UNIVERSIDADE ESTADUAL DA PARAÍBA

CAMPUS CAMPINA GRANDE

CENTRO DE CIÊNCIAS JURÍDICAS

CURSO DE DIREITO

BRUNO DUTRA SERAFIM SOARES

O ORDENAMENTO JURÍDICO E OS CRIMES VIRTUAIS

CAMPINA GRANDE – PB

2016

BRUNO DUTRA SERAFIM SOARES

O ORDENAMENTO JURÍDICO E OS CRIMES VIRTUAIS

Artigo apresentado à disciplina Trabalho Acadêmico Orientado como requisito parcial à conclusão do curso de Bacharelado em Direito da Universidade Estadual da Paraíba.

Orientadora: Ana Alice Ramos Tejo Salgado

CAMPINA GRANDE – PB

2016

S676o Soares, Bruno Dutra Serafim.
O ordenamento jurídico e os crimes virtuais [manuscrito] / Bruno Dutra Serafim Soares. - 2016.
28 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2016.
"Orientação: Profa. Dra. Ana Alice Ramos Tejo Salgado, Departamento de Direito".

1. Ordenamento Juridico. 2. Crimes Virtuais. 3. Ambiente virtual. I. Título.

21. ed. CDD 345

BRUNO DUTRA SERAFIM SOARES

ORDENAMENTO JURÍDICO E CRIMES VIRTUAIS

Artigo apresentado à disciplina Trabalho Acadêmico Orientado como requisito parcial à conclusão do curso de Bacharelado em Direito da Universidade Estadual da Paraíba.

Área de concentração: Direito Penal.

Aprovada em: 03 / 11 / 2016

BANCA EXAMINADORA

Ana Alice Ramos Tejo Salgado
Prof. Dra. Ana Alice Ramos Tejo Salgado (Orientador)
Universidade Estadual da Paraíba (UEPB)

Thiago Gomes da Silva Nunes
Prof. Me. Thiago Gomes da Silva Nunes
Universidade Estadual da Paraíba (UEPB)

Prof. Me. Ramon Bolívar Germano
Universidade Federal de Campina Grande (UFCG)

AGRADECIMENTOS

Agradeço inicialmente aos meus pais, Janduí e Jacinta, pelo suporte disponibilizado e pela compreensão das minhas necessidades em cada um dos difíceis momentos de execução deste trabalho e por sempre acreditarem nas minhas capacidades.

Aos meus irmãos, Breno e Ysabel, por todo apoio moral concedido à minha formação intelectual.

A minha orientadora, professora Ana Alice Ramos Tejo Salgado, pelo tempo e paciência prestados a orientação deste trabalho.

A todos os professores do curso de Direito, da UEPB, que contribuíram para o meu desenvolvimento intelectual e emancipação do curso.

Por fim, agradeço aos amigos que conquistei durante o curso e que me auxiliaram, de diversas formas, nos inesquecíveis anos de minha licenciatura.

É o real, e não o mapa, cujos vestígios subsistem aqui e ali, nos desertos que já não são os do Império, mas o nosso. O deserto do próprio real.

Jean Baudrillard, em *Simulacros e Simulação*

RESUMO

Tendo em vista que o ordenamento jurídico recebe o influxo para elaboração de novas normas jurídicas das inovações ocorridas na sociedade, ele deve sempre se atualizar sob pena de tornar-se ineficaz. A questão dos crimes virtuais é extremamente premente na sociedade contemporânea devido justamente à inovação proporcionada pela tecnologia da informação. Uma das mais recentes inovações tecnológicas, a tecnologia da informação elaborada pelo ser humano a partir da segunda metade do século XX veio a modificar radicalmente a maneira de ser do homem em sociedade. Como a criminalidade é uma das características inerentes à existência humana que precisa ser coibida pelo ordenamento jurídico, nada mais correto do que a absorção pelo direito das novas formas de criminalidade que surgem a partir da revolução proporcionada por tal tecnologia. Temos, assim, justificada a feitura deste trabalho. Nosso artigo consiste numa pesquisa de cunho bibliográfico e tem como problemática justamente as dificuldades e soluções elaboradas no que diz respeito aos crimes cometidos no âmbito virtual. Para tanto, temos como objetivo geral a compreensão do que são esses crimes e como eles são tratados pelo ordenamento jurídico pátrio. Como objetivos específicos, observamos todos os tópicos atinentes a tais crimes, desde a terminologia relacionada ao criminoso virtual, passando pela tipificação e cobertura do princípio da legalidade, os novos tipos penais e as analogias aplicáveis aos crimes virtuais, até a competência para julgar tais crimes.

Palavras-chave: Direito, crime, ambiente virtual.

ABSTRACT

Given that the law receives influx for drafting new legal rules of the innovations that have occurred in society, it should always be updated otherwise become ineffective. The issue of cybercrime is extremely urgent in contemporary society due precisely to innovation provided by information technology. One of the latest technological innovations, information technology developed by humans from the second half of the twentieth century came to radically change the way of being of man in society. As crime is one of the characteristics inherent to human existence that needs to be curbed by law, nothing more correct than the absorption by the law of the new forms of crime emerge from the revolution provided by such technology. We have thus justified the making of this work. Our article is a bibliographic nature of research and is problematic precisely the difficulties and solutions worked out with regard to crimes committed in the virtual environment. Therefore, we have the general objective of understanding what are these crimes and how they are treated by the Brazilian legal order. As specific objectives, we observe all topics relating to such crimes, since the terminology related to the cyber criminal, through the classification and coverage of the principle of legality, the new criminal types and analogies apply to cybercrimes, to the jurisdiction over such crimes.

Keywords: law, crime, virtual environment.

SUMÁRIO

INTRODUÇÃO

Atualmente, a presença da tecnologia em nossas vidas já se tornou algo tão comum que nem nos damos conta das mudanças radicais que ocorreram ao longo de apenas meio século. A invenção da Internet, a rede mundial de computadores, alterou de tal maneira a nossa forma de coexistir que as distâncias já praticamente não existem e as comunicações são feitas, em sua maioria, por meios eletrônicos.

É evidente que a Internet possibilitou à sociedade contemporânea uma grande quantidade de avanços, mas com todo avanço também advém malefícios. Tal característica parece inerente à noção de tecnologia, tendo em vista que pode ser identificada em todos os grandes inventos que datam do final do século XIX ao início do século XXI, desde a invenção do automóvel à energia nuclear. Com a Internet não poderia ser diferente, parece que é inerente ao ser humano fazer uso nocivo das tecnologias.

Apesar de um número cada vez maior de defesas virtuais, parece que a criatividade humana para cometer crimes não possui limites e os criminosos que atuam na rede mundial de computadores sempre conseguem desenvolver novas maneiras de cometer delitos virtuais. Resta a pergunta: como os ordenamentos jurídicos podem lidar com tal velocidade das inovações, tanto de tecnologias virtuais, como de delitos cometidos por meio dessa via? Temos, assim, a problemática de nosso trabalho.

Seguindo essa linha de raciocínio, podemos enunciar nossos objetivos. Primeiramente, a informática oferece ambiente fértil e ilimitado para práticas ilícitas contra os direitos alheios, tipificados como crimes virtuais. A legislação brasileira, apesar de ser uma as maiores e mais complexas do mundo, carece de normas jurídicas que reprimam os diversos aspectos do crime virtual. Tudo é muito novo e faltam leis que tipifiquem o crime virtual, mecanismos tecnológicos de rastreamento a nível mundial e, acima de tudo, informação.

Há de se acompanhar a evolução da criminalidade, já que o Código Penal brasileiro foi elaborado em 1940, época em que nem se pensava em formas delituosas relacionadas à informática. Precisamos esclarecer as alterações que foram feitas no código ao longo dos anos no sentido de adaptá-lo aos novos tempos. Combater os crimes virtuais não é tarefa das mais fáceis quando a polícia tem à mão um Código Penal escrito em 1940. Enviar um e-mail com uma isca, um "phishing" bancário, não é crime – a menos que a polícia consiga provar que o programa levou alguém a ter prejuízo financeiro, caracterizando estelionato.

Em segundo lugar, na Internet, os cibercriminosos estão livres para fabricar todo tipo de programa nocivo e apontá-lo para suas vítimas, mas só poderão ser punidos depois que a polícia consiga comprovar que realmente o feito foi prejudicial para alguém, ou esperar que alguns crimes, como os que vêm ocorrendo recentemente com os famosos, ganham tal notoriedade que a população como um todo se veja consternada e force a atuação do poder legislativo no intuito de coibir tais delitos.

Com o agravamento de crimes virtuais impunes, aliado a um Código Penal que, por datar da década de 1940, não consegue abranger todos os atos que são praticados nos meios digitais e tidos como lesivos e criminosos pela sociedade, a Câmara Federal deu um importante passo aprovando a primeira lei brasileira voltada especificamente para punir cibercrimes. Até hoje, o país não tem mecanismos legais para lidar com crimes cometidos nos meios digitais, e a justiça tem agido baseada em leis de caráter geral.

Essas novas leis serão contra: falsificação de dados e cartões, colaboração ao inimigo, racismo e a criação de delegacias especializadas no combate a crimes digitais. Ficaram de fora os pontos mais polêmicos, como a guarda de *logs* por três anos por parte dos provedores de internet, e a possível criminalização do compartilhamento de arquivos. Trata-se de um grande passo no que diz respeito à punição de crimes virtuais e vem a mostrar que o governo brasileiro está se adequando ao novo mundo, identificando e combatendo condutas ilícitas que não param de aumentar e que muitas pessoas acham que não serão passíveis de punição.

Tendo em vista que cada vez mais os crimes digitais vêm ocorrendo e assustando a população brasileira e mundial, esse trabalho tem como fundamento esclarecer a população acerca de uma realidade crescente e que precisa ser discutida e combatida o quanto antes, pois com leis antigas e pouco voltadas para a área tecnológica, as brechas são imensas, fazendo com que muitas das vezes, esses hackers passem impunes.

O que se busca com a presente pesquisa é abrir os olhos aos profissionais do Direito quanto a importância de se adequarem a nova realidade no que concerne aos crimes que são perpetrados tendo como meio a internet, e, a necessidade do poder público aprovar os projetos já existentes em pauta, e aplicar mecanismos de maior rigor na apuração de ilícitos que venham a ocorrer em ambiente virtual, sendo que aos poucos a sociedade está migrando para uma sociedade cada vez mais digital.

1. ESCORÇO HISTÓRICO DO DESENVOLVIMENTO DOS CRIMES VIRTUAIS

A Internet é uma rede de computadores, integrada por outras redes menores, comunicando entre si. Os computadores se comunicam através de um endereço lógico, chamado de endereço IP, onde uma gama de informações é trocada, surgindo um problema: existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a disposição de milhares de pessoas que possuem acesso à internet, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que buscam na rede o cometimento de crimes, os denominados crimes virtuais. Mas a Internet não surgiu do dia para a noite, ela é o resultado de milênios de desenvolvimento tecnológico.

Ao longo da história da humanidade, o ser humano procura desenvolver métodos que facilitem as atividades do dia a dia, métodos que tornem mais fáceis realizar tarefas antes consideradas difíceis e de longo prazo. Com o surgimento de novas tecnologias, as atividades que antes demandavam um longo período de tempo para serem efetuadas passaram a ser efetuadas de forma mais rápida, quase imediatas. Um exemplo disso foi a Revolução Industrial, iniciada no Reino Unido por volta do século XVIII, mudando por completo o modo de vida da humanidade. Os camponeses mudaram-se para as cidades, os trabalhadores trocaram a atividade artesanal para controlar máquinas e com isso as fábricas passaram a produzir cada vez mais e, com a implantação dessas novas tecnologias, os navios e as locomotivas a vapor tornaram a circulação das mercadorias mais rápido, fazendo com que mais pessoas tivessem acesso aos produtos antes difíceis de acessar.

De acordo com Marcelo Xavier de Freitas Crespo (2011), o primeiro computador digital criado foi o ENIAC (*Eletronic Numerical Integrator and Calculator*), desenvolvido pelo exército norte-americano. Estima-se que seu peso seria de aproximadamente 30 toneladas e media 140 metros quadrados. O surgimento da internet se deu por uma necessidade militar, pois na época vivia-se o cenário da Guerra Fria. Aproximadamente no ano de 1996 algumas universidades uniram-se para desenvolver a ARPANET (*Advanced Research Projects Administration* – Administração de Projetos e Pesquisas Avançados) (CRESPO, 2011). A Internet surgiu, portanto, com o intuito de facilitar a comunicação em modo real, fazer pesquisas, para compartilhar arquivos e ideias.

A comunicação entre os computadores se dá através de um endereço lógico conhecido como IP, onde há uma gigantesca troca de mensagens e é por meio dessas trocas de mensagens e informações que surge um problema, pois há uma quantidade enorme de informações pessoais disponíveis na internet que encontram-se vulneráveis a milhares de pessoas que possuem acesso à internet. Tais informações, quando não disponíveis pelo próprio usuário de rede, são procuradas por

outros usuários que as buscam em razão de vantagem própria e criminosa, ou seja, os denominados Crimes Virtuais.

Atualmente, a internet encontra-se disponível em vários dispositivos de diferentes formas, incluindo dispositivos portáteis, o que oferece mais comodidade para que as pessoas possam utilizar da internet por mais tempo e usufruir das várias opções que a internet disponibiliza, como comunicar-se em modo real através de mensagens de texto ou videoconferências, leitura de livros, mídias sociais, estudos, etc. Deste modo, a rede mundial de computadores pode ser considerada como uma rede mundial de indivíduos, que trocam informações e as disponibilizam na rede e consequentemente há uma demanda de crimes virtuais.

Segundo Gabriel Cesar Zaccaria Inellas (2004), na década de 70 começaram a ocorrer os primeiros crimes de informática. Tais crimes eram cometidos, em sua esmagadora maioria, por indivíduos expertos em informática. O alvo desses indivíduos era os sistemas de segurança de empresas envolvidas principalmente com movimentação financeira. Hodiernamente, o estado de coisas mudou bastante, não temos mais um perfil específico para os praticantes de crimes digitais, qualquer pessoa que tenha um conhecimento não muito aprofundado de informática pode cometer tais crimes. A realização de um crime virtual, muitas vezes, depende somente do acesso à Internet, algo que um usuário doméstico pode realizar facilmente.

2. COMPREENDENDO O QUE SÃO CRIMES VIRTUAIS

Pierre Lévy, em sua obra *O futuro da Internet*: em direção a uma ciberdemocracia (2010), já havia identificado um crescente aumento por parte das pessoas que utilizavam a internet, e já previa um aumento substancial, tendo em vista o desenvolvimento de novas tecnologias, interfaces de comunicação sem fios, e o uso integrado de dispositivos portáteis. No entanto, a grande maioria dos usuários da internet desconhece procedimentos de segurança, utilizam sistemas operacionais piratas, não atualizam o antivírus e deixam informações pessoais gravadas no HD. De posse destas informações, algum hacker pode aproveitar-se delas para adquirir produtos via cartão de crédito, transferência bancária, chantagem e outras formas ilícitas de extorsão.

Os primeiros crimes da informática foram cometidos, na maior parte das vezes, por especialistas em informática com intuito de atingir as instituições financeiras, driblando seus sistemas de segurança. Tais responsáveis por crimes virtuais são denominados Hackers e Crackers, mas existe uma importante diferença entre os dois tipos: Hackers são pessoas dotadas de amplo conhecimento de programação e utilizam este conhecimento para o bem, criando ou melhorando sistemas e buscam superar seus próprios limites. Crackers são pessoas também dotadas de grande conhecimento de programação, mas utilizam este conhecimento para atividades ilícitas, invadindo e destruindo sistemas, roubando informações, praticando transações bancárias fraudulentas, chantageando, extorquindo e toda série de infrações ao direito alheio.

Com o passar dos anos, o número de pessoas que cometem crimes de informática vem aumentando, devido ao fácil acesso à internet. Portanto, não é preciso um conhecimento tão aprofundado de informática para se cometer um crime virtual. Vale salientar, porém, que são complexas as situações nas quais ocorrem os crimes virtuais, por isso deve-se estar atento se o mesmo é um crime virtual ou não para que se procure e se aplique o tipo penal correspondente, considerando o bem jurídico tutelado.

Compreende-se como crimes digitais ou virtuais os delitos de informática ou qualquer atividade não autorizada, que geralmente são as condutas destrutivas, infrações como intercepção de comunicações, incitação ao ódio e a discriminação, distribuição de materiais com contendo conteúdo ilegal, como pornografia infantil, dentre tantos outros.

2.1 CLASSIFICANDO OS CRIMES DE INFORMÁTICA

Há diversas formas de compreender e classificar as distinções entre os crimes considerados virtuais. Em alguns casos, atribui-se os meios eletrônicos como objeto protegido, ou seja, bem jurídico; em outros, os meios eletrônicos funcionam como ferramenta para se atingir e lesionar outros bens.

Com o aumento de indivíduos que fazem uso da internet e a criação constante de web sites, encontra-se várias formas de usufruir dos benefícios dados pelo mundo virtual, como pagar contas, comprar produtos, concluir uma graduação, dentre tantos outros benefícios que tornaram-se mais acessíveis e fáceis com a criação da internet, porém, assim como também existem os benefícios, existem os malefícios, pois há indivíduos que fazem uso da internet como meio para cometerem seus crimes.

Não é tarefa fácil constatar e classificar os crimes virtuais, posto que a tecnologia sofre uma evolução repentina e constante todos os anos, o que influi diretamente na opinião de doutrinadores. As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática. Enfim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual.

Alguns doutrinadores classificam os crimes virtuais subdividindo tais delitos em infrações à intimidade, ilícitos econômicos, ilícitos de comunicação pela emissão ou difusão de material ilegal ou perigoso, dentre tantos outros ilícitos.

Segundo Carla Rodrigues Araujo de Castro, em *Crimes de informática e seus Aspectos Processuais* (2003), os crimes digitais podem ser conceituados como sendo às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros.

Certas condutas exigem o uso de computadores para consumar tais delitos, já em outros casos a consumação destes delitos não seria possível sem a utilização do sistema de informática.

Em meados da década de 80, Tiedemann formulou a classificação dos crimes de informática formula-se como:

> a) Manipulações: podem afetar o input (entrada), o output (saída) ou mesmo o processamento de dados;
> b) Espionagem: subtração de informações arquivadas abarcando-se, ainda, o furto ou emprego indevido de software;
> c) Sabotagem: destruição total ou parcial de programas;
> d) Furto de tempo: utilização indevida de instalações de computadores por empregados desleais ou estranhos (TIEDEMANN apud CRESPO, 2011, p. 60)

Já Vicente Greco Filho (2000) adota uma classificação de crimes virtuais baseada na noção de Internet. Para ele, devemos compreender se os crimes são praticados por meio da Internet, mas que atingem outros bens protegidos que a própria Internet, ou se são cometidos contra a própria Internet como bem jurídico autônomo.

Nas classificações podemos observar que algumas determinam os meios eletrônicos como bem jurídico a ser protegido, ao passo que outras apontam para o meio eletrônico como meio de que se faz uso para lesionar outros bens. Esta última classificação nos proporciona mais oportunidades para enquadrar condutas ilícitas cometidas por meio virtual.

3. CRIMES QUE PROCEDEM POR MEIO DO USO DE COMPUTADOR

Tendo em vista que a relação entre indivíduos por meio da internet também compromete a uma espécie de sociedade, a sociedade digital, o Direito penal procura exercer as mesmas leis aplicadas na sociedade real, pois como parte de uma sociedade, os indivíduos devem tomar uma conduta que não venha a prejudicar outro indivíduo.

Quando a conduta do agente interfere na Sociedade da informação, nos seus bens jurídicos por exemplo, o Direito penal passa a exigir uma intervenção legislativa para uma nova formação de novos instrumentos de punição, ou seja, para que haja de fato a punição para determinado crime praticado por meio digital, é preciso que o tipo de penalidade a se exercer esteja de acordo com as normas já existentes.

Trata-se de princípio basilar de nosso ordenamento jurídico aquela expressa no art. 5, XXXIX, da Constituição Federal que determina que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Essa norma, conhecida como princípio da legalidade, estabelece que, para que se possa punir os crimes praticados por meio digital, sejam determinados de antemão pela legislação vigente ou, caso isso não ocorra, que tais delitos possam ser incorporados ao ordenamento.

Analisar uma atividade criminosa na internet é uma tarefa complicada, devido à dificuldade de rastrear os agentes executores de tais crimes. Ademais, é necessário que haja uma pena adequada para cada tipo de crime. Na legislação nacional, as primeiras manobras legislativas ocorreram com o advento do Plano de Informática e Automação (Conin), representado pela lei n. 7.232/84, que tinha como objetivo versar sobre as diretrizes no âmbito da informática em solo brasileiro. Logo, surgiu a Lei n. 7.646/87, sendo revogada pela Lei n. 9.609/98. Esta Lei foi a primeira ordem criada para descrever os delitos de informática.

Devemos citar também a Lei Carolina Dieckmann, como ficou conhecida a Lei 12.737/2012, sancionada em 2 de dezembro de 2012 pela Presidente Dilma Rousseff, que promoveu alterações no Código Penal, incluindo alguns artigos referentes a delitos informáticos. Essa lei foi oriunda do Projeto de Lei 2.793/2011, apresentado pelo Deputado Paulo Teixeitra (PT-SP) e tramitou em regime de urgência e foi aprovada em tempo record. Tal celeridade na aprovação do Projeto decorre de uma experiência particular tida pela atriz cujo nome aparece na lei. Em outros termos, a lei resultou de um furor midiático criado em torno da atriz Carolina Dieckmann, que teve fotos íntimas suas copiadas a partir de seu computador pessoal e divulgadas na Internet.

Essa lei trouxe algumas mudanças significativas do Código Penal, dentre as quais:

a) alteração do Código Penal pela inserção do delito “Invasão de dispositivo informático” que, por meio do art. 154-A, veio a tipificar a conduta de “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”;

b) alteração do Código Penal pela inserção do tipo penal “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” por meio do § 1º de seu art. 266;

c) alteração do Código Penal pela inserção do tipo penal “Falsificação de cartão” por meio parágrafo único do art. 298 do Código Penal.

Outro projeto de lei também ampliado é o PLC n. 89/2003, que visa assumir novas tipificações de crimes para as novas condutas criminosas.

Nos crimes de Fraude virtual, por exemplo, a prática do agente dar-se por meio de uma invasão do computador ou alteração no sistema de processamento de dados. Alguns exemplos de Fraudes Virtuais são os Cavalos de Troia, páginas falsas, direitos autorais, entre tantos outros. O agente executor utiliza de páginas falsas ou falsas mensagens se passando por instituições conhecidas para vantagem pessoal, com objetivo de induzir o usuário ao fornecimento de seus dados pessoais.

Quanto às fraudes virtuais, há que se salientar que existe controvérsia a respeito delas poderem ser enquadradas no tipo penal do furto mediante fraude (art. 155, § 4º, II, do CP) ou como estelionato (art. 171, caput, do CP). Os crimes são diferenciados a partir da ideia de que, no estelionato, o agente obtém a coisa a partir de transferência por parte da vítima, que foi induzida a erra, ao passo que, no furto qualificado pela fraude, o objeto é subtraído, em discordância expressa ou presumida do detentor, tendo em vista que o agente do crime utiliza-se da fraude para retirar o objeto da esfera de vigilância da vítima.

No estelionato, segundo o Código Penal, em seu art. 171, o agente obtém para si vantagem ilícita induzindo alguém em erro, ou seja, o agente ilude a vítima até obter seu consentimento, enviando links no corpo da mensagem que leva a páginas falsas onde a vítima digita suas informações pessoais. No que se refere ao estelionato digital, várias são as condutas que os perpetradores podem adotar para cometer tal delito.

Muitos desses crimes virtuais são realizadas mediante envio de e-mail falso (*phishing*) para o computador de uso pessoal com informações falsas que direcionam o usuário para um site, no qual este disponibiliza seus dados bancários para o agente do crime. É possível tipificá-las como estelionato, tendo em vista que o meio informático oferece inúmeras possibilidades de iludir a vítima e levá-la a, voluntariamente, entregar dados bancários.

Uma ferramente bastante útil no que diz respeito tanto a frade virtual como ao estelionato virtual é o antivírus que, após instalado, oferece uma proteção conta esses e-mails falsos. Outra forma de defesa é configurar o sistema de segurança do *Firewall* para que e-mails indesejados nem sejam recebidos pelo usuário, evitando, assim, que este sequer os leia.

Outra modalidade de crime bastante comum no meio digital é o crime contra a honra. Tais crimes ocorrem quando o agente difama (art. 139 do CP) e expõe a vítima imputando-lhe fato ofensivo à sua reputação. Neste crime, a lei não exige que a atribuição seja falsa, basta expôr algo que ofenda a honra e a reputação de alguém. Já no crime de calúnia (art. 138 do CP), de modo enganoso o agente atribui à vítima algo definido como crime, ou seja, o agente sabe que tal atribuição é falsa e mesmo assim não hesita em expôr a vítima afetando sua honra objetiva e sua reputação. No crime de injúria (art. 140 do CP) o agente expõe uma qualidade negativa da vítima que diz respeito às suas qualidades morais, intelectuais ou físicas, afetando a honra subjetiva da vítima. Tais modalidades de crimes foram potencializados pelo advento da internet, tendo em vista que esta é uma ferramenta que agiliza as comunicações e troca de dados.

Nos crimes de pornografia infantil o agente disponibiliza material contendo pornografia infantil, não sendo necessário que o agente tenha acesso ao material para cometer este crime, pois basta ter esse material sob sua guarda. Segundo o código Penal, em seu art. 234: “Fazer, manipular ou ter esse material sob sua guarda para fins de comercialização ou exposição pública tem como penalidade de seis meses a dois anos ou multa”. O crime de pornografia infantil tem como elemento subjetivo o dolo, que ocorre quando o agente tem a intenção de cometê-lo. Neste caso, para que encontre o agente que executou este crime é preciso muitas vezes que haja quebra de sigilo.

Os crimes de espionagem eletrônica geralmente são executados com intuito de coletar ou apagar informações que o espião tem interesse. Esta conduta não possui tipo penal específico, mas é definida pelo Código Penal, em seus arts. 154 e 184, como crime de violação de segredo profissional e crime de violação de direito autoral.

O crime de violação de segredo profissional possui a seguinte redação: “Art. 154: Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano,

ou multa". Tal crime pode ser cometido tanto por pessoas estranhas à empresa, como por funcionários. Por conta dessa característica, esse crime é muito difícil de ser combatido, posto que o agente normalmente é um usuário legítimo do sistema da empresa (*"insider"*), possuindo, assim, acesso regular ao mesmo. Também é muito fácil apagar os registros de acessos e eliminar os rastros de algum crime que, porventura, venha a ser cometido. É preciso que a empresa incorra em um controle maior das informações. Controle este que pode ser exercido de três maneiras: controle físico; controle lógico e controle comportamental. Vale salientar que, de acordo com o artigo 482, "g", da CLT, se um funcionário cometer tal conduta em uma empresa, estará sujeito a ter seu contrato rescindido por justa causa.

Os crimes contra os direitos autorais são aqueles nos quais o agente disponibiliza materiais de forma ilícita, como cópias de materiais ou a pirataria, quando consiste na venda não autorizada destes materiais. São tipificados da seguinte maneira pelo código Penal: "Art. 184: Violar direitos de autor e os que lhe são conexos: pena de detenção, de três meses a um ano, ou multa". A Lei nº 9.610, de 19 de fevereiro de 1998, que trata dos direitos autorais, dispõe que é necessário dar ao indivíduo criador da obra os devidos direitos de propriedade intelectual, para que possa usufruir dos benefícios resultantes de sua obra.

Um dos grandes problemas para se fazer respeitar as normas que dizem respeito ao direito autoral é a concepção por parte dos usuários da Internet de que o que está exposto nos sites como produto a ser baixado sem custo algum é domínio público e que, portanto, é lícito apropriar-se de tal produto. A facilidade de acesso não elide a ilicitude dessa atitude.

Os softwares que não são livres não podem ser copiados ou distribuídos sem que o usuário faça uma contraprestação. Tais softwares possuem um código-fonte que não pode ser copiado; porém, uma das formas mais comuns de pirataria é justamente a cópia não autorizada desses softwares. Tais cópias ilegais podem ser feitas por usuários finais, que as redistribuem entre outros usuários. A venda não autorizada por parte de revendedores que possuem somente um pacote do software. A forma mais comum é aquela que se dá pelo acesso a sites que disponibilizam de maneira não autorizada o produto para que possa ser feito o download.

Outros delitos que remetem ao livre mercado são tipificados no Código de Defesa do Consumidor (Lei 8.078/11). Podemos citar:

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
> Pena – Detenção de seis meses a um ano ou multa.

> Art. 73. Deixar de corrigir imediatamente informações sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
> Pena – Detenção de um a seis meses ou multa.

A tendência em torno dessas condutas é somente de aumentar porque vivemos num momento em que o capitalismo se recrudesce e as empresas procuram qualquer tecnologia que lhes proporcione o mínimo de vantagem sobre as concorrentes. Torna-se premente a intromissão do poder público em tais relações mercantis, no intuito de proteger os hipossuficientes de serem manipulados pelas empresas no sentido de consumirem produtos que não necessitam.

Outro crime extremamente comum é aquele que remete à invasão de privacidade (art. 154-A do CP). Tais crimes, diante da notoriedade de certas pessoas públicas, são extremamente populares devido à demanda por imagens ou vídeos de famosos. Inúmeros são os casos desses tipos de ilícitos cometidos no Brasil e no exterior, tendo alguns até mesmo sido veiculados pela imprensa nacional e internacional. Mas não devemos pensar que tais condutas são consideradas ilícitas quando cometidas somente contra pessoas conhecidas na mídia, pois até mesmo a coleta de dados de consumidores, sem o devido conhecimento, por parte de empresas também incide em tal tipificação.

4. COMO PROCESSAR E JULGAR CRIMES VIRTUAIS

4.1 COMO PROCESSAR E JULGAR CRIMES VIRTUAIS: LEGISLAÇÃO NACIONAL

No que diz respeito ao processamento de ações referentes a crimes virtuais, devemos ter em mente que a competência deve ser determinada, primeiramente, a partir do local onde se desenrolou a conduta ilícita, i.e., em qual território a ação de desenvolveu. Temos, assim, um problema, tendo em vista que a internet, por ser uma rede mundial de computadores, dificulta muito a demarcação de territórios.

Através da internet, as mais improváveis relações jurídicas são criadas. Por exemplo, usuários criam sites em países diversos daqueles nos quais têm domicílio. Aliás, os acessos a sites podem ser feitos de qualquer lugar do mundo; isso significa que pessoas que possuem residência no Brasil podem estar acessando sites sediados nos EUA.

Consideram-se hodiernamente vários princípios para se determinar a autoria e a lei a ser aplicada em cada caso, dentre os quais encontramos o princípio do endereço eletrônico, o do domicílio do consumidor, do local no qual se cometeu a conduta ou onde se realizam os efeitos, o da localidade do réu e o da eficácia na execução judicial (PINHEIRO, 2010).

No Brasil, para que possamos determinar a competência para processar e julgar os crimes praticados na internet, são aplicados os artigos 5º e 6º do Código Penal brasileiro:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
> Art. 6º - Considera-se 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.

Percebe-se, assim, que nosso Código Penal adotou a teoria da ubiquidade, na qual consideram-se locais do crime tanto o local no qual foi cometida a conduta, no todo ou em parte, como o local onde se produziu ou deveria se produzir o resultado. O art. 7º do Código Penal determina, ainda, que, em relação aos crimes cometidos por brasileiro, tanto no país como fora dele, seja aplicada a legislação pátria. Essas normas possibilitam grande abrangência no que diz respeito a aplicabilidade da lei penal. Tal característica é bastante pertinente quando lidamos com crimes.

4.2 COMO PROCESSAR E JULGAR CRIMES VIRTUAIS: LEGISLAÇÃO INTERNACIONAL

A preocupação com os problemas causados pela criminalização por meio digital é uma questão que vem sendo analisada há vários anos, mundialmente falando. Existem várias entidades e organizações que discutem esses problemas, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), da qual fazem parte os países comprometidos em apoiar o crescimento econômico sustentável, qualidade de vida, e visam contribuir para o crescimento do comércio mundial.

Por meio destes países, a OCDE desenvolveu legislações nacionais apresentando critérios que tinham por objetivo uma cooperação internacional para criminalizar as condutas definidas como abuso informático, tais como Fraude informática; Falsificação informática; Sabotagem informática; Cópia ilegal de programas informáticos; Acesso ilegal a sistemas informáticos, Introdução, alteração, destruição e/ou supressão de dados informáticos e/ou programas de computador, realizadas intencionalmente como forma de se praticar falso, Introdução, alteração, destruição e/ou supressão de dados informáticos e/ou programas de computador ou qualquer outra interferência em sistemas informáticos, realizadas com o fim de obstaculizar o funcionamento do sistema informático ou de telecomunicações; Transgredir de direito exclusivo de propriedade de programa informático protegido, com o fim de explorá-lo comercialmente, introduzindo-o no mercado; Acesso ou interceptação não autorizados a sistema informático ou de telecomunicações, com finalidade fraudulenta ou danosa.

O primeiro país a tipificar e aplicar penalidade aos crimes cometidos por meio do uso da informática foi os Estados Unidos da América. A proposta foi criada por Ribicoff Bill no ano de 1978 e apesar de não ter sido aprovada foi de grande utilidade para elaboração de legislações posteriores. Porém, nos Estados Unidos da América, cada Estado cria seus estatutos penais e a intervenção Legislativa Federal tem papel secundário (CRESPO, 2011).

Na Europa em 1995 foi elaborada a Recomendação R (95) a qual contém sete princípios de atuação penal para as condutas criminosas por meio do uso da informática, são estes: Registro; Vigilância técnica; Obrigações de cooperação com autoridades investigadoras; Prova eletrônica; Uso de criptografia; Buscas, estatísticas e treinamento; Cooperação internacional (CRESPO, 2011).

Na Espanha, seu Código Penal, em seu art. 197,1, incrimina o indivíduo que, sem autorização, se apodera de correspondências eletrônicas ou qualquer outro documento com o intuito

de violar a intimidade de outrem. Neste caso, no inciso 2º do artigo referente, há incriminação de intercepção de telecomunicações.

Em Portugal, os crimes de entidade digital passaram a ser criminalizados por meio da Lei n.109/91, que criminaliza as condutas de: Falsidade Informática; Dano a dados ou programas informáticos; Sabotagem informática; Acesso Ilegítimo; Interceptação ilegítima; Reprodução ilegítima; Reprodução ilegítima de programa protegido (CRESPO, 2011).

Na América Latina, o Chile foi o primeiro país a incorporar alguns crimes digitais em sua legislação. A Lei n. 19.223/93, em seu art. 2º, pune o indivíduo que danifique ou inutilize um sistema ou seus componentes. No art. 2º há incriminação de interceptação indevida em sistema. No art. 3º pune-se o indivíduo que altera, danifica ou destrua os dados contidos em determinados sistemas (CRESPO, 2011).

4.3 AS DIFICULDADES EM PROCESSAR E JULGAR CRIMES VIRTUAIS

As dificuldades em processar e julgar os crimes virtuais são inúmeras, visto que todo processo necessita de provas, para ter andamento e para que se confirme o delito. Coletar essas provas no mundo virtual não é tarefa fácil. Porém, como consta no art. 332 do Código de Processo Civil: "Todos os meios legais, bem como os moralmente legítimos são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa". Ainda, a Medida Provisória nº 2.200-1/2001 em seu art. 1º versa que:

> Fica Instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

No caso de um documento não assinado ou em que seu certificado não esteja vinculado ao ICP-Brasil, realiza-se uma perícia no computador para que se verifique a autenticidade da documentação. Neste caso, o juiz dispõe do Livre Convencimento Motivado, posto que o credenciamento consta como um selo de qualidade técnica, não sendo completamente necessário para a apreciação da prova.

Atualmente, faz-se uso da assinatura digital e certificação digital, que é uma espécie de tecnologia de criptografia onde há uma ferramenta de codificação usada para envio de mensagens

seguras em redes eletrônicas. Esses instrumentos são o que dão a autenticidade dos documentos virtuais e assim, sabe-se de sua origem. O código pessoal fornecido pela assinatura eletrônica é uma chave privada que não pode ser reproduzida e impede que o conteúdo transmitido ou compartilhado seja acessado por outro indivíduo, ou seja, esse conteúdo só pode ser acessado por aquele indivíduo que possua a mesma chave, que é reconhecida com a mesma validade da assinatura tradicional.

Quanto ao endereço de IP-Internet Protocol, este número é fornecido ao usuário para sua identificação em rede. Porém, caso o usuário não tenha optado por um endereço de IP fixo, como é o caso de muitos criminosos virtuais, quando o modem é desligado, o endereço de IP que foi atribuído ao usuário passa para outro e assim por diante. Por isso, é tão difícil encontrar o agente do crime.

Nos crimes virtuais, quando se tem o endereço de IP, deve-se pedir ao provedor de acesso à internet a data, hora em que a conexão foi feita e o fuso horário. Sem estes dados aumenta-se a dificuldade em pedir uma quebra de sigilo. Se houver a localização do provedor, a quebra de sigilo dos dados deve ser requisitada pelo juiz. Após isso, faz-se uma investigação sobre as atividades feitas por aquele endereço de IP suspeito, comparando a hora e em qual território o crime ocorreu. Ainda, vários usuários registram sites em um país diferente daquele de onde ocorrem as atividades, ou seja, o fato de um site ser registrado em um país não impede que usuários que outros países pratiquem suas atividades nesse site.

CONCLUSÃO

Nosso trabalho voltou-se para as dificuldades apresentadas pelo advento de um novo tipo de criminalidade voltada para o meio virtual. Procuramos evidenciar como o Direito Penal pátrio e internacional está buscando tipificar condutas ilícitas ocorridas no ambiente virtual.

Partimos da classificação não somente daqueles indivíduos que cometem crimes em ambientes virtuais, mas também dos tipos de condutas que podem ser consideradas ilícitas nesse meio. Tornou-se evidente para nós que o número de pessoas que procuram fazer uso dos meios virtuais para cometer crimes está aumentando, devido à facilidade com que tais delitos podem passar impunes. Trata-se de todo um novo ambiente que se torna mais complexo a cada dia, com estruturas cada vez mais elaboradas e que, justamente por isso, escapam ao ordenamento jurídico, que ainda é extremamente moroso na sua tentativa de tipificar tais condutas e determinar a jurisdição e o processamento das mesmas.

Chegamos à conclusão de que o ambiente virtual funciona como uma duplicação do mundo real, na medida em que ele não somente reproduz as relações sociais ocorridas em nosso dia a dia, como também gera novas identidades para qualquer pessoa que queira passar despercebido ou permanecer anônimo em tal meio. Esta oportunidade abre todo um leque possibilidades para que indivíduos mal intencionados possam liberar seu lado mais obscuro e perpetrar condutas torpes, que vão desde estelionato até pornografia infantil.

Como exemplo, nós podemos citar a confecção de identidades falsas em redes sociais que estão abertas a todas as faixas etárias. Tais redes sociais dão até mesmo a crianças mal supervisionadas pelos pais a possibilidade de criar perfis públicos, o que as torna, por sua vez, alvos fáceis para qualquer indivíduo mal intencionado que crie um perfil falso e entre em contato com tais crianças.

Cremos que o meio virtual funciona como um exponencial para o cometimento de condutas ilícitas, porque gera uma ilusão de que podemos disfarçar nossas identidades, ilusão esta que, muitas vezes, pode ser considerada verdadeira, devido à dificuldade de identificar Ips, seja por meio de habilidades desenvolvidas pelos usuários ou, até mesmo, devido ao uso de meios públicos de acesso ao ambiente virtual.

Mas não é preciso ser um experto em computação para cometer crimes virtuais, basta lembrar da modalidade de ilícito penal conhecida como crime contra a honra que, nas suas modalidades de calúnia, injuria e difamação, pode acarretar em consequências graves à reputação de um indivíduo. O cometimento de tais crimes tornou-se extremamente comum com o advento de

meios de comunicação muito ágeis, nos quais alguma mensagem ou vídeo podem ser passados adiante rapidamente e o poder público não possui meios de punir todos os envolvidos.

Não devemos olvidar, porém, a importância dos crimes contra a propriedade intelectual que, na era da reprodutibilidade técnica, tornou-se por demais comum. Tidos, às vezes, como inofensivos e cometidos por ampla maioria da população, tais crimes não consistem somente nas condutas de hospedar ou fazer download de conteúdos protegidos, mas também na conduta de realizar plágios de conteúdos obtido legalmente na internet. Tais reproduções, sem a devida menção do autor, são crimes, pois, de acordo com a legislação cível, é necessário que haja uma contrapartida do autor da obra, ou seja, é necessário que uma relação se estabeleça entre aquele que utiliza o conteúdo protegido e aquele que produziu tal conteúdo, de forma a não somente proteger a autoria, como fomentar a produção de mais obras.

Tratamos ainda dos delitos ligados à invasão de privacidade, que vão desde aqueles ligados à mídia até aqueles ligados ao capital, na figura de grandes empresas que traçam perfis de consumidores.

Nosso trabalho considerou também a legislação nacional e estrangeira no que diz respeito a tipificação de tais condutas, bem como no tocante as dificuldades relativas à jurisdição e processamento de tais crimes. Ficou claro para nós que alguns desses delitos cometidos por meio informático são abrangidos pela legislação pátria, mas há outras condutas que, por enquanto, permanecem somente como objeto de projetos de lei.

Como dissemos acima, o direito é lento e a justiça, morosa. A relação entre direito e sociedade é *mutatis mutandis*, ou seja, enquanto a sociedade muda, o direito tenta acompanhá-la, ao passo que o próprio direito acarreta mudanças na sociedade. Em termos práticos, isso significa que os criminosos sempre procuram se adaptar às mudanças efetuadas no ordenamento jurídico. Como exemplo, podemos citar os crimes que são executados por meio de cópia de senhas bancárias obtidas por meio de programas que copiam os dados inseridos nos teclados de computadores pessoais ou, até mesmo, caixas eletrônicos. As agências bancárias sempre procuram novos meios de dificultar a realização de tais crimes, mas os criminosos continuam conseguindo desenvolver novos meios de obter as senhas e desfalcar contas privadas em bancos.

Para finalizar nosso trabalho, repetimos o que foi dito na introdução a respeito do objetivo mais amplo da pesquisa, que consiste justamente em abrir os olhos não somente dos operadores do direito, como também da população em geral acerca da complexidade dos crimes virtuais e do alto grau de facilidade com que tais crimes podem ser cometidos, caso alguém se veja minimamente motivado a cometê-los.

REFERÊNCIAS

BAUDRILLARD, Jean. *Simulacros e Simulação.* Trad. de Maria João da Costa Pereira. Portugal, Lisboa: Relógio d'Água, 1991.

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

CRESPO, Marcelo Xavier de Freitas. *Crimes digitais.* São Paulo: Saraiva, 2011.

GIL, Antônio de Loureiro. *Fraudes Informatizadas*. 2 ed. São Paulo: Atlas, 1999.

GRECO FILHO, Vicente. *Algumas observações sobre o direito penal e a internet*. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

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

LEMOS, André & LÉVY, Pierre. *O futuro da Internet*: em direção a uma ciberdemocracia. São Paulo: Paulus, 2010.

LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança computacional*. Campinas, SP: Ed. Millennium, 2005.

LIMBERGER, Têmis. *O direito à intimidade na era da informática*: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado Editora, 2007.

PEREIRA, Ricardo Ancântara. *Breve introdução ao mundo digital*. Opice Blum (org). Direito eletrônico: a internet e os Tribunais. São Paulo: Edipro, 2001.

PINHEIRO, Patrícia Peck. *Direito Digital*. 4. Ed. São Paulo: Saraiva, 2010.

TIEDEMANN, Klaus. *Lecciones de derecho penal económico*. Barcelona: PPU, 1993.

VADE MECUM. 15ª Ed. São Paulo: Saraiva, 2015.