ETIC 2015 - Encontro de Iniciação Científica
ISSN 21-76-8498

CRIMES CIBERNÉTICOS: UMA ABORDAGEM JURÍDICA SOBRE OS CRIMES REALIZADOS NO ÂMBITO VIRTUAL

Gabriel Marcos Archanjo ORRIGO[1]
Matheus Henrique Balego FILGUEIRA[2]

RESUMO: O presente artigo é um estudo sobre crimes cibernéticos, não visa esgotar o tema, mas sim, levar ao leitor uma visão de conhecimento geral em relação a tais crimes. O trabalho é iniciado mostrando a evolução do computador e da internet, desde as respectivas criações até os dias atuais, com dados e informações históricas. Em seguida, expõe a classificação dos crimes cibernéticos e define quem são e as características dos sujeitos do delito, inclusive com exemplos. Posteriormente realiza uma análise de como definir a competência de quem processará e julgará os crimes e, por fim, traz uma análise, artigo por artigo, sobre a Lei 12.737/12, que teve o objetivo de atualizar a legislação penal brasileira no tocante aos crimes cometidos no mundo virtual.

Palavras-chave: Crimes cibernéticos. Internet. Hacker. Conexão. Aparelhos tecnológicos. Computador.

1. INTRODUÇÃO

Na última década a informática passou a fazer parte do cotidiano de grande parte da população mundial e no Brasil isso não é diferente. A velocidade com que criam e reinventam novas tecnologias eletrônicas é impressionante. A cada ano, aparelhos eletrônicos que eram tidos como novos se tornam defasados em questão de meses.

Toda essa velocidade resultou em um avanço tecnológico que era inimaginável até o começo dos anos 2000. Hoje, computadores, celulares, tablets e smatphones, estão todos conectados a internet quase 24 horas por dia e nas mãos da maioria da população mundial.

Os benefícios da tecnologia são indiscutíveis, encurtou fronteiras, proporcionou maior avanço em todos os setores de produção e leva quase que instantaneamente notícias para todo o mundo.

[1] Discente do 3º ano do curso de Direito do Centro Universitário "Antonio Eufrásio de Toledo" de Presidente Prudente. E-mail, gabrielorrigo@muthcorretora.com.br
[2] Discente do 3º ano do curso de Direito do Centro Universitário "Antonio Eufrásio de Toledo" de Presidente Prudente. E-mail, filgueiramatheus@hotmail.com

A internet é de fato uma maravilha tecnológica, porém atrás de todo o avanço e facilidades alcançadas através dela existem incontáveis tipos de crimes cometidos com o auxílio de aparelhos eletrônicos conectados a ela.

À vista disso, o trabalho abordou o surgimento do computador desde a sua polêmica criação até o surgimento da inteligência artificial e as máquinas que conhecemos hoje. Abordou da mesma forma a internet passando por suas fases, seu início no Brasil durante os anos de 1988 até os dias atuais.

Posteriormente, classificou os crimes cibernéticos em próprios e impróprios, expôs os sujeitos ativos e passivos do delito, evidenciando suas peculiaridades, a diferença de Hacker e Cracker e como qualquer pessoa pode praticar um crime virtual.

Ainda em um âmbito estritamente jurídico, delimitou-se o caminho para se indicar qual a competência para processar e julgar o delito, quando será da Justiça Federal ou Estadual, e em qual foro se realizar. Por fim, fez uma análise meticulosa da lei 12.737/12, mais conhecida como Lei Carolina Dieckmann, que introduziu os artigos 154-A e 154-B ao Código Penal Brasileiro e ainda alterou os artigos 266 e 298 do mesmo código.

Para a elaboração do artigo, foi utilizado o método bibliográfico, com o levantamento de dados de livros especializados, artigos científicos, jurisprudência e monografias, sempre possuindo o intuito de passar o conhecimento da melhor forma.

2. Histórica do computador

O primeiro computador, nos moldes dos que conhecemos hoje, tem sua origem ainda discutida, por alguns o criador da máquina foi Howard W. Aiken, outros afirmam que foi Atasanoff e Berry. Respectivamente nos anos de 1937 e 1940, estes anos foram o auge da 2º Guerra Mundial, onde se buscava novas ferramentas para que com menos esforço fosse possível expandir os limites conhecidos e assim aumentar as possibilidades de armazenamento de informações e materialização de ideias.

O que historiadores concordam é que existem cinco gerações de computadores.

A primeira, entre os anos de 1940 e 1952, onde o uso de computadores era restrito aos militares e os computadores funcionavam à base de válvulas a vácuo. Já aqui o direito, através do advogado americano, Lee Loevinger, viu possível utilidade nas maquinas para facilitar a prática jurídica (cabe salientar que, era a colaboração do computador nas atividades jurídicas e não uma ciência jurídica voltada para computação);

A 2ª geração, entre 1952 e 1964, visando dar maior agilidade substituiu as válvulas por transistores, e ainda, neste período, o computador passou de uso exclusivamente militar para também uso de civis, no âmbito administrativo/gerencial;

A 3ª geração teve início em 1964 e foi até 1971 com o surgimento dos circuitos integrados, em decorrência disto a substituição dos antigos transistores por eles. Teve como principal avanço a diminuição do tamanho das máquinas, a evolução dos softwares e criação de chips de memória, dando surgimento assim, aos microcomputadores;

A 4ª geração se desenvolveu durante a próxima década, entre 1971 e 1981, esta substituiu os circuitos pelos até hoje utilizados microprocessadores, houve criação dos disquetes e em consequência o aumento na capacidade no armazenamento de dados, o que tornou possível a criação de máquinas de grande porte;

Finalmente chegamos a 5ª geração que teve inicio em 1981 e segue até os dias atuais, nela ocorreram incontáveis avanços como, a criação de inteligência artificial, o processamento de dados em alta velocidade e o que possui maior relevância para os meios de comunicação da história recente: a internet.

3. História Da Internet

A internet é a rede mundial de computadores, onde através de um provedor ou portal, pessoas podem se comunicar e trocar informações de qualquer lugar do mundo. A internet que conhecemos hoje surgiu durante a Guerra Fria, mais uma vez como aconteceu com algumas das grandes invenções da humanidade,

surgiu para fins militares. Os cientistas a desenvolveram para que mesmo sobre ataque, caso uma de suas bases fossem destruídas, as demais conseguissem manter contato entre si, uma vez que os dados não estariam fixos em uma única base e sim na rede, hoje conhecida como “nuvem”. Num exemplo, se a base B fosse destruída A e C ainda estariam em contato.

Em 1969 ocorreu a interligação entre 4 (quatro) maquinas em universidades distintas dos EUA. No ano de 1971 a rede já abrangia órgãos militares e do governo americano. Em 1972 foi criado um correio eletrônico interligando os EUA o Reino Unido e a Noruega, conhecido como e-mail.

O mundo nas próximas duas décadas deu um salto tecnológico considerável em relação à internet. Porém o Brasil só tomou conhecimento da internet em 1988, por iniciativa da Fundação de Amparo Pesquisa do Estado de São Paulo (FAPESP), Universidade Federal do Rio de Janeiro (UFRJ) e Laboratório Nacional de Computação Cientifica (LNCC).

O ministério de ciências e tecnologia em conjunto com o ministério da educação em 1990 criou o Backbone, que é a rede nacional de pesquisas que interligava 11 (onze) estados. No ano de 2013, o Brasil já acumulava mais de 83 milhões de internautas, segundo o IBGE (Instituto Brasileiro de Geografia e Estatística).

A internet não possui nenhum órgão governamental que a regule, e chega ao mundo todo pelo TCP/IP que permite a comunicação entre aparelhos eletrônicos. Em novembro de 2001 após os ataques do 11 de setembro, a comunidade europeia criou uma convenção com a intenção de estabelecer pilares sobre direito material processual e tipos sobre crimes da internet para que entre os signatários tenha um padrão para julgar e controlar delitos cometidos na rede, uma vez que a internet não possui fronteiras. Isto é o mais próximo que há de uma legislação em âmbito mundial sobre a internet.

4. Classificação dos crimes cibernéticos

Existem várias classificações doutrinarias sobre a natureza jurídica dos crimes cibernéticos. Adotaremos, neste artigo, a vertente que divide os crimes em: crimes cibernéticos próprios e impróprios.

Os crimes cibernéticos próprios são aqueles em que o agente, para cometer um delito, necessita do computador, ou seja, o computador é o meio de execução essencial. Os bens jurídicos afetados, pelos crimes cibernéticos próprios são os dados armazenados em outra máquina ou rede.

O delito é cometido por meio do computador e se consuma também pelo meio informático. Na nossa legislação um exemplo é a Invasão de Dispositivo Informático

Já os crimes cibernéticos impróprios, também são cometidos por meio do computador, porém o bem jurídico ofendido aqui pode ser afetado de “n” maneiras, não necessariamente com a utilização do computador, ou seja, não é essencial a máquina, o delito atinge o mundo físico, diverso da informática.

São exemplos de crimes impróprios tipificados na nossa legislação: Calúnia; injúria; difamação; ameaça; furto; apropriação indébita; estelionato; dano; violação ao direito autoral; pedofilia; crime contra a propriedade intelectual;

Observe que todos eles podem ser cometidos sem o uso do computador, mas também é possível comete-los usando o computador como meio.

5. Sujeitos do crime

Em relação ao sujeito ativo é um crime comum quanto ao agente e estes podem ter diversos níveis de periculosidade, podem ser uma pessoa comum sem grandes conhecimentos técnicos sobre informática, programação e internet, como também, podem ser uma pessoa com conhecimento técnico aprofundado.

Por exemplo, uma pessoa que divulga foto íntima de outra, sem autorização em uma rede social, causando assim uma ofensa à honra, é um sujeito ativo de crime cibernético de natureza impróprio. Já alguns crimes cometidos por meio de computadores, exigem uma condição mais específica do agente, que é o conhecimento técnico, tais crimes podem atingir inúmeros bens jurídicos e de extrema importância. Em um comunicado no ano de 2014, após um ataque de invasão aos dados da empresa americana Sony Pictures, Kevin Mandia, especialista em segurança cibernética, disse: “O malware era indetectável por programas antivírus comuns na indústria, e destruidor o suficiente para fazer com que o FBI emitisse um alerta para outras organizações sobre a ameaça.”. Desta afirmação é

possível dimensionar o que ataques cibernéticos podem gerar, desde crimes comuns contra a honra ou até se infiltrar em Estados e grandes Corporações.

Estes últimos sujeitos ativos descritos, são comumente chamados “hackers”. Porém é preciso separar “Hackers” de “Crackers”, os Hackers utilizam de seus conhecimentos técnicos para ações lícitas enquanto os intitulados Crackers (nome criado pelos próprios Hackers para distingui-los de especialistas que possuem condutas ilícitas), são as pessoas com conhecimentos e habilidades equivalentes aos dos Hackers, porém com fins ilícitos.

A identificação desses agentes é dada pelo endereço de IP (Internet Protocol é um número que o computador -ou roteador- recebe quando se conecta a Internet. É através desse número que o computador é identificado e pode enviar e receber dados), é como se fosse uma identidade virtual. Essa identificação, por vezes é problemática, pois os provedores não guardam tais informações por muito tempo e ainda dependem de autorização judicial para divulgá-las, além de que é possível camuflá-los ou alterá-los com facilidade com o devido conhecimento técnico.

Independente da identificação, o sujeito ativo dos crimes é sempre quem, fazendo o uso de sua inteligência acessa outras máquinas com intuito de cometer delitos, ou mesmo, quem sem um conhecimento tão avançado, como os Hackers e Crackers, fazem uso da internet para cometer delitos.

O sujeito passivo é uma figura mais fácil de descrever, pode ser qualquer indivíduo que tenha um bem jurídico lesado ou ameaçado de lesão por ações através do computador. Pode ser tanto a Pessoa Física quanto Pessoa Jurídica.

6. Competência

O senso comum pode imaginar que por se tratar de crimes praticados por meio de computadores e internet, a competência para processar e julgar é da Justiça Federal, porém, tal pensamento é equivocado.

Para que se firme a competência é necessário observar a territorialidade do delito, mais especificamente, os elementos de internacionalidade, ou seja, o crime será julgado pela Justiça Federal caso ultrapasse as fronteiras do

Estado Brasileiro, seja dando publicidade ao delito em outros países ou afetando diretamente bens jurídicos em outros países e, além disso, que os países estrangeiros sejam signatários de tratados internacionais, de acordo com nossa Constituição Federal em seu artigo 109.

Caso não seja demonstrado às circunstancias anteriores, de forma subsidiária a Justiça Estadual será competente para apurar o crime cibernético.

Todas as regras de territorialidade são respeitadas, portanto os delitos serão julgados onde se consumaram o que é, onde o bem jurídico foi afetado. O STJ nos crimes contra a honra abre uma exceção firmando que a competência será o local do Provedor que hospedou o ato ilícito.

7. Lei 12.737/12

A situação da nossa legislação penal é defasada em relação a crimes cibernéticos, porém em contramão a isso, no ano de 2012, após um crime contra a honra, cometido por meio da internet, ter sido levado a público em razão de a vítima ser uma famosa atriz brasileira (que posteriormente veio dar o nome a lei), foi regulamentada a Lei mais recente em nosso ordenamento referente a crimes cibernéticos. A lei é 12.737/12, mais conhecida como Lei Carolina Dieckmann.

O legislador teve como 'mens legis' atualizar e incluir algumas situações no nosso ordenamento jurídico. Através da lei foram introduzidos os artigos 154-A e 154-B e alterados os artigos 266 e 298 do Código Penal.

O artigo 154-A do Código Penal possui a seguinte redação:

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

O objeto jurídico tutelado por esse artigo é a proteção do direito constitucional à intimidade. O ilícito consiste em invadir um sistema pessoal, particular da vítima e obter, alterar ou danificar, informações contidas ali. O legislador foi inteligente ao usar a expressão “dispositivo informático”, assim não se limitando a computadores, abrangendo aparelhos celulares, smartphones, tablets, etc.

Em resumo este novo artigo, tem o objetivo de proteger dados pessoais conectados ou não a internet de agentes que tenham intenções inidôneas e punir não somente quem de fato cometeu a invasão, mas também quem facilitou o delito, através da criação de programas ou dispositivos informáticos e ainda um agente que difunda as informações particulares.

Em seguida o artigo 154-B, dispõe:

“Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos”

Esta segunda inclusão, veio definir que os delitos do art.154-A estão condicionados à ação penal pública mediante representação, salvo nos casos de o Sujeito Passivo é a Administração Publica, neste caso a ação penal será pública incondicionada.

Além das duas inclusões acima, a lei modificou a redação do artigo 266 do código penal, que hoje está redigido desta forma:

“ Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

§ 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012)

§ 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012) “

A lei 12.737/12 ampliou o alcance deste artigo passando a tutelar a interrupção dos serviços telemáticos ou informação de utilidade pública.

Se no artigo 266 a alteração já era sutil, no artigo 298 é aparentemente menor, porém de conteúdo ainda mais relevante, segue a redação do artigo:

"Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
Pena - reclusão, de um a cinco anos, e multa.
Falsificação de cartão (Incluído pela Lei nº 12.737, de 2012) Vigência
Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012)"

O legislador aqui acabou com uma discussão que existia na doutrina e jurisprudência sobre a natureza do cartão bancário com a inclusão do parágrafo único, afirmando que o cartão bancário de crédito ou débito é documento particular. A alteração é mais sentida no âmbito dos crimes monetários, porém se estende aos crimes cibernéticos, no tocante ao roubo de dados de cartões bancários na internet e sua utilização indevida.

8. CONCLUSÃO

Diante do exposto, é possível aferir que o computador surgiu durando a 2ª Guerra Mundial, com o intuito de ajudar no armazenamento de dados e aperfeiçoar ideias que sem tecnologia não sairiam do papel. Da mesma forma a internet foi criada, também para fins militares, porém durante a Guerra Fria, aqui com o objetivo de interligar os dados armazenados nos computadores. Ambas as invenções evoluíram e hoje são de uso comum, tanto de militares como de civis, e com inúmeras utilidades, como o já citado armazenamento de dados, interligação de máquinas, e também, correio eletrônico, meios de comunicação e interação de pessoas através de comunidades virtuais.

Pessoas de todo o mundo estão conectadas quase que em tempo integral à internet, realizando atividades diversas, desde a troca de fotos até operações bancárias, proporcionando assim um campo amplo de bens jurídicos que podem ser alvo de dano ou ameaça. Com toda essa evolução, as atividades criminosas chegaram até o âmbito virtual, e de forma perigosa, uma vez que, agentes criminosos enxergaram na internet uma maneira de cometer delitos de todos os gêneros e com certo anonimato.

Os ilícitos penais cometidos no mundo virtual, assim como os demais delitos tipificados em nosso ordenamento, são divididos pela doutrina por sua natureza. Existem basicamente, dois tipos de crimes cibernéticos. Os crimes cibernéticos próprios, que são cometidos por meio do computador ou outro aparelho eletrônico e atinge bem jurídico também no mundo virtual, ou seja, o meio eletrônico é indispensável para que ocorra a consumação do crime e o bem jurídico lesado também está dentro da esfera virtual. Já os crimes cibernéticos impróprios, são aqueles em que o a gente pode cometer o delito através de diferentes meios, porém faz uso de algum aparelho eletrônico para atingir um bem jurídico fora do mundo virtual.

Os sujeitos do crime se dividem entre quem comete o ato ilícito, com o escopo de ferir bem jurídico alheio através da internet e a vítima do respectivo ato. O agente que comete o delito, pode tanto possuir conhecimento elevado de informática, e então será chamado de forma genérica, de Cracker quanto pode ser também ser um individuo comum, sem conhecimento técnico, que através da internet cometeu ato tipificado pelo nosso ordenamento jurídico.

As regras de competência para processar e julgar os crimes cibernéticos são as mesma dos demais crimes, devendo-se observar a incidência ou não de internacionalidade e o local em que o bem jurídico lesado se situa, para que seja fixada a competência e o foro. A única observação que cabe sobre o assunto, é que o Supremo Tribunal de Justiça, já cristalizou o entendimento de que nos crimes contra a honra, cometidos através da internet, é competente o foro onde se situa o provedor do site em que a ofensa foi publicada.

A criação da Lei 12.737/12 foi realmente necessária para atualizar ordenamento jurídico pátrio, mesmo sendo fruto de oportunismo midiático é um diploma legal que com suas inclusões e alterações cumpriu com a sua intenção e trouxe, mesmo que relativa, maior segurança no sentido de que quem cometer ou proporcionar que sejam cometidos crimes na internet, serão punidos.

É clara a discrepante velocidade em que os meios de comunicação e armazenamento de dados evoluem em comparação as normas jurídicas, isso torna impossível que o direito tutele toda e qualquer lesão ou ameaça de lesão à bem jurídico feita por meio da internet, porém é essencial que assim como aconteceu na Lei 12.737/12, o legislador fique sempre atento e ao verificar novos tipos de delitos ou algum tipo de impunidade aferida graças ao uso de tecnologia, haja rápido para

combater a atividade ilícita. Dessa forma proporcionando que a internet e aparelhos eletrônicos tenham apenas a finalidade para que fora criada, que é facilitar a vida em sociedade e as novas descobertas da humanidade.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL, **Código Penal, de 7 de dezembro de 1940**. DECRETO-LEI Nº 2.848,1940.

_____. **Constituição Federal, de 05 de outubro de 1988**. Brasília: Senado, 1988.

_____. **Lei 12.737/12**. Brasília: Senado, 30 de Novembro de 2012.

_____. **CC 121215/PR**, Rel. Ministra Alderita Ramos de Oliveira (desembargadora convocada do TJ/PE), TERCEIRA SEÇÃO, julgado em: 12/12/2012, DJe 01/02/2013.

_____. **Decreto legislativo nº 28 de 14/09/1990, e do Decreto nº 99.710 de 21/12/1990**, a Convenção sobre direitos da Criança adotada pela Assembleia Geral das Nações Unidas.

CARTA FORENSE. Válter Kenji Ishida. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal**

Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986>

CENTRO UNIVERSITÁRIO "ANTONIO EUFRÁSIO DE TOLEDO". **Normalização de apresentação de monografias e trabalhos de conclusão de curso.** 2007 – Presidente Prudente, 2007, 110p.

FOLHA DE SÃO PAULO. ROMANI, Bruno. Entenda o caso da invasão hacker à Sony Pictures. **Disponível em:** <http://www1.folha.uol.com.br/tec/2014/12/1562817-entenda-o-caso-da-invasao-hacker-a-sony-pictures.shtml >

JUS BRASIL. **STJ analisa competência para os chamados crimes informáticos (crimes virtuais = cybercrimes): competência territorial do local de hospedagem do site.** Disponível em: <http://www.jusbrasil.com.br/noticias/2659329/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site>

LAFIS. Brasil: **Serviços de telecomunicações: internet**. São Paulo, SP. 2001

LAINE MORAES SOUZA ADVOGADOS E CONSULTORES, SOUZA, Laine Moraes. **Aspectos Jurídicos dos novos Crimes Informáticos no Brasil** Disponível em: <http://www.lainesouza.adv.br/aspectos-juridicos-dos-novos-crimes-informaticos-no-brasil/ >

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro: Parte Especial** - 14ª Ed. São Paulo: Revista dos Tribunais, 2015.

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

SILVA, Rita de Cássia Lopes da. **Direito Penal e sistema informático: Problemas fundamentais.** Dissertação Mestrado, Universidade Estadual de Maringá, Maringá, 2002.

SZNICK, Valdir**. Novos Crimes e Novas Penas no Direito Penal.** São Paulo: Livraria e Editora Universidade de Direito, 1992.