bem explícita. Outras atividades não tipificadas, mas prejudiciais, também são cometidas por meio ou contra a internet, computadores e dispositivos informáticos, tornando, assim, indispensável um regramento para este gigantesco e, muitas vezes, descontrolado universo.

A matéria provoca controvérsia. Qual o conceito de crime informático? Quais suas formas? Dada a complexidade de algumas atividades, como o processo penal lida com tais situações? Na ausência de legislação, podem as outras fontes do direito suprirem essa lacuna? Poderia se falar em crime sem prévia cominação legal? A legislação vigente é suficientemente abrangente? Estas serão as questões abordadas no decorrer deste trabalho. Um tema novo dentro da ciência penal, os crimes informáticos possuem uma importância relevante no sentido de que a ausência de normas aplicáveis a esse tipo de crime, deixa uma série de condutas ilícitas carentes de punição, o que se agrava

com o aumento da criminalidade e da sensação de insegurança dominante nesse novo universo, contribuindo, assim, ao não aproveitamento de todas as vantagens oferecidas pela utilização dos meios informáticos.

2. Conceito de Crime Informático:

A internet é hoje o meio mais utilizado para a comunicação das pessoas. Não só isso, ela também é utilizada de diferentes formas: seja para o trabalho; fazer comprar; agendar viagens; movimentar contas bancárias e, até mesmo, cometer crimes. O mundo inteiro está conectado e, por conta disso, a internet é quase essencial para certas atividades, tornando-se um mar de oportunidades para atividades delituosas.

Conforme Furlaneto Neto (2012, pag. 25) citando Ferreira (2000, p.209), o surgimento dos crimes informáticos remonta à década de 1960, quando houve os primeiros registros do “uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas”. Apenas nos anos de 1970 verificaram-se “estudos sistemáticos e científicos sobre essa matéria, como emprego de métodos criminológicos”, relativos a delitos informáticos verificados na Europa em instituições de renome internacional.

Tal aspecto culminou para que nos anos 1980 se potencializassem as ações criminosas “que passaram a incidir em manipulações de caixas bancários, pirataria de programas de computador, abusos nas telecomunicações etc., revelando a vulnerabilidade que os criadores do processo não haviam previsto” (FERREIRA, 2000, p. 209-210). A esse cenário, acrescenta-se o delito de pornografia infantil perpetrado por meio da internet, igualmente difundido na época, mas com maior potencialidade na década de 1990. (FURLANETO NETO, 2012, pag. 25).

A criminalidade informática no entender de Gomes (2000), conta com as mesmas características da informatização global:

a) **transnacionalidade**: todos os países fazem uso da informatização (qualquer que seja o seu desenvolvimento econômico, social ou cultural); logo, a delinquência correspondente, ainda que em graus distintos, também está presente em todos os continentes;
b) **universalidade**: integrantes de vários níveis sociais e econômicos já tem acesso aos produtos informatizados (que estão se popularizando cada vez mais);

c) **ubiquidade**: a informatização está presente em todos os setores (públicos e privados) e em todos os lugares. (Grifo do autor)

Importa ressaltar, no entanto, que a doutrina não chegou a um consenso quanto ao nome jurídico do crime, tampouco quanto ao conceito dos crimes em espécie. Como ressalta Lima (2006), a doutrina aborda a temática sobre o título dos crimes virtuais, crimes digitais, crimes informáticos, crimes de informática, crimes de computador, delitos computacionais, crimes eletrônicos etc.

Uma primeira abordagem da questão é desenvolvida por Corrêa (2000b, p. 43), no contexto dos denominados “crimes digitais”, conceituados como “todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar”.

Percebe-se que o autor leva em consideração, no caso citado, os crimes cometidos contra o computador, ou seja, contra as informações e *softwares* nele contidos, ou ainda contra informações ou dados transmitidos de computador para computador, com dolo específico de ameaça e fraude, não abordando aqueles crimes praticados com o computador, mas cujo o bem protegido pelo ordenamento jurídico é diverso, como, por exemplo, a pornografia infantil.

Já Pinheiro (2001, p. 18-19), dá uma classificação diferente aos crimes informáticos, sendo ela: crimes informáticos puros, mistos e comuns. Segundo o autor, crime virtual puro é aquele em que o computador, em seu aspecto físico, ou os dados e programas nele contidos são objetos de uma ação ou omissão antijurídica. O crime virtual misto, por sua vez, caracteriza-se pelo emprego obrigatório da internet no *iter criminis,* embora o bem jurídico a ser lesado seja diverso, citando como exemplo as transferências ilícitas de valores de uma *home banking*, caracterizando, assim, a internet como instrumento do crime. Já o crime virtual comum, segundo o citado autor, é aquele em que a internet é um instrumento para o cometimento de um crime já previsto no ordenamento jurídico penal. E cita, como exemplo, o crime de pornografia infantil que, antes do advento da rede mundial, era praticado de outras formas, enquanto agora se dá por meio de e-mails, sala de bate papo etc. Arremata seu raciocínio ao afirmar que, neste caso, “mudou a forma, mas a essência do crime permaneceu a mesma”. (PINHEIRO, 2001, p. 19-19).

De uma forma mais abrangente e com base no conceito analítico do crime, Ferreira (2000, p. 210) define crime informático como “toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão”. Furlaneto Neto (2012, pag. 27-28) explica que a autora:

> baseia no conceito analítico de crime, entendendo-o como o fato típico, antijurídico e culpável, apesar de boa parte da doutrina nacional retirar a culpabilidade de tal conceito, entendendo-a como pressuposto da pena. Porém, Fragoso (1989), Bittencourt (2008), entre outros autores mantêm a culpabilidade como elemento da estrutura do ilícito penal, alegando que a ação típica e antijurídica para constituir o crime tem que ser culpável.

Mesmo com todas as definições e as diferentes abordagens dos doutrinadores quanto ao conceito de crime informático, percebe-se o seguinte consenso: ora o computador é o instrumento do crime, ora como seu objeto.

Neste sentido, a fim de elucidar melhor os tipos de crimes informáticos, passar-se-á a discorrer acerca de alguns exemplos de crimes informáticos, tanto os crimes em que o computador e a internet são utilizados como instrumento para o cometimento de delitos já tipificados, quanto os que o computador ou dispositivo informático, seus dados, programas e informações, são alvo dos agentes criminosos.

2.1. Exemplos de crimes informáticos

Conforme já visto, o computador pode ser tanto o instrumento para o cometimento de crimes, quanto o objeto de um crime, nesse caso, os programas, informações e dados nele contidos. Nesse mister, passar-se-á a discorrer alguns exemplos de crimes já tipificados que podem ser cometidos por meio do computador (crimes informáticos impróprios), bem como os que o computador e seus dados são o alvo do crime (crimes informáticos próprios), conforme segue.

2.1.1. Estelionato

O art. 171 do Código Penal conceitua o crime de estelionato como quando o agente obtém, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. Na visão de Pierangeli (2005, p. 486), o crime em tela é

uma “forma evoluída de criminalidade, que apresenta uma característica típica dos tempos modernos, modernidade que concedeu aos agentes avançadas maneiras de execução”. Esse tipo penal tem como tutela o patrimônio, enquanto objeto jurídico, em face dos atentados que podem ser praticados mediante fraude, engodo, etc.

O legislador quando não limita as formas para o cometimento do crime de estelionato, abrange também o cometido com uso do computador, por meio da internet e que tem, na sua essência, toda a descrição do tipo penal, apenas a maneira de execução, como disse Pierangeli, é que se modernizou. Para alguns autores, a pessoa enganada também deve ser considerada objeto material, consistindo, de acordo com Nucci (2003, p. 576), em “conseguir um benefício ou um lucro ilícito em razão do engano provocado pela vítima. Essa colabora com o agente sem perceber que está despojando de seus pertences”.

Furlaneto Neto (2012, p. 63) diferencia o estelionato do furto afirmando que “o que se visa não é especificamente a coisa alheia móvel, mas sim a vantagem ilícita, a qual deve ter caráter econômico, pois se encontra inserido entre os delitos contra tal bem jurídico, tratando-se de qualquer tipo de lucro, vantagem, ganho, devendo ser ilícito”.

Percebe-se, portanto, que no estelionato a vantagem ilícita deve ser de natureza econômica, prejuízo alheio significa dano patrimonial. A vítima deve ser pessoa certa e determinada. Não admite a modalidade culposa, consequentemente, é um crime com dolo específico. E é um crime com duplo resultado: obtenção de vantagem ilícita e o prejuízo alheio. Furlaneto Neto (2012, pag. 65) dá dois exemplos de como o crime de estelionato pode ser cometido por meio da internet:

> Por se tratar de um tipo penal aberto, o crime de estelionato pode ser praticado por qualquer meio eleito pelo sujeito ativo, inclusive pela internet, como por exemplo, na hipótese da denominada arara virtual, em que o sujeito ativo cria um *site* de comércio eletrônico para a venda de produtos informáticos, ofertando os produtos a preços convidativos e prometendo a entrega em 15 dias úteis, mediante o pagamento em depósito do valor em conta corrente. Nesse período, contabiliza o lucro com as vendas fraudulentas, sem fazer nenhuma entrega, de forma que, após um tempo, retira o *site* do ar, deixando inúmeras vítimas em prejuízo.

Percebe-se, nesse exemplo dado pelo autor, a presença do duplo resultado do crime de estelionato, qual seja: o lucro obtido pelo sujeito ativo mediante vantagem ilícita (fez todos os usuários do *site* transferir valores para sua conta e jamais entregou os produtos) e o prejuízo alheio (nenhum produto foi entregue pelo sujeito ativo em que pese as transferências bancárias, ocasionando prejuízo aos sujeitos passivos). E segue o autor:

> Outra hipótese que pode vir a caracterizar o estelionato é a venda de bens em *sites* hospedeiros, como por exemplo, um par de tênis, em que o suposto vendedor oferece o produto que pode ser adquirido por outrem mediante lance, de forma que, após a vítima ser declarada vencedora, o agente exige o pagamento em conta corrente para fazer a entrega do bem, porém, ao invés do tênis oferecido, o agente envia à vítima, via sedex, uma pedra. (FURLANETO NETO, 2014, p. 65)

O estelionato é, portanto, um crime já previsto no Código Penal e que pode ter como uma das formas de execução, a utilização do computador e/ou da internet. Percebe-se que é um crime em que o computador e/ou a internet pode ser o meio para se alcançar o resultado. É um “crime virtual comum”, conforme o supracitado Pinheiro (2001, p. 19) sendo a internet um instrumento para o cometimento de um crime já previsto no ordenamento jurídico penal.

2.1.2. Furto

Outro tipo penal já previsto pelo nosso Código e que tem grande ocorrência no mundo informático devido às inúmeras formas e possibilidades que a internet proporciona, é o crime de furto. Previsto no art. 155, tem como conduta central a de subtrair para si ou para outrem, coisa alheia móvel. A coisa alheia é apresentada por Nucci (2003, p. 519) como elemento normativo do crime em análise, e “é toda coisa que pertence a outrem, seja a posse ou a propriedade”. É um delito que pode ser praticado por qualquer pessoa, desde que não tenha ela a posse da coisa móvel, se não estaríamos diante do crime de apropriação indébita, bem como a vítima pode ser qualquer pessoa.

O Código Penal prevê inúmeras formas de furto qualificado, entre elas, o emprego da fraude. Há a necessidade de se deter mais na forma qualificada do furto, pois a fraude é a maneira mais usual de furto na internet. Fraude significa engano, trapaça, embuste, definida por Nucci (2003, p. 525) como “manobra enganosa destinada a iludir alguém, configurando também uma forma de

enganar a confiança instantânea estabelecida. O agente cria uma situação especial, voltada a gerar na vítima um engano, objetivando o furto".

Hipoteticamente, um usuário de *internet banking*[1] acessa sua conta corrente por meio da internet e descobre pela análise do extrato que houve um saque indevido de valor considerável. Assim, verifica com o gerente da instituição bancária e constata que o valor foi transferido de sua conta corrente para conta de um terceiro, de onde foi sacado, antes que se possibilitasse o bloqueio do valor. Toda a operação de transferência se deu com o emprego da senha pessoal do usuário junto à *internet banking*, subtraída com emprego de um *keylog*[2]*.* Isso permitiu que o agente se passasse pelo correntista e, sem provocar suspeita, transferisse eletronicamente um valor considerável de dinheiro para certa conta corrente junto a uma instituição bancária situada em município distante, de onde sacou o valor.

Esse breve exemplo demonstra uma das inúmeras formas que o furto mediante fraude é perpetrado pela internet. Conforme ensina Furlaneto Neto (2012, p. 53) em virtude do tipo penal não exigir condição especial do agente "qualquer pessoa poderá ser autora do crime de furto praticado por meio do computador, tratando-se de crime comum, no que se refere ao sujeito ativo". E segue o citado autor quanto ao sujeito ativo "em regra, trata-se de indivíduo com conhecimento em informática, criativo e obcecado por novos desafios". O referido autor, ainda, demonstra a forma com que o sujeito ativo pode obter as informações necessárias do computador do usuário:

> Aproveitando-se de portas vulneráveis, o invasor envia *e-mails* que contêm programas executáveis, de forma que permite, após sua instalação, o monitoramento do computador escolhido, viabilizando o seu controle. Assim, com a execução do programa espião, dados como número da conta corrente e senha do *internet banking* são capturados e enviados diretamente ao invasor que, de posse de tais informações, poderá perpetrar a subtração do dinheiro existente na conta corrente da vítima. (FURLANETO NETO, 2012, p. 53)

---

[1] *Internet banking* é um serviço disponibilizado pelas instituições financeiras que permite ao cliente acessar a sua conta corrente para saber saldo, obter extratos e realizar operações financeiras, como pagamento de contas; transferências, etc.

[2] *Keylog* é a ação de gravar e/ou registrar as informações digitadas em um teclado, de forma que a pessoa não tenha o conhecimento de que isso esteja sendo feito.

Esse é apenas um dos métodos que podem ser utilizados pelos fraudadores, obviamente existe inúmeros outros, como por exemplo a utilização de uma página falsa, idêntica à da instituição o qual o usuário costuma realizar operações pela *internet*, todavia, seu único objetivo é coletar as informações que o usuário irá inserir e encaminhar para o fraudador, que poderá utilizar para a subtração dos valores da conta. Isso pode ser facilmente realizado pelo fraudador quando encaminha vários *e-mails* a diferentes usuários, com a informação de que a instituição bancária X está com um novo método de proteção para os seus usuários e que basta acessarem o *link* contido no *e-mail* e inserirem os dados bancários que o novo sistema estará em funcionamento.

Sem desconfiar de que está sendo enganado, o usuário, na intenção de se proteger de ataques à sua conta corrente, clica no *link* e abre uma página idêntica ao da instituição bancária, insere as informações pessoais, enviando-as ao fraudador e acreditando estar fortalecendo a segurança da sua conta bancária. Furlaneto Neto (2012, p. 53) chama atenção para outra forma do fraudador realizar o furto, dizendo que:

> torna-se necessária cautela na análise da prova da autoria, pois o Cavalo de Tróia[3] permite ao *cracker*[4] monitorar completamente o computador de outrem. Assim, nada impede que, visando camuflar a conduta, o *cracker* invada o computador de uma pessoa e a partir deste faça o ataque a outros equipamentos ou utilize para acessar o *net banking* e fazer a subtração do dinheiro ou a operação fraudulenta. Alguns programas permitem que o *cracker* passe a ter o total controle da máquina infectada com o programa espião.

Verifica-se a dificuldade que se terá com provas periciais e as mais complexas formas de verificar se de fato houve o controle por um terceiro, que seria o fraudador verdadeiro, na máquina do suposto fraudador que teria subtraído valores da conta bancária da vítima. Quanto ao sujeito passivo, uma dúvida que pode se instaurar é, no caso dos exemplos de subtração de valores da conta por meio do *internet banking,* é se o sujeito passivo é o titular da conta corrente ou a instituição bancária, em cuja a posse estava o dinheiro no ato da

[3] Cavalo de Tróia é um programa malicioso que age entrando no computador e criando uma porta para uma possível invasão.
[4] Cracker é um indivíduo que pratica a quebra (*craking)* de um sistema de segurança de forma ilegal.

subtração. Conforme ensina Bitencourt (2003), primeiramente se protege a posse, secundariamente, a propriedade.

O citado autor acentua que, “se a posse e detenção são equiparadas a um bem para o possuidor ou detentor, é natural que os titulares desse bem se sintam lesados quando forem vítimas da subtração” Bitencourt (2003, p. 6). Dessa afirmação, se conclui que ambos, possuidor e detentor, podem ser vítimas de furto. Nesse pensamento, Furlaneto Neto afirma que:

> Verifica-se, portanto, uma dupla subjetiva passiva material no furto mediante fraude praticado pela internet, já que tanto o correntista como a instituição bancária devem figurar como vítimas, tendo em vista que a fraude atingiu inicialmente o correntista e possibilitou a obtenção de seus dados sigilosos, viabilizando, posteriormente, ao sujeito ativo do crime, acesso ao *net banking*, de forma que passar por titular da conta corrente e consuma a subtração. (FURLANETO NETO, 2012, p. 55)

Nota-se a complexidade que o uso do computador e da internet trazem para o crime de furto mediante fraude. Todavia, é um tipo crime previsto no Código Penal Brasileiro e a forma utilizada (fraude) é uma das suas qualificadoras. Estamos diante, novamente, de um crime informático comum ou, conforme Castro [5](2003), um crime informático impróprio.

2.1.3. Invasão de dispositivo informático

Tratando de um crime propriamente informático, o art. 154-A do Código Penal, inserido pela Lei 12.737 de 2012, define como crime:

> 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.

[5] CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais,* 2003, classifica os crimes informáticos em próprios e impróprios, tema que será discutido mais adiante.

> § 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 obtidas.
>
> § 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.

Abimael Borges[6], ao tecer comentários sobre o crime em questão assim se posicionou:

> A fim de proteger o direito ao sigilo de dado e informação pessoal ou profissional, o art. 154-A veio tipificar duas condutas: a principal é invadir dispositivo informático e a acessória é instalar vulnerabilidade. Podem ocorrer na forma simples (com a aplicação da pena básica) ou qualificada (com o agravamento da pena).
>
> O agente ativo dessa conduta pode ser uma pessoa física ou jurídica. Apesar de a lei não tratar essa matéria de forma especial, pois em nosso entender, deve haver uma legislação especial sobre o assunto, acreditamos ser esta uma espécie de crime próprio, pois para o cometimento de crimes eletrônicos, cibernéticos, exige-se do agente ativo que tenha certa habilidade no campo da informática, por mínima que seja, por isso esse não é um crime comum. Não é qualquer pessoa que o pratica, o chamado “analfabeto digital”, aquele que não tem contato algum com aparelhos eletrônicos. Sem conhecimento técnico, mesmo que seja o simples fato de saber ligar e desligar um dispositivo informático, a conduta se torna impossível.

[6] Abimael Borges é bacharel em Direito e teve seus comentários publicados pelo *site* JusBrasil no *link:* *http://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal* *acessado em 13/03/2015.*

Nota-se que o tipo penal trazido pela citada Lei tipifica duas condutas: invadir dispositivo informático e instalar vulnerabilidade. Entende o autor dos comentários que o agente ativo do crime deve ter certas habilidades no campo da informática, por mínima que seja, demonstrando não se tratar de um crime comum. O crime, nesse caso, é contra o computador, seus dados e programas, diferentemente dos outros crimes já trazidos, onde o computador e a internet eram um instrumento. O tipo penal em análise traz o verbo “invadir”, tratando-se da conduta do agente, que é tipicamente dolosa, pois a ação de invadir depende de vontade. Quanto à invasão, comenta Abimael:

> O resultado normativo da invasão poderá ser o de obter, adulterar ou destruir dados ou informações. Podem surgir resultados naturalísticos, aqueles que permeiam o mundo físico, como foi o caso da divulgação de fotos íntimas da atriz Carolina Dieckmann, pois feriu a honra, a dignidade, a liberdade pessoal da vítima, mas sua existência não é exigível na consumação do fato, mas o caráter formal do tipo independe do resultado, a consumação do delito se dá com a mera invasão, o resultado da invasão pode determinar a qualificação do tipo e o mero exaurimento da conduta delitiva.

Significa dizer, portanto, que a invasão consuma o delito. Independente da forma utilizada, o tipo penal não especifica o método de invasão, mas sim a sua finalidade. Segue Abimael:

> Invadir pressupõe a utilização de força, artimanha, violação indevida de mecanismo de segurança, desrespeito à vontade do proprietário do equipamento, ultrapassar o limite de autorização fornecida pelo titular do equipamento. É o tipo comissivo, em que o agente realiza a conduta proibida. (...) Se não houver nenhuma forma de resistência, a invasão não pode ser caracterizada.

Aqui verifica-se que para a consumação da invasão é necessária a violação indevida de mecanismo de segurança. O que acontece, então, com o uso não autorizado de dispositivo eletrônico que não possui senha ou mecanismo de segurança? O invasor pode ser um conhecido e pode usar o dispositivo da vítima para enviar as informações pessoais desta para outro dispositivo a fim de divulgar, chantagear a vítima, etc. O tipo penal traz apenas os casos de invasão com a violação de mecanismo de segurança.

Tratando da conduta de instalar vulnerabilidades, Abimael entende que:

> Quanto a conduta de instalar vulnerabilidade, o resultado previsto é a própria vulnerabilidade do equipamento, que pode ensejar a ocorrência dos resultados anteriores (obter, adulterar ou destruir dados ou

> informações). A conduta de instalar é acessória à invasão, já que aquela depende desta para ocorrer, os resultados são compartilhados, portanto.

A conduta acessória trazida pelo tipo penal é dependente da principal. Ou seja, para que instale uma vulnerabilidade no dispositivo da vítima o agente terá que invadi-lo antes. Ainda, o parágrafo 3º do art. 154-A aplica a mesma pena para quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida pelo caput. É, portanto, o delito de invasão de dispositivo informático, um crime informático próprio, pois o dispositivo informático (seja ele qual for) é o alvo da ação delituosa.

2.2. Crimes informáticos próprios e impróprios

Conforme visto anteriormente, a doutrina classifica os crimes informáticos de diversas formas, como na visão de Pinheiro (2001, p.18-19), onde o autor classifica os crimes informáticos em puros, mistos e comuns. Ainda, de maneira mais simples, Castro (2003), classifica os crimes em próprios e impróprios e será a forma utilizada para classificar os crimes informáticos neste trabalho. Os crimes informáticos impróprios são aqueles onde o papel do computador resume-se a mero instrumento para lesão de bens jurídicos não-computacionais. Este tipo de delito é normalmente amparado pelo Direito Penal tradicional, exigindo apenas, em alguns casos, pequenas adaptações na legislação. Conforme já citado, o crime de estelionato e o crime de furto mediante fraude, são comumente cometidos por meio do computador e da internet e servem de exemplos de crimes informáticos impróprios, pois o agente se utiliza de um computador, *smartphone* ou outro dispositivo informático, conectado ou não à internet, a fim de obter vantagem ilícita e/ou subtrair para si ou para outrem coisa alheia móvel.

Os crimes informáticos próprios são aqueles perpetrados contra os dados, programas ou estrutura física de sistemas computacionais. Estes exigem, na maioria das vezes, a adição de novas figuras penais, mormente em relação às ofensas contra os dados e programas. Desvio de DNS[7], fraudes eletrônicas,

[7] **DNS** significa *Domain Name System*, ou Sistema de Nomes de Domínios. É um computador com uma espécie de banco de dados que relaciona o endereço "nominal" de um site como www.uol.com.br com o endereço real onde está a página na rede, para poder acessá-la.

invasão de dispositivo informático, como já teve um exemplo citado, instalação de vulnerabilidades em dispositivos informáticos, de forma que o invasor tenha acesso total e irrestrito ao dispositivo alvo, apropriação de *passwords* por *fishing*[8] e sabotagem eletrônica através de vírus são exemplos de condutas antijurídicas contra sistemas computacionais. Nessa abordagem, vale destacar as lições de Ferreira (2000) que assim se posiciona:

> Por outro lado, inúmeros problemas e grandes prejuízos podem e têm sido causados por ações praticadas diretamente contra o funcionamento da própria máquina, como é o caso da disseminação proposital do chamado 'vírus do computador' que destrói programas e fichários dos usuários, e cujos resultados ultrapassam as fronteiras nacionais, pelo uso da Internet, adquirindo modernamente uma importância que não se ajusta aos estreitos limites do crime de dano conforme a tipificação feita no Código Penal.

O crescimento exponencial dos crimes informáticos, mais precisamente os próprios, onde os dispositivos, dados e *softwares* são os alvos, faz com que cada vez mais o Direito Penal precise se adequar e eliminar lacunas deixadas pela Lei. A distinção entre crimes informáticos próprios e impróprios se faz necessária, pois, como visto, os crimes em que o computador e a internet são utilizados com meio para a execução de atividade delituosa, já são previstos no ordenamento jurídico e, dessa forma, poderá o agente ser processado e julgado de acordo com as suas ações. Todavia, quando se trata de crimes informáticos onde o computador, seus dados e programas são o alvo, seja para a destruição do sistema, seja para coleta de dados sigilosos ou qualquer outra forma de deturpação, os crimes e as formas utilizadas vão se tornando tão complexos que o Direito Penal, até mesmo com as atualizações recentes, pode não comportar tais crimes, deixando uma lacuna na lei e uma porta aberta para tipos delituosos tão lesivos quanto os já previstos.

2.3. Aplicabilidade da Analogia nos Crimes Informáticos

A analogia, no entender de Mirabete (2012, p. 30) "é uma forma de auto integração da lei. Na lacuna desta, aplica-se ao **fato não regulado expressamente** pela norma jurídica, um dispositivo que disciplina hipótese

[8] ***Phishing***, termo oriundo do inglês (*fishing*) que quer dizer pesca, é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais.

semelhante" (*grifei*), neste sentido a analogia pode ser utilizada no Direito Penal "quando se vise, na lacuna evidente da lei, favorecer a situação do réu por um princípio de equidade" (Mirabete, 2012, p. 30). Todavia, não pode ser utilizada de maneira a contrariar o princípio da legalidade, pois não se pode impor sanção penal a fato não previsto em lei. Ou seja, "é inadmissível o emprego da analogia para *criar* ilícitos penais ou estabelecer sanções criminais" (Mirabete, 2012, p. 30).

Para Furlaneto Neto (2012, p. 21) o estudo da analogia é de suma importância, quando se trata de tipo penal positivo englobar ou não determinada ação ou omissão e assim se posiciona:

> Importante a discussão que se produz em volta da analogia sempre que se debate sobre o fato de um tipo penal positivo englobar ou não determinada ação ou omissão, não prevista de modo literal ou expresso na legislação existente, mas semelhante ao que foi legalmente previsto, ou seja, onde existe uma lacuna ou um meato.

A analogia é uma forma de integração da lei e não de interpretação, é prevista na Lei de Introdução às normas do Direito Brasileiro, em seu art. 4º: "quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito". Pela análise do artigo, percebe-se que a analogia é o primeiro recurso que o juiz pode se valer diante de uma lacuna na lei, por isso a sua importância. Para Maria Helena Diniz (1994, p. 110), a aplicação da analogia requer:

> Que o caso *sub judice* não esteja previsto em norma jurídica; que o caso não contemplado tenha com o previsto, pelo menos, uma relação de semelhança; que o elemento de identidade entre os casos não seja qualquer um, mas sim fundamental, ou de fato que levou o legislador a elaborar o dispositivo que estabelece a situação a qual se quer comparar a norma não contemplada.

Quanto ao fato da divisão, por alguns autores, entre *analogia legis*, como o fato da aplicação de uma norma já existente para solucionar um caso semelhante ao que ela previu, e *analogia juris*, no dizer da citada autora, a que se "estriba num conjunto de normas, para extrair elementos que possibilitem sua aplicabilidade ao caso concreto não contemplado, ou aos princípios gerais de ordem jurídica positiva, segundo, também, Heleno Cláudio Fragoso (1990). Uma outra divisão da analogia existente é entre analogia *in malam partem,* que é

aquela em que se prejudica de algum modo o réu, e analogia *in bonam partem,* como sendo aquela que de algum modo favoreça o réu.

Paulo José da Costa Júnior (1999, p. 25) sustenta que, em Direito Penal, a analogia *in bonam partem* é amplamente admitida, ao esclarecer que "o processo de integração da analógica, que se socorre dos princípios gerais do direito, é plenamente aceito para excluir a ilicitude ou a culpabilidade do agente, desde que não se tratem de normas excepcionais, em sentido estrito". Da mesma forma se posiciona Fragoso, ao observar que, em face do princípio da reserva legal, não se pode criar novas figuras penais, agravar a posição do réu ou ainda se aplicar penas ou medidas de segurança que não estejam legalmente previstas, pois, segundo ele, "analogia é somente admissível, em princípio, nos casos em que beneficia o réu (analogia *in bonam partem*), mas não pode ser acolhida em relação às normas excepcionais" (FRAGOSO, 1990, p.86).

Pode se dizer que este é o posicionamento mais acertado, pois com ele se alcança segurança jurídica, a qual, no Direito Penal, é demasiadamente necessária, ou de outra forma haveria o risco de punir condutas não previstas legalmente como delituosas, pelo mero entendimento jurídico, ao aplicar-se a analogia, desfigurando o Estado Democrático de Direito. Cabem aqui as palavras de Zaffaroni e Pierangeli (2001, p. 173):

> Se por analogia, em direito penal, entende-se completar o texto legal de maneira a estendê-lo para proibir o que a lei não proíbe, considerando antijurídico o que a lei justifica, ou reprovável o que ela não reprova ou, em geral, punível o que não é por ela penalizado, baseando-se na conclusão em que proíbe, não justifica ou reprova condutas similares, este procedimento de interpretação é absolutamente vedado no campo da elaboração cientifico-jurídica do direito penal.

Desta forma, percebe-se um consenso quanto à impossibilidade de se aplicar a analogia ao criar figura delitiva ou sanção penal não previstas legalmente de modo expresso, mesmo porque, em face das garantias constitucionais previstas no art. 5º da Constituição Federal, não é permitido tal tipo de integração da norma. Justamente por isso, trata-se aqui da aplicabilidade da analogia aos crimes informáticos, pois, sem uma legislação verdadeiramente abrangente, deve-se ter muito cuidado para não estar aplicando indevidamente o instituto da analogia, vedado, como se viu, para criar novas figuras penais.

Certos aspectos processuais merecem uma atenção especial no sentido de que, alguns, podem confundir os julgadores e, dessa maneira, criar-se-ia um vício ou nulidade no processo. A exemplo disso temos o local do crime em relação aos crimes informáticos, pois, dada a complexidade aplicada ao delito, possivelmente, haveria confusão em delimitar onde ocorreu, de fato, e qual juízo teria competência para julgar. Outro ponto a ser analisado seria o do tempo do crime, a fim de verificar se o ato cometido teria tipicidade à época. É o que será tratado no capítulo a seguir.

3. Direito Penal e Crimes Informáticos

Com o advento da era digital e o avanço exacerbado da internet e dos dispositivos informáticos, novos crimes e novas formas de execução foram sendo criadas e aperfeiçoadas nos crimes informáticos, de maneira que, cada vez mais, dificultou-se precisar quando o crime foi cometido, em que lugar se deu, quem seria competente para julgar crimes plurilocais e outras tantas questões penais que se tornaram cada vez mais controvertidas. Discorrer-se-á, a seguir, sobre algumas questões penais importantes e a sua aplicabilidade com relação aos crimes informáticos.

3.1. Tempo do crime

A fixação do instante em que o crime foi praticado é importante sob vários aspectos, mormente para, entre outras hipóteses legais, determinar a lei vigente no momento que o delito se consumou, no caso de sucessão de leis penais, para aferir a inimputabilidade penal, ou seja, se o agente tinha 18 anos na ocasião da consumação, ou se ao tempo da ação ou omissão era inteiramente incapaz de entender o caráter ilícito do fato ou ao menos se determinar de acordo com esse entendimento, além do exame das circunstâncias do crime e aplicação de eventual anistia condicionada no tempo.

Para Andreucci (2010, p. 102) “a questão referente ao tempo do crime apresenta particular interesse quando, após realizada a atividade executiva e antes de produzido o resultado, entra em vigor nova lei, alterando os dispositivos sobre conduta punível”. Nesse mister, o autor levanta o seguinte questionamento: “Qual a lei deve ser aplicada ao criminoso: a do tempo da

atividade ou aquela em vigor por ocasião da produção do resultado?", assim apresenta três teorias a respeito:

a) *Teoria da atividade*, segundo o qual se considera praticado o delito no momento da ação ou omissão, aplicando-se ao fato a lei em vigor nessa oportunidade;
b) *Teoria do resultado,* segundo o qual se considera praticado o delito no momento da produção do resultado, aplicando-se ao fato a lei em vigor nessa oportunidade;
c) *Teoria mista ou ubiquidade,* segundo o qual o tempo do crime é indiferentemente o momento da ação ou do resultado, aplicando-se qualquer uma das leis em vigor nessas oportunidades. (ANDREUCCI, 2010, p. 102)

Assim, o nosso Código Penal adotou a *teoria da atividade* no seu art. 4.º, que diz: "*Art. 4.º Considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado."* Portanto, considera-se tempo do crime o momento da ação ou omissão do agente, ou seja, no momento da prática da conduta prevista da norma penal incriminadora.

Sendo assim, com relação aos crimes informáticos, o tempo do crime é de suma importância, pois o agente pode ter cometido algum ato delituoso não previsto, na época, em nossa Lei Penal. Isso torna-se uma tarefa árdua aos julgadores, visto que, atualmente, tem-se pouca matéria tipificada sobre crimes informáticos enquanto há um universo de possibilidades para os agentes que cometem esse tipo de crime.

3.2. Local do crime

A fixação do lugar do crime é importante para fins de delimitar a competência do órgão jurisdicional para julgar o caso. Novamente Andreucci (2010, p. 112) nos traz três teorias que procuram solucionar o problema:

a) *Teoria da atividade*, segundo a qual o local do crime é aquele onde é praticada a conduta criminosa (ação ou omissão);
b) *Teoria do resultado*, segundo a qual o local do crime é aquele onde ocorre o resultado; e

c) *Teoria mista* ou *da ubiquidade*, também conhecida por *teoria da unidade*, segundo a qual o local do crime é aquele onde ocorreu tanto a conduta quanto o resultado, ou seja, qualquer etapa do *iter criminis.*

O legislador adotou em nosso Código Penal a teoria da ubiquidade, de maneira que se considera “praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”.[9]

A importância de se definir o lugar do crime ganha destaque nos casos de tentativa, em que, iniciada a execução do crime, este não se consuma por circunstâncias alheias à vontade do agente, bem como na hipótese de crimes a distância, naquelas infrações em que a ação ou omissão se dá em um país e o resultado em outro, situação muito comum quando se trata de crimes informáticos.

Interpretando a norma trazida, desde que no Brasil tenham sido praticados atos de execução, no todo ou em parte, ou aqui se tenha produzido o resultado do comportamento ilícito, é de aplicar-se a legislação pátria. Numa abordagem de questões de jurisdição e territorialidade nos crimes praticados por meio da internet, Valin (2000, p. 116) aponta problema para análise do caso quanto a situação compreender a segunda figura da norma comentada, ou seja, quando se considerar praticado o crime onde se produziu ou deveria produzir-se o resultado, “principalmente com o que diz respeito aos crimes que podem ser cometidos com a divulgação de informações, o ataque a servidores e furto de dados”.

O mesmo autor exemplifica levantando a hipótese de um ataque estrangeiro que acabe por retirar do ar um servidor de renome como o *Yahoo,* fisicamente não presente no território nacional, de forma que não permite que um usuário brasileiro possa acessá-lo no período.

Nessa hipótese, em que o crime realmente surtiu os seus efeitos e lesionou um bem juridicamente protegido de um cidadão brasileiro, qual seja, o

[9] Conforme art. 6.º do Código Penal.

direito de acesso à informação[10], pela análise fria da legislação, poderia ser julgado pelo Direito pátrio, ainda que o autor do delito e o portal *Yahoo*, vítima principal, não estejam fisicamente no território nacional. Porém, Valin (2000, p. 116-117) questiona se seria eficaz o julgamento realizado no Brasil, até por uma questão de aplicabilidade da lei penal.

Propõe o autor a revisão da matéria por meio de regras estabelecidas em tratado internacional, sendo adotado, para os crimes praticados por meio da internet, "algo semelhante à teoria da atividade que determina como sendo o local do crime aquele em que o agente praticou o delito", definindo-se qual o local efetivo da prática do ato, "se é o local onde se encontra o autor, ou se é o local em que as ofensas foram publicadas" (VALIN, 2000, p. 116-117).

Na opinião do autor, a melhor solução seria considerar como local do crime "aquele em que está o autor da infração". Justifica sua posição por considerar o país de domicílio do réu o melhor para aplicar eventual pena, além de evitar o processo de extradição, sempre moroso, bem como por ser o país do local da publicação o único com poder legal para retirar a página da rede, o que eventualmente poderá ser feito por meio de outro processo, independente do criminal.

3.3. Competência para julgar crimes plurilocais

A doutrina definiu crimes plurilocais como sendo "aqueles em que a ação ou a omissão se deu em um determinado local e o resultado em outro, mas dentro do território nacional (NUCCI, 2005). Tendo em vista as peculiaridades, é justamente dentro do conceito de crimes plurilocais que se insere a maior gama dos crimes praticados por meio da internet, como o furto mediante fraude, por exemplo.

Se imaginarmos a situação hipotética em que, após ter feito emprego de um *keylog* e subtrair dados da vítima, o agente conecta-se a um provedor de banda larga de Foz do Iguaçu – PR, acessa a *home banking* de uma instituição

[10] O direito ao acesso à informação foi elevado a garantia individual pelo inciso XIV do art. 5.º da CF. Outros institutos que o corroboram são o direito de petição e o *habeas data,* igualmente previstos no texto constitucional.

financeira particular de Marília – SP, onde fornece o número da conta corrente e a senha do cliente, e efetua a transferência de um valor razoável da conta bancária até a conta de um terceiro, situada em uma agência de Balneário Camboriú – SC. A vítima somente percebe a subtração no dia seguinte, quando o agente já providenciou o saque do valor respectivo da conta corrente do terceiro, para onde o valor tinha sido transferido de forma fraudulenta.

Percebe-se no exemplo trazido que o *iter criminis* se iniciou em Foz do Iguaçu – PR, passou por Marília – SP e se consumou em Balneário Camboriú – SC. Assim, como se delimita a competência no caso em tela? É de suma importância saber precisar a competência nesse caso, pois, como já dito, a maioria dos crimes cometidos pela internet tem essa característica.

Levando em consideração a regra geral de competência em razão do foro, prevista no art. 70 do Código de Processo Penal, o juízo da Comarca de Marília – SP é que deve conhecer e julgar o processo. Conforme abordado anteriormente, o furto é um crime material cuja consumação se verifica com a produção do resultado naturalístico. Segundo Nucci (2005, p. 223), “tal regra somente tem pertinência aos crimes materiais, isto é, aqueles que possuem resultado naturalístico e pode haver clara dissociação entre ação, omissão e resultado”. Portanto, fica afastada essa regra nos casos de crimes formais ou de mera conduta, cuja consumação se dá com ação de omissão.

Essa questão não é pacífica na doutrina, tanto é que Inellas (2004) defende a tese de que os crimes praticados por meio da internet são crimes formais. Para o autor, tais delitos se consumam no “local onde foi realizada a ação” (INELLAS, 2004, p. 85). Outros autores como Furlaneto Neto (2003) discordam desse posicionamento: “é verdade que a grande rede mundial de computadores trouxe a necessidade de algumas reflexões nos campos de Direito Penal e Processual Penal, porém, por si só, não teve o condão de modificar alguns institutos jurídicos.”

Nesse contexto, como já abordado ao apresentar a classificação dos crimes informáticos, há crimes já tipificados pela legislação e que não sofreram nenhuma alteração com o surgimento da internet, apenas tivemos a modificação do seu *modus operandi*. É sabido que algumas condutas necessitam ser

reexaminadas, tais como, a título de exemplo, o furto de tempo[11], cuja ação, no entendimento de Inellas (2004), se amolda por equiparação ao furto de energia elétrica, bem como o dano perpetrado pela disseminação de vírus, porém, assim como o tipo penal do homicídio não precisou ser modificado com o surgimento da arma de fogo, não se faz necessária a alteração de inúmeros crimes já tipificados pelo nosso Código e leis extravagantes com o fundamento no surgimento da internet.

Tendo em vista a dupla subjetividade passiva do crime de furto mediante fraude praticado por meio da internet, se o dinheiro subtraído estivesse depositado em uma agência da Caixa Econômica Federal, por se tratar de uma empresa pública, a competência para conhecer e julgar o crime seria da Justiça Federal, conforme entendimento do STJ:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE. (...) 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. (...) No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal. 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR. (STJ, CC nº 200601661530 (67343), GO, 3ª S., Relatora Min. Laurita Vaz)

Tendo como base a ementa supracitada e o entendimento utilizado pela Relatora Min. Laurita Vaz, no caso do furto mediante fraude exemplificado anteriormente, por se tratar de instituição financeira particular, a competência seria da Justiça Comum de Marília – SP, local onde se situa a agência bancária.

Nesse sentido, há também entendimento do TRF da 4ª Região:

> PROCESSO PENAL. COMPETÊNCIA. TRANFERÊNCIA FRAUDULENTA PRATICADA PELA INTERNET. SUBTRAÇÃO DE VALORES DEPOSITADOS EM BANCO. FURTO MEDIANTE FRAUDE.

[11] Inellas (2004) trata como furto de tempo o prejuízo experimentado pelos usuários da rede quando recebem *spams,* ou seja, mensagens indesejadas de natureza comercial, as quais lotam a caixa de mensagens e demandam perda de tempo, além de custos com energia elétrica.

> COMPETÊNCIA. LOCAL DA SUBSTRAÇÃO. 1. Em que pese a existência de recentes julgados desta Corte entendendo tratar-se de estelionato (com a divergência deste Relator) firmou-se a jurisprudência do Superior Tribunal de Justiça no sentido de que a hipótese de subtração, por meio eletrônico, de valores depositados em instituição bancária configura o crime de furto mediante fraude. 2. Modificada a orientação da 4ª Seção para, com base nos precedentes citados, declarar competente a Subseção Judiciária onde está situada a agência que mantém a conta corrente da qual os valores foram subtraídos. (TRF 4ª R., SER 2007.71.00.000608-6, 8ª T., Rel. Des. Fed. Luiz Fernando Wowk Penteado, DJe de 21.11.2007)

Importante salientar que as demais regras de competência previstas no CPP devem ser aplicadas à criminalidade informática, conforme o entendimento de Castro (2003) e todas elas auxiliam no sentido de esmiuçar a complexidade que se percebe em alguns delitos informáticos, tanto pela sua complexidade técnica, quanto pela complexidade jurídica.

Na tentativa de sanar a lacuna existente na legislação penal com relação aos crimes informáticos, o legislador, por meio da Lei 12.737, cria um novo tipo penal “invadir dispositivo informático” e, assim, inúmeras questões surgem em torno dessa nova modalidade. O objetivo do capítulo a seguir é apresentar, de uma forma geral, porém abrangente, essa alteração feita pelo legislador e as inúmeras consequências que dela se originam.

4. Legislação Brasileira e Crimes Informáticos

Como já visto anteriormente, muitos criminosos informáticos não são devidamente repreendidos, por conta de ausência de legislação que regule o comportamento do agente a fim de punir atividades ilícitas na internet ou contra dispositivos informáticos. Sendo assim, cada vez mais se faz necessária a presença de uma legislação ampla e abrangente, de maneira a não deixar lacunas e tentar preencher o máximo todas as possibilidades já encontradas de crimes informáticos. Vale lembrar que existem os crimes informáticos impróprios que já estão previstos no nosso Código Penal e não é sobre eles que há necessidade de legislar, mas sim sobre os crimes informáticos próprios, aqueles em que a internet, o computador e os dispositivos informáticos são alvos do agente criminoso.

Foi com esse objetivo que, em 2012, entrou em vigor a Lei 12.737 que altera o Código Penal e dá outras providências. Tida como novidade no âmbito jurídico, a Lei Carolina Dieckmann, como é conhecida pela imprensa, tenta exaurir essa lacuna existente na legislação penal quanto aos crimes informáticos. Será devidamente abordada em tópico especial.

4.1. Lei 12.737 de 30 de novembro de 2012

Apelidada de "Lei Carolina Dieckmann", a Lei nº 12.737, de 30 de novembro de 2012, entrou em pleno vigor no último dia 3 de abril de 2013, alterando o Código Penal para tipificar os crimes informáticos propriamente ditos (invasão de dispositivo telemático e ataque de denegação de serviço telemático ou de informação), ou seja, aqueles voltados contra dispositivos ou sistemas de informação e não os crimes praticados por meio do computador e que já são previstos no ordenamento penal.

Colateralmente equiparou o cartão de crédito ou débito como documento particular passível de falsificação. A lei é fruto de projeto apresentado pelo Deputado Federal Paulo Teixeira (PT-SP), cujo trâmite foi acelerado depois da invasão, subtração e exposição na internet de fotografias íntimas da referida atriz.

> 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.

O professor Eduardo Cabette[12], autor do livro Direito Penal – Parte Especial I da coleção Saberes do Direito (2013) tece comentários, em seu blog, à Lei supramencionada e assim se manifesta:

> É interessante notar que a legislação sob comento acabou ganhando o epíteto de "Lei Carolina Dieckmann", atriz da Rede Globo de televisão que foi vítima de invasão indevida de imagens contidas em sistema informático de

[12] Autor do artigo publicado no *link* http://atualidadesdodireito.com.br/blog/2013/01/03/novos-artigos-no-codigo-penal/ acessado em abril de 2015.

> natureza privada e cujo episódio acabou acelerando o andamento de projetos que já tramitavam com o fito de regulamentar essas práticas invasivas perpetradas em meios informáticos para modernização do Código Penal Brasileiro. Antes disso, era necessário tentar tipificar as condutas nos crimes já existentes, nem sempre de forma perfeita. A questão, sob esse ponto de vista, é agora solucionada pela Lei 12.737/12.

Quanto ao bem jurídico tutelado pela Lei em comento, o autor diz que:

> O bem jurídico tutelado é a liberdade individual, eis que o tipo penal está exatamente inserido no capítulo que regula os crimes contra a liberdade individual (artigos 146 – 154, CP), em sua Seção IV – Dos Crimes contra a inviolabilidade dos Segredos (artigos 153 a154 – B, CP). Pode-se afirmar também que é tutelada a privacidade das pessoas (intimidade e vida privada), bem jurídico albergado pela Constituição Federal em seu artigo 5º., X. Percebe-se, portanto, que a tutela é individual, envolvendo os interesses das pessoas (físicas e/ou jurídicas) implicadas, nada tendo a ver com a proteção à rede mundial de computadores e seu regular funcionamento.

E segue o citado autor ao se referir aos sujeitos ativo e passivo:

> O crime é comum, de modo que pode ser sujeito ativo qualquer pessoa. O mesmo se pode dizer com relação ao sujeito passivo. O funcionário público também pode ser sujeito ativo dessa infração, mas a lei não prevê nenhuma causa de aumento de pena. Pode-se recorrer nesse caso às agravantes genéricas previstas no artigo 61, II, “f” ou “g”, CP, a depender do caso. Também pode ser sujeito passivo a pessoa jurídica. É óbvio que as pessoas jurídicas também podem ter dados ou informações sigilosas abrigadas em dispositivos informáticos ligados ou não à rede mundial de computadores, os quais podem ser devassados, adulterados, alterados ou destruídos à revelia da empresa ou do órgão responsável. Isso se torna mais que patente quando se constata previsão de qualificadora para a violação de segredos comerciais ou industriais e informações sigilosas definidas em lei (artigo 154 – A, § 3º., CP), o que deixa claro que podem ser vítimas pessoas jurídicas de direito privado ou público. Entende-se que melhor andaria o legislador se houvesse previsto um aumento de pena para a atuação do funcionário público no exercício das funções, bem como para os casos de violação de dados ou informações ligados a órgãos públicos em geral (administração direta ou indireta).
>
> Também será sujeito passivo do crime qualificado, nos termos do § 3º. do dispositivo, o titular do conteúdo de “comunicações eletrônicas privadas, segredos comerciais ou industriais ou informações sigilosas, assim definidas em lei”. Podem ainda ser sujeitos passivos empresas privadas concessionárias ou permissionárias de serviços públicos também com relação a qualquer dos entes federativos. O sujeito passivo da infração é, portanto, qualquer pessoa passível de sofrer dano moral ou material decorrente da ilícita obtenção, adulteração ou destruição de dados ou informações devido à invasão ou violação de seu sistema informático, mediante vulneração de mecanismo de segurança. Assim também é sujeito passivo aquele que sofre a instalação indevida de vulnerabilidades em seu sistema para o fim de obtenção de vantagens ilícitas.

Ainda, o autor trata da consumação e tentativa acerca do novo crime previsto pelo Código Penal:

> O crime é formal e, portanto, se consuma com a mera invasão ou instalação de vulnerabilidade, não importando se são obtidos os fins específicos de coleta, adulteração ou destruição de dados ou informações ou mesmo obtenção de vantagem ilícita. Tais resultados constituem mero exaurimento da infração em estudo. Não obstante formal, o ilícito é plurissubsistente, de forma que admite tentativa. É plenamente possível que uma pessoa tente invadir um sistema ou instalar vulnerabilidades e não o consiga por motivos alheios à sua vontade, seja porque é fisicamente impedida, seja porque não consegue, embora tente violar os mecanismos de proteção.

Por fim, o autor faz uma classificação doutrinária do crime de invasão de dispositivo, classificando-o da seguinte forma:

> O crime é comum, já que não exige especial qualidade do sujeito ativo. É também formal porque não exige no tipo básico (simples) resultado naturalístico para sua consumação, mas a mera invasão ou instalação de vulnerabilidade. Também é formal na figura equiparada porque não exige que o material para a prática delitiva cheque efetivamente às mãos do destinatário, ou seja, realmente utilizado. Já nas figuras qualificadas é material porque exige para consumação a obtenção efetiva de conteúdo ou o controle remoto não autorizado do dispositivo invadido. Em qualquer caso o crime é plurissubsistente, admitindo tentativa. Trata-se ainda de crime instantâneo, comissivo, doloso (não há figuras culposas ou omissivas) e unissubjetivo ou monossubjetivo porque pode ser perpetrado por uma única pessoa, não exigindo concurso. Também pode ser comissivo por omissão quando um garante deixar de cumprir com seu dever de agir nos termos do artigo 13, § 2º., CP. Finalmente trata-se de crime simples por tutelar apenas um bem jurídico, qual seja a privacidade e o sigilo de dados e informações contidos em dispositivos informáticos de qualquer natureza.

Apresentando essa alteração da Lei Penal de uma forma mais objetiva, o Ministério Público de São Paulo[13], tece comentários e interpretações ao novo crime de invasão de dispositivos informáticos:

> O objeto jurídico tutelado pela norma é a liberdade individual do usuário do dispositivo informático. As penas para esses delitos são de reclusão de 3 (três) meses a 1 (um) ano de detenção, e multa, podem aumentar de 1/6 a 1/3 se a invasão resulta prejuízo econômico. O crime é qualificado, com penas que vão de 6 (seis) meses a 2 (dois) anos de reclusão e multa, caso a conduta não configure outro crime mais graves, quando a invasão resultar a obtenção de conteúdo de comunicações

[13] Texto: Novas Leis de crimes cibernéticos entra em vigor. Ministério Público de São Paulo. Centro de Apoio Operacional Criminal. Disponível em: http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf. Acesso em maio/2015. (com adaptações)

> eletrônicas privadas, segredos comerciais ou industriais, informações definidas em lei como sigilosas. Se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas, a pena do crime qualificado será também aumentada de 1/3 a 2/3.

Quanto às penas previstas:

> As penas, conforme os casos, (tipos simples ou qualificados) serão aumentadas de 1/3 até a metade, se o crime for praticado contra Presidente da República, Governadores e Prefeitos, Presidente do Supremo Tribunal Federal, da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal, ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Quando não se caracteriza o crime de invasão de dispositivo:

> Importante salientar que se a conduta for mais grave que a simples invasão com a finalidade de obtenção, adulteração ou destruição dos dados ou informações, ou a instalação de vulnerabilidades, como por exemplo, fraudes em *netbanking* (furto qualificado, como já visto anteriormente), estelionato ou extorsão, interceptação de comunicação telemática, o crime de invasão de dispositivo informático será desconsiderado, porque constituirá somente um meio para o cometimento daquelas condutas. Para que o criminoso possa ser investigado pela Polícia e processado pelo Ministério Público, é preciso que a vítima autorize, oferecendo a representação. O Ministério Público pode processar diretamente o criminoso somente quando o crime é praticado 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.

Interrupção de serviço telemático ou de informação pública, alterando a denominação prevista pelo art. 266 do Código Penal:

> O art. 266 do Código Penal pune a conduta de interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento, estabelecendo penas que variam de 1 (um) a 3 (três) anos de reclusão e multa, que são aplicadas em dobro em caso de calamidade pública. A Lei nº 12.327 alterou a denominação do crime do art. 266 do Código Penal, acrescentando que a interrupção de serviço telemático ou de informação de utilidade pública, bem como impedir ou dificultar-lhe o restabelecimento também é crime. Essa interrupção ou impedimento pode ser realizada de várias formas (crime de forma livre), por exemplo, a destruição física de uma determinada rede. Mas também pode ser feita mediante um ataque virtual, o qual também está contemplado pela alteração legislativa.

Alguns exemplos de crimes de interrupção de serviço telemático ou de informação pública:

> Portanto, hoje, no Brasil, é crime a conduta denominada ataque de denegação de serviço (DOS/DDOS). O DOS (*denial of service*[14]) não constitui geralmente uma invasão de sistema alvo, mas uma sobrecarga de acessos que fazem com que o fluxo de dados da rede seja interrompido. É chamado de ataque de denegação de serviço difundido ou DDOS (*distributed denial of service*) quando o criminoso infunde por meio de seu computador (mestre) vulnerabilidades ou programas maliciosos em vários computadores (zumbis), fazendo com que contra a vontade ou mesmo sem que os usuários afetados percebam, acessem simultaneamente ou sequencialmente o serviço que pretende ser travado.

Quanto à equiparação do cartão de crédito como documento particular:

> A nova Lei também equiparou o cartão de crédito ou débito com o documento particular, transformando-os em objetos materiais do crime de falsidade documental. Para a configuração do crime basta que exista a inserção de dados impregnados na tarja magnética (parte juridicamente relevante do documento), que permite o acesso a sistemas bancários ou de crédito pertencentes a determinado correntista, não emitidos pela instituição correspondente. Todavia, somente a conduta de falsificar no todo ou em parte o cartão será considerado crime, o que não ocorre com a simples posse de um cartão clonado por quem não foi responsável pela falsificação. Se utilizado o cartão e alcançado o dano patrimonial, em regra, tratar-se-á de crime de furto qualificado pela fraude e a falsidade será absorvida.

Concluindo os comentários à Lei nº 12.737

> Como visto, a Lei nº 12.737, embora represente certo avanço ao tipificar crimes informáticos próprios, contém inúmeras deficiências e confrontos com o sistema penal e processual penal vigente, a exemplo do que foi trazido no capítulo II desse trabalho, que devem ser delicadamente analisados quando for tratado esse tipo de crime. Os crimes informáticos próprios são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer delitos.
>
> O legislador não contemplou a invasão de sistemas, como os de *clouding computing*[15], por exemplo, optando por restringir o objeto material àquilo que denominou dispositivo informático, sem, contudo, defini-lo.

---

[14] Ataque de denegação de serviço (DOS/DDOS) *(denial of servisse)* é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Alvos típicos são servidores web, e o ataque tenta tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

[15] O conceito de computação em nuvem (em inglês, *cloud computing*) refere-se à utilização da memória e das capacidades de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, seguindo o princípio da computação em grade.

> Atividades de comercialização de *cracking codes*[16] e de engenharia reversa de *software*[17] também não foram objeto da norma.

Por fim, o Centro de Apoio Operacional Criminal do Ministério Público do Estado de São Paulo, conclui com algumas reflexões acerca da nova lei, bem como algumas críticas relevantes:

> Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira. Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a complexidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo).
>
> Em síntese, os tipos e penas da Lei nº 12.737 se mostram carentes de abrangência, no sentido que se trata de uma lei que visa exaurir toda uma atividade criminosa nova. É cristalino o fato de que a internet criou um "universo paralelo" onde inúmeras coisas novas surgem com o passar do tempo. Embora muitas dessas coisas sejam para o benefício e utilidade da sociedade, há que ter em mente que os criminosos também estão criando novas maneiras de cometer crimes e isso o legislador deve levar em consideração ao criar leis para esse fim.

Mesmo tendo sido um avanço e tanto a tipificação de invasão de dispositivos informáticos, muito ainda há que ser feito com relação às atitudes delituosas na internet. Conforme visto anteriormente, muitos crimes comuns na internet não são contemplados pela nossa legislação vigente e, com o surgimento cada dia mais precoce de atitudes ilícitas na internet e nos meios eletrônicos, cada vez mais a sociedade clama por regramentos e possíveis sanções para determinados indivíduos que estão utilizando-se dessas ferramentas para o cometer delitos. Com o objetivo de tornar a legislação mais abrangente, inúmeros projetos de lei vão surgindo na Câmara, todos com o objetivo de estreitar as lacunas legislativas existentes a fim de tipificar e regulamentar as mais variadas situações existentes no meio eletrônico, sobretudo na internet.

---

[16] Um *crack* é um pequeno *software* usado para quebrar um sistema de segurança qualquer. Seu uso mais comum é para transformar programas em versões limitadas, seja em funcionalidade ou tempo de uso, os chamados *shareware*, em um programa completo, removendo ou enganando o sistema de segurança que limita o uso ou verifica o número serial.

[17] A engenharia reversa é o processo de descobrir os princípios tecnológicos e o funcionamento de um dispositivo, objeto ou sistema, através da análise de sua estrutura, função e operação.

4.2. Propostas Legislativas acerca dos Crimes Informáticos

Como visto, com o objetivo de estreitar as lacunas existentes na legislação quanto às atitudes na internet e nos meios eletrônicos, inúmeros projetos de lei surgem na Câmara, alguns sem muita relevância, outros com total importância e abordando temas muito comuns na internet, mas que não possuem uma regulamentação e controle necessários. A exemplo disso temos o projeto de lei n.º 7758/14, do deputado Nelson Marchezan Junior (PSDB-RS), que tipifica penalmente o uso de falsa identidade através da rede mundial de computadores.

Cabe lembrar que o art. 307 do Código Penal já prevê o crime de falsa identidade. Todavia, o projeto de lei visa acrescentar ao art. 307 os perfis falsos encontrados na internet e que tem por objetivo de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio. Nesse sentido, vejamos a atual redação do art. 307 e a respectiva alteração que ocorreria com o projeto de lei:

> Falsa identidade
>
> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem.
>
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

O projeto de lei 7.758/14 prevê o seguinte:

> Art. 1º Esta lei tipifica penalmente o uso de falsa identidade na rede mundial de computadores.
>
> Art. 2º O art. 307 do Decreto-Lei no 2.848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte parágrafo único:
>
> 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.

A respeito do citado projeto de lei, Marcelo Xavier de Freitas Crespo[18] e Coriolano Aurélio de Almeida Camargo Santos[19] tecem comentários no site Migalhas[20]. E assim se manifestam:

> Em primeiro lugar, o projeto como proposto não tem um parágrafo único como menciona o seu art. 2º, mas apenas uma alteração no caput do art. 307 do Código Penal, portanto o próprio projeto fala uma coisa e propõe outra...
>
> Em segundo lugar, a proposta pretende tratar do assunto como se as condutas de criação de perfis falsos nas redes sociais fosse algo que, por ser atividade recente praticada com uso de tecnologia, demandaria intervenção na legislação penal. Vimos acima que isso é um tremendo equívoco.
>
> Em terceiro lugar, o argumento para a necessidade de intervenção penal neste caso é falho porque não faz o menor sentido criar uma figura típica apenas porque determinado crime passou a ser praticado com o auxílio de uma ferramenta tecnológica. Seria como criar um crime específico de homicídio para casos em que houvesse o uso de arma de fogo ou um pedaço de pau! Evidentemente, algumas ferramentas (como a Internet) podem propiciar uma exposição bastante maior da vítima em determinados casos. Mas isso não seria justificativa para a criação de um novo tipo penal e sim de uma figura agravada ou qualificada do delito já existente.

Percebe-se que os autores criticam o projeto de lei no sentido de que não há um novo tipo penal criado pelos perfis falsos na internet, mas sim, uma qualificadora de um tipo penal já existente, o de falsa identidade no art. 307, sendo, portanto, um crime informático impróprio como já visto anteriormente. Quanto à pena já aplicada pelo art. 307, os autores novamente criticam o projeto de lei:

> O projeto se justificaria se fosse uma proposta para aumentar a pena da conduta prevista no art. 307, caso fosse praticado em ambiente da Internet, mas sequer previu pena maior para esta situação. A pena é idêntica à prevista no Código Penal. Então, indaga-se: para que esta mudança? Mais uma mudança que seria absolutamente inócua na prática.

---

[18] Marcelo Xavier de Freitas Crespo é advogado do escritório Crespo & Santos Advogados, especialista em Direito Digital, doutor e mestre pela USP, possui pós-graduação em Segurança da Informação pela Universidade de Salamanca.

[19] Coriolano Aurélio de Almeida Camargo Santos é advogado CEO do escritório Almeida Camargo Advogados, doutor em Direito pela FADISP e mestre em Direito na Sociedade da Informação pela FMU.

[20] Migalhas é um site na internet que publica inúmeros artigos de conteúdo jurídico relevante. A matéria trazida pode ser encontrada no *link:* http://www.migalhas.com.br/dePeso/16,MI213736,81042-Perfis+falsos+nas+redes+sociais+e+o+projeto+de+lei+775814. Acesso em maio/2015.

> Por fim, não fosse isso suficiente, o texto do art. 307, segundo o projeto, passaria a contar com as finalidades especificas de “prejudicar, intimidar, ameaçar”, o que é prejudicial porque “prejudicar” é termo atécnico e vago, e caso seja a intenção de ameaçar, o crime de ameaça já seria imputado a título de concurso de crimes. Intimidar, por fim, é pressuposto da ameaça. Vê-se, portanto, que o projeto não merece prosperar nos termos em que se encontra.

Os autores criticam a criação de um projeto que nada mais seria do que uma redundância legislativa. E, com isso, concluem que:

> Lembramos que em casos de Direito Digital, quase sempre é melhor deixar a legislação como está do que promover alterações pontuais desprovidas de análise contextual, até porque a tecnologia muda muito mais rapidamente que qualquer intervenção legislativa. Sabemos que nossos legisladores são ávidos por alterações pontuais, o que os auxilia a ganhar destaque nas mídias, embora as mudanças propostas representem pouca efetividade em vários casos. Mas isso deve ser evitado.
>
> Em Direito Digital, é preciso parar com as tentativas de invenção da roda e, mais do que nunca, é caso de ouvir especialistas que sejam reconhecidamente autoridades no assunto antes de cometer equívocos ao modificar a legislação.

A respeito do mesmo projeto de lei, a EBC (Empresa Brasil de Comunicação) entrevistou[21] o advogado e professor de Direito Digital, Rafael Maciel, que falou aos ouvintes da Rádio Nacional de Brasília sobre o crime de falsa identidade na internet e de que forma a legislação brasileira lida ou deveria lidar com este tipo de infração no meio digital:

> Rafael Maciel explicou que o crime de falsidade ideológica já está previsto há muitos anos na Constituição Brasileira e que, por esta razão, o projeto de lei que tramita na Câmara é equivocado, uma vez que, segundo ele, o Código Penal não especifica lugares ou ambientes em que o crime tenha que ser cometido para haver punição.
>
> O advogado ressaltou, ainda, que a ideia de inserir expressões como “praticados em ambientes digitais” ou “praticados na internet” nos artigos da legislação brasileira é uma atitude desnecessária. O que se deve fazer, na opinião do também professor de Direito Digital, é apenas punir efetivamente as condutas por meio de investigações, estrutura e aparelhamento judiciário e policial.
>
> Além disso, Rafael Maciel contou que são raros os casos em que o Artigo 307 do Código Penal não alcança os crimes praticados na internet. Os crimes relacionados à invasão de dispositivos informáticos, por exemplo, não eram previstos na legislação e, por esta razão, foi criado um projeto

[21] Entrevista da EBC Rádios disponível em: http://radios.ebc.com.br/revista-brasil/edicao/2015-01/pl-775814-tipifica-penalmente-o-uso-de-falsa-identidade-no-meio. Acesso em maio/2015.

> de lei para punir esse tipo de conduta, a chamada Lei Carolina Dieckmann.

Tendo como base o mesmo pensamento e críticas dos autores anteriormente citados, o entrevistado Rafael Maciel ainda traz um outro ponto muito importante que é o fato de que o Código Penal não especifica lugares ou ambientes que o crime deva ser cometido, dessa maneira, amplia-se a ideia de local e forma de cometimento de crime, abrangendo, também, os perfis falsos contidos na internet e que tem o objetivo obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem, conforme já previsto pelo art. 307.

Há, também, um projeto de lei de autoria da deputada Maria do Rosário (PT-RS), que define crimes de ódio e intolerância. Em matéria publicada no site EcoDebate[22], o texto, publicado pela redação do site, traz algumas considerações acerca desse projeto que visa também coibir discurso de ódio, fabricação e distribuição de conteúdo discriminatório, inclusive pela internet:

> O objetivo é punir a discriminação baseada em classe e origem social, orientação sexual, identidade de gênero, idade, religião, situação de rua, deficiência, condição de migrante, refugiado ou pessoas deslocadas de sua região por catástrofes e conflitos. Quem agredir, matar ou violar a integridade de uma pessoa baseado nesses tipos de preconceito será condenado por crime de ódio e terá a pena do crime principal aumentada em no mínimo 1/6 e no máximo 1/2.
>
> Já o crime de intolerância terá pena de um a seis anos de prisão, além de multa, para quem exercer violência psicológica (*bullying*); negar emprego ou promoção sem justificativa legal; negar acesso a determinados locais ou serviços, como escola, transporte público, hotéis, restaurantes; negar o direito de expressão cultural ou de orientação de gênero; e negar direitos legais ou criar proibições que não são aplicadas para outras pessoas. A exceção a essa regra é o acesso a locais de cultos religiosos, que poderá ser limitado de acordo com a crença.
>
> Para quem praticar, induzir ou incitar a discriminação por meio de discurso de ódio ou pela fabricação e distribuição de conteúdo discriminatório, inclusive pela internet, a pena também será de um a seis anos de prisão, além de multa, e poderá ser aumentada entre 1/6 e 1/2 se a ofensa incitar a prática de crime de ódio ou intolerância.

Levando em consideração inúmeros casos desse tipo que são vivenciados por pessoas todos os dias na internet, é uma proposta muito boa

[22] Projeto de Lei define crimes de ódio e intolerância; Preconceito poderá render pena de até seis anos de prisão. Disponível em http://www.ecodebate.com.br/2014/09/19/projeto-de-lei-define-crimes-de-odio-e-intolerancia-preconceito-podera-render-pena-de-ate-seis-anos-de-prisao/. Acesso em maio/2015

para coibir esse tipo de atitude. Segundo Maria do Rosário, “o caráter abrangente deste projeto de lei tem o objetivo de demonstrar que nenhuma situação de vulnerabilidade pode ser utilizada para justificar ou mascarar violações de direitos humanos”, seria, portanto, mais uma ferramenta que poderia ser utilizada para reprimir atitudes lesivas dos usuários na internet, bem como, na sociedade como um todo.

Existe, também, um Projeto de Lei do Senado que tramita há oito anos. O projeto, PLS 236/2012, foi apresentado pelo senador José Sarney e, em que pese as inúmeras críticas que recebeu, traz consigo um título que seria especificamente sobre crimes informáticos. O Título IV[23] do “Novo Código Penal” teria a seguinte redação:

> PARTE ESPECIAL
>
> TÍTULO VI
>
> DOS CRIMES CIBERNÉTICOS
>
> **Conceitos**
>
> Art. 213. Para efeitos penais, considera-se:
>
> I – “sistema informatizado”: computador ou qualquer dispositivo ou conjunto de dispositivos, interligados ou associados, em que um ou mais de um entre eles desenvolve o tratamento automatizado de dados informatizados através da execução de programas de computador, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informatizados armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos;
>
> II – “dados informatizados”: qualquer representação de fatos, informações ou conceitos sob forma suscetível de processamento num sistema informatizado, incluindo programas de computador;
>
> III – “provedor de serviços”: qualquer entidade, pública ou privada, que faculte aos utilizadores de seus serviços a capacidade de comunicação por meio de seu sistema informatizado, bem como qualquer outra entidade que trate ou armazene dados informatizados em nome desse serviço de comunicação ou de seus utentes;
>
> IV – “dados de tráfego”: dados informatizados relacionados com uma comunicação efetuada por meio de um sistema informatizado, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente;

[23] Texto retirado do relatório do senador Pedro Taques (PDT-MT), que foi o revisor do projeto, conjuntamente com várias juristas e que teve seu relatório publicado no link http://www.pedrotaquesmt.com.br/uploads/downloads/Relatorio-do-senador-Pedro-Taques-ao-Novo-Codigo-Penal.pdf. Acesso em maio/2015

V – “artefato malicioso”: sistema informatizado, programa ou endereço localizador de acesso a sistema informatizado destinados a permitir acessos não autorizados, fraudes, sabotagens, exploração de vulnerabilidades ou a propagação de si próprio ou de outro artefato malicioso;

VI – “credencial de acesso”: dados informatizados, informações ou características individuais que autorizam o acesso de uma pessoa a um sistema informatizado.

Acesso indevido

Art. 214. Acessar, indevidamente, por qualquer meio, direto ou indireto, sistema informatizado:

Pena – prisão, de um a dois anos.

Acesso indevido qualificado

§1º Se do acesso resultar:

I – prejuízo econômico;

II – obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, arquivos, senhas, informações ou outros documentos ou dados privados;

III – controle remoto não autorizado do dispositivo acessado: Pena – prisão, de um a quatro anos.

§2º Se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos:

Pena – prisão, de dois a quatro anos.

Causa de aumento de pena

§3º Nas hipóteses dos §§ 1º e 2º, aumenta-se a pena de um a dois terços se houver a divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados, arquivos, senhas ou informações obtidas, se o fato não constituir crime mais grave.

Ação penal

§4º Somente se procede mediante representação, salvo na hipótese do § 2º deste artigo.

Sabotagem informática

Art. 215. Interferir sem autorização do titular ou sem permissão legal, de qualquer forma, na funcionalidade de sistema informatizado ou de comunicação de dados informatizados, causando-lhes entrave, impedimento, interrupção ou perturbação grave, ainda, que parcial:

Pena – prisão, de um a quatro anos.

§1º Na mesma pena incorre quem, sem autorização ou indevidamente, produz, mantém, vende, obtém, importa ou por qualquer outra forma distribui códigos de acesso, dados informáticos ou programas, destinados a produzir a ação descrita no caput.

§2º A pena é aumentada de um a dois terços se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos: Pena – prisão, de dois a quatro anos.

Dano a dados informatizados

Art. 216. Destruir, danificar, deteriorar, inutilizar, apagar, modificar, suprimir ou, de qualquer outra forma, interferir, sem autorização do titular ou sem permissão legal, dados informatizados, ainda que parcialmente:

Pena – prisão de um a três anos.

Parágrafo único. Aumenta-se a pena de um a dois terços se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos.

Fraude informatizada

Art. 217. Obter, para si ou para outrem, em prejuízo alheio, vantagem ilícita, mediante a introdução, alteração ou supressão de dados informatizados, ou interferência indevida, por qualquer outra forma, no funcionamento de sistema informatizado:

Pena – de prisão, de um a cinco anos.

Parágrafo único. A pena aumenta-se de um terço se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

Obtenção indevida de credenciais de acesso

Art. 218. Adquirir, obter ou receber, indevidamente, por qualquer forma, credenciais de acesso a sistema informatizado:

Pena – prisão, de um a três anos.

Parágrafo único. Aumenta-se a pena de um a dois terços se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos.

Artefato malicioso

Art. 219. Constitui crime produzir, adquirir, obter, vender, manter, possuir ou por qualquer forma distribuir, sem autorização, artefatos maliciosos destinados à prática de crimes previstos neste Título, cuja pena será a prevista para o crime fim, sem prejuízo da aplicação das regras do concurso material.

Excludente de ilicitude

Parágrafo único. Não são puníveis as condutas descritas no caput quando realizadas para fins de:

I – investigação por agentes públicos no exercício de suas funções;

II - pesquisa acadêmica;

III – testes e verificações autorizadas de vulnerabilidades de sistemas; ou

> IV – desenvolvimento, manutenção e investigação visando o aperfeiçoamento de sistemas de segurança.

O Título IV teve seu texto comentado por um blog[24] e, segundo o autor, o blog "Garoa Hacker Clube" teve todas as sugestões feitas acolhidas no parecer do senador Pedro Taques:

> É importante ressaltar que o Senador Pedro Taques submeteu o projeto para diversas entidades especializadas, e o capítulo sobre crimes cibernéticos foi avaliado também pelo Ministério Público Federal, que tem um grupo especializado em crimes cibernéticos, que é baseado em São Paulo. O Garoa Hacker Clube, através do Alberto Fabiano, ajudou o pessoal do MPF nesse trabalho de revisão, e as sugestões foram incorporadas ao projeto, incluindo as definições no início da lei e a questão de exclusão de licitude no artigo sobre artefatos maliciosos.

O senador Pedro Taques, em seu relatório, ao avaliar o Título IV que trata dos crimes informáticos, assim se manifestou:

> Embora o CP, em regra, não seja diploma que traga conceitos, no caso de crimes cibernéticos, em razão dos aspectos técnicos envolvidos e o pouco conhecimento popular, entendemos ser essencial o estabelecimento de conceitos básicos, de modo a orientar a posterior interpretação, assim como diligentemente fez a Comissão de Juristas. Um Código não é escrito apenas para os operadores do Direito, mas para a sociedade como um todo. O art. 208 do Projeto traz os mesmos conceitos da Convenção de Budapeste, de 2004. A nossa proposta traz conceitos semelhantes, de modo a facilitar eventuais pedidos de cooperação internacional, mas inclui outros termos e conceitos mais modernos, suprindo lacunas já percebidas e criticadas em países que aderiram à Convenção.

Quanto ao art. 209 trazido pelo Título dos "Crimes Cibernéticos", o senador assim se posicionou:

> No art. 209, pune-se o acesso indevido. Hoje, há artigo semelhante em vigor, introduzido pela Lei nº 12.737, de 2012 (art. 154-A do CP). A redação do Projeto é melhor, porque fala em "acesso" e não em "invasão". Além disso, o art. 154-A exige dolo específico – finalidade de destruir, adulterar ou obter dados ou instalar vulnerabilidade para obter vantagem indevida. O art. 209 não exige essa finalidade. A redação do Projeto exige, contudo, que o sistema informático seja "protegido". Tecnicamente, não faz diferença alguma se o sistema é ou não protegido. O desvalor reside no tipo de acesso, se devido ou indevido. A redação do art. 209 ainda traz o problema da "porta aberta" – o tipo exige que, do

[24] Com a alcunha "Anchises" o autor do blog publicou um texto relatando a respeito do Título IV do PLS 236/2012. Disponível em http://anchisesbr.blogspot.com.br/2013/09/seguranca-nova-lei-dos-crimes.html. Acesso maio/2015.

> acesso, resulte exposição a risco de divulgação. Não sabemos como isso operaria na prática. Sugerimos retirar essa expressão, que pouco agrega.

Segue o senador em seu relatório, agora falando dos parágrafos que já são contemplados pela Lei 12737/12:

> O § 2º foi deslocado de lugar. O § 3º reproduz o § 3º do artigo 154-A em vigor, o qual, oportuno acrescentar, esqueceu de punir também a pessoa que obtém dados privados que não sejam comunicações eletrônicas ou segredos industriais. Por isso, sugerimos a melhor organização do artigo. A sugestão também é de um maior intervalo entre as penas mínimas e máximas, permitindo a melhor adequação e individualização no caso concreto. Os §§ 1º e 2º do art. 153 do CP punem a divulgação de segredos contidos em sistemas de dados e qualificam a conduta se o banco de dados for de órgão público. As penas neles trazidas são bem maiores do que as do §§ 4º e 5º do art. 209, que punem aquele que acessa indevidamente e depois divulga as informações obtidas. A sugestão, aqui, é de readequação das penas, de modo que a conduta mais grave (acesso indevido, obtenção mais divulgação) seja punida de forma adequada. Por fim, o § 5º do Projeto (§ 2º na nossa proposta) é melhor do que o § 5º do art. 154-A do CP, que prevê causa de aumento se o crime é praticado contra determinadas pessoas. A proteção da Administração Pública parece ser mais adequada.

Por fim, o senador fala sobre a proposta ter a criação de tipos penais:

> Propomos outros dois tipos penais. Primeiro, é necessária a punição da obtenção de credenciais, como senhas e impressões digitais, hoje utilizadas quase como documentos de identificação. Documentos servem para identificar pessoas no mundo real e credenciais no mundo virtual. Isso também é importante no caso mais comum de fraude bancária – atualmente, os e-mails trazem links que redirecionam para páginas falsas de bancos, onde são colhidas as informações a serem usadas posteriormente. Essa situação não é coberta por nenhum artigo (pois não há vírus, não há invasão). Daí a importância de se punir a obtenção, e, em outro artigo, o programador que faz o artefato. Entendemos ser mais adequada e didática a reunião de todas as condutas do programador em um único artigo, com referência secundária aos demais, para evitar repetições. Foi incluída a excludente para evitar a punição de pesquisadores e desenvolvedores que trabalham para a criação de novas tecnologias de segurança e também das empresas que investigam os artefatos para aperfeiçoamento dos sistemas de segurança. Por fim, suprimimos o art. 211 do Projeto, em razão da dificuldade de processamento por ação penal privada. Algumas condutas descritas no Título poderiam gerar milhares de ações individuais, em vários estados da Federação, em razão da difusão dos danos decorrentes da ação criminosa.

Alvo de inúmeras críticas, o PLS 236/2012, está há oito anos em análise pelo senado e, levando em consideração a complexidade da matéria, já que visa uma reforma completa no Código Penal, seja suprimindo algumas condutas, seja criando novos tipos penais, não é de se admirar que ainda esteja em análise e

apresente pontos negativos. Todavia, a iniciativa de se modificar o Código Penal deve ser considerada, uma vez que é datado de 1940, inúmeras novas condutas, sobretudo na internet, surgiram e colocaram a prova a abrangência e o caráter protetivo de nosso Código. Variadas são as iniciativas legislativas acerca de condutas lesivas tanto na internet, quanto nos meios eletrônicos, mas vale lembrar o que disseram Marcelo Xavier de Freitas Crespo e Coriolano Aurélio de Almeida Camargo Santos, “(...), é preciso parar com as tentativas de invenção da roda e, mais do que nunca, é caso de ouvir especialistas que sejam reconhecidamente autoridades no assunto antes de cometer equívocos ao modificar a legislação. ”

Vê-se, portanto, a necessidade de uma legislação que acompanhe o avanço exacerbado da sociedade, todavia, deve haver todo um acompanhamento técnico da matéria a ser proposta em legislação, sob pena de se tornar carente e redundante, sem a mínima eficácia, criando lacunas legislativas onde se escondem os agentes criminosos e onde a justiça não pode atuar.

5. Conclusão

A informação antes transmitida pela fala, gestos, sinais, hoje é transmitida por veículos mais rápidos, a exemplo da televisão, rádio e a internet. Acontecimentos do outro lado do mundo tem a sua notícia espalhada quase que instantaneamente por meio da internet. Os sistemas informáticos, outrora coadjuvantes das atividades humanas, assumem papel imprescindível na vida da sociedade moderna. Controlar quem e como é utilizada a informação nesta gigantesca rede é tarefa que se torna cada vez mais onerosa.

Acreditava-se que para o cometimento de alguma atividade ilícita na internet era necessário um vasto conhecimento técnico na área da informática. Percebe-se que o mais simples usuário pode se valer de uma vantagem ilícita e, dessa forma, ludibriar outro usuário e conseguir a informação que necessita. A informatização da sociedade teve como consequência esse tipo de facilidade. Todavia, mesmo um simples usuário pode criar uma situação tão complexa que o direito penal deverá estar preparado para abarcar e, assim, penalizar atividades lesivas. O Direito e a legislação devem tentar ser, se não mais rápidos, paralelamente evolutivos com a informatização, do contrário, as consequências por não conseguir acompanhar essa constante evolução poderá acarretar em situações irreversíveis. O que se percebe na tentativa legislativa para essa matéria é a inexperiência do legislador, porém, a sua iniciativa em tentar controlar esse universo deve ser considerada.

Percebe-se, portanto, a necessidade de criação de normas flexíveis, adequáveis a essa diversidade de possibilidades encontradas pelos criminosos. Muito embora a legislação brasileira tenha dado um salto gigantesco com a criação da lei que regula invasão de dispositivos, alterando o Código Penal, bem como o Marco Civil da internet que tem por objetivo o de estabelecer princípios, garantias e deveres para o uso da internet no Brasil, muito ainda deve ser feito, sobretudo com relação à matéria penal, para que a norma se adeque e acompanhe o surgimento de tipos penais, assim, estabelecendo sanções às condutas danosas e suprindo todas as lacunas existentes em nosso ordenamento.

6. Bibliografia

ANDREUCCI, Ricardo Antônio. *Legislação Penal e Especial*, 7ª ed., São Paulo: Saraiva, 2010.

BITENCOURT, Cezar Roberto, *Tratado de Direito Penal* – Parte Especial. São Paulo: Saraiva, 2003. V. 3.

BORGES, Abimael. Lei Carolina Dieckmann – Lei nº 12.737/12, art. 154-A do Código Penal. 2014. Disponível em: http://jusbrasil.com.br. Acesso em: mar. 2015.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. 1988. Disponível em: http://www.senado.gov.br. Acesso em: fev. 2015.

_____, Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. 1940. Disponível em: http://www.senado.gov.br. Acesso em: fev. 2015.

_____, Decreto-Lei nº 3.689, de 2 de outubro de 1941. Código de Processo Penal. 1941. Disponível em: http://www.senado.gov.br. Acesso em: fev. 2015.

_____, 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. 2012. Disponível em: http://www.senado.gov.br. Acesso em: fev. 2015.

_____, Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2014. Disponível em: http://www.senado.gov.br. Acesso em: fev. 2015.

_____, Poder Judiciário de Santa Catarina. Jurisprudência. Disponível em: http://www.tjsc.jus.br. Acesso em: mar. 2015.

_____, Poder Judiciário do Rio Grande do Sul. Jurisprudência. Disponível em: http://www.tjrs.jus.br. Acesso em: mar. 2015.

_____, Senado Federal. Textos e Relatórios. Disponível em: http://www.senado.gov.br. Acesso em mai. 2015.

_____, Superior Tribunal de Justiça. Jurisprudência. Disponível em: http://www.stj.jus.br. Acesso em: mar. 2015.

_____, Tribunal Regional Federal 4ª Região. Jurisprudência. Disponível em: http://www.trf4.gov.br. Acesso em: abr. 2015.

CABETTE, Eduardo. Novos artigos no Código Penal. Disponível em: http://atualidadesdodireito.com.br. Acesso em: abr. 2015.

CAPEZ, Fernando. *Curso de Processo Penal*. 2ª ed., São Paulo: Saraiva, 1998.

_____, *Curso de Processo Penal*. 13ª ed., São Paulo: Saraiva, 2006.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2ª ed., Rio de Janeiro: Lumen Juris, 2003.

COELHO, Rodrigo Durão. Fraude online cresce e vira epidemia mundial. Disponível em: http://terra.com.br. Acesso em: mar. 2015.

CORRÊA, Gustavo Testa. A questão da tributação na internet. In: ROVER, Aires José (Org.). *Direito, sociedade e informática: limites e perspectivas da vida digital.* Florianópolis: Boiteaux. 2000b.

COSTA, Marcos Aurélio Rodrigues da. Crimes de informática. *Jus Navigandi.* 1997. Disponível em http://www.jus.com.br. Apud PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. *IBCCrim*, São Paulo, ano 8, v.101, abr. 2001.

COSTA JÚNIOR, Paulo José da. *Direito Penal* – Curso completo. 5ª ed., São Paulo: Saraiva, 1999.

CRETELLA JÚNIOR, José. *Comentários à Constituição Brasileira de 1988*. Rio de Janeiro: Forense Universitária, 1988, v. 1.

DELMANTO, Celso. Código Penal Comentado. 6ª ed. atual. e ampl., Rio de Janeiro: Renovar, 2002.

ESTEFAM, André*. Direito Penal: Parte Especial* (arts. 121 a 183). v. 2, São Paulo: Saraiva, 2010.

FERRACINI, Luiz Alberto. *Do Crime de Estelionato e outras Falcatruas*. São Paulo: LED, 1996.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.) *Direito & Internet: Aspectos Jurídicos Relevantes*. Bauru: Edipro, 2000.

FRAGOSO, Heleno Cláudio. *Lições de Direito Penal: Parte Especial*. 6ª ed., Rio de Janeiro: Forense, 1989. vol. II.

FURLANETO NETO, Mario. *Crimes na internet e inquérito policial eletrônico* / Mario Furlaneto Neto, José Eduardo Lourenço dos Santos, Eron Veríssimo Gimenes – São Paulo: EDIPRO, 1ª ed., 2012.

GAGLIARDI, Pedro Luiz Ricardo. Crimes cometidos com o uso de computador. São Paulo, 1994. 137 f. Tese (Doutorado em Direito Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo.

GLOBO, Portal de Notícias. Disponível em: http://www.globo.com. Acesso em: abr. 2015.

GOMES, Luiz Flávio. Crimes informáticos. 10 dez. 2000. Disponível em http://www.ibccrim.org.br. Acesso em: abr. 2015.

GRINOVER, Ada Pelegrini. *Novas Tendências no Direito Processual*. Rio de Janeiro: Forense Universitária, 1990.

INELLAS, Gabriel César Zaccaria de. *Crimes na Internet*. São Paulo: Juarez de Oliveira, 2004.

JESUS, Damásio Evangelista de. *Direito Penal – Parte Geral*. São Paulo: Saraiva, 1993ª.

_____, *Direito Penal – Parte Especial.* 28ª ed., São Paulo: Saraiva, 2º vol., 2007.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. Campinas: Millennium, 2006.

LYRA, Romero. O combate à pedofilia na internet. Disponível em: http://www.direitonaweb.com.br. Acesso em: abr. 2015.

MARQUES, José Frederico. Tratado de Direito Penal. Campinas: Bookseller, vol. II, 1997ª.

MIGALHAS, *site. Perfis falsos nas redes sociais e o projeto de lei 7.758/14, por Marcelo Xavier de Freitas Crespo e Coriolano Aurélio de Almeida Camargo Santos.* Disponível em: http://www.migalhas.com.br. Acesso em mai. 2015.

MIRABETE, Julio Fabrini. *Processo Penal*. 18ª ed., São Paulo: Atlas, 2006.

NUCCI, Guilherme de Souza. *Código Penal Comentado*. 4ª ed., rev., atual. e ampl., São Paulo: Revista dos Tribunais, 2003.

_____, *Código de Processo Penal Comentado*, 6ª ed., São Paulo: Revista dos Tribunais, 2007b.

_____, *Manual de Direito Penal: Parte Geral: Parte Especial*. São Paulo: Revista dos Tribunais, 2005.

PAESANI, Liliana Minardi. *Direito e internet: liberdade de informação, privacidade e responsabilidade civil*. São Paulo: Atlas, 2000.

PIERANGELI, José Henrique. *Manual de Direito Penal Brasileiro: Parte Especial* (arts. 121 a 234). São Paulo: Revista dos Tribunais, 2005.

PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. *IBCCRM*, São Paulo, ano 8, v. 101, abr. 2001.

PRADO, Luiz Regis. *Curso de Direito Penal Brasileiro: Parte Especial*. 2ª ed., São Paulo: Revista dos Tribunais, v. 2, 2002.

ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. *Caderno Jurídico*, São Paulo, ano 2, nº 4, jul. 2002.

SILVA, De Plácido e. *Vocabulário Jurídico*. 8ª ed., Rio de Janeiro: Forense, v. III, 1984.

TAQUES, Pedro. Senador da República. *Relatório do Novo Código Penal.* Disponível em: http://www.pedrotaquesmt.com.br. Acesso em mai. 2015.

VIANNA, Túlio Lima. Dos crimes pela internet. *Revista do Caap*, Belo Horizonte, v. 9, 2000. Apud INELLAS, Gabriel César Zaccariade. Crimes na Internet. São Paulo: Juarez de Oliveira. 2004.

ZAFFARONI, Eugenio Raúl, PIERANGELI, José Henrique. Manual de Direito Penal Brasileiro: Parte Geral. 3ª ed., São Paulo: Revista dos Tribunais, 2001.

ZANELLATO, Marco Antônio. Condutas ilícitas na sociedade digital. *Caderno Jurídico*, São Paulo, ano 2002, nº 4, jul. 2002.