A evolução criminológica do Direito Penal: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012.

Carolina Borges Rocha

(email: carolinabor@gmail.com)

Graduada pela Universidade do Estado da Bahia. Advogada e consultora jurídica

1. Considerações introdutórias

O debate sobre os crimes na internet se mostra relevante, haja vista que com a evolução tecnológica, a informática, em especial a internet, se tornou um meio hábil e eficaz de comunicação e informação transformando, assim, o cotidiano do homem moderno. Sucede que esta modernização estendeu-se também sobre o Direito, em especial no campo do Direito Penal.

No limiar dessa evolução tecnológica é possível constatar que, atualmente, o Código Penal de 1940 tende a lidar com situações criminosas que vão além do plano físico. Hoje, o agente delituoso não necessita ir às ruas para cometer determinados ilícitos como furto, racismo, crimes contra à honra, dentre outros.

Relevante ressaltar, todavia, que, ao passo em que o Direito Penal ganhou novos entornos criminológicos com a internet sendo utilizada como instrumento de práticas delituosas, muitas questões afligem a comunidade jurídica que teve suas discussões alavancadas sobre o presente tema com a nova Lei 12. 737/2012.

2. A internet e o Direito Penal

É percebido que o Direito encontra-se, assim, diante de uma nova realidade, uma realidade virtual totalmente diversa do mundo físico que até então regulamentava o

ordenamento jurídico brasileiro de modo que, inclusive, o pesquisador Marcio Pinto defendeu a existência de um novo ramo do Direito: o Direito da Informática[1].

De qualquer sorte, cumpre salientar que essa influência da informática avança na maioria dos ramos do Direito, como pode ser constatado, por exemplo, no Direito Civil quanto ao comércio eletrônico, em que é perceptível a utilização das normas contratuais estipuladas no Código Civil de 2002 e por isto, a conceituação do contrato como um negócio jurídico e que depende para sua existência da exteriorização da vontade se aplica perfeitamente aos contratos eletrônicos. O mesmo regramento do comércio eletrônico também é visto a luz do Código de Defesa do Consumidor em que é constatado a ampla publicidade e propaganda de serviços e produtos que são divulgados na internet como forma de atrair mais consumidores.[2]

A internet e informática também ganharam relevância no tocante à disciplina Processo Civil, em especial às execuções, na medida em que com a chamada penhora *online*, esta permite ao juízo da execução informar ao Banco Central a determinação do bloqueio das aplicações financeiras do executado evitando, assim, a morosidade da expedição de carta precatória. Sem contar a existência, atualmente, dos chamados processos virtuais existentes nos Juizados Especiais Federais [3]. É percebido, portanto, que estamos diante de uma nova realidade jurídica.

Ocorre que, esta inovação também repercutiu no âmbito do Direito Penal e Processual Penal, haja vista que até o ano de 2012, a internet era isenta de qualquer regulamentação jurídica específica e em virtude disto, se tornou meio apto para a realização de crimes e condutas danosas.

A internet/infomática se mostra um instrumento facilitador para a consecução de crimes, pois, em muitos casos, o agente delituoso não precisa utilizar de nenhum instrumento físico que seja ou violento ou ameaçador para realização daqueles, bastando

---

[1] PINTO, Marcio Morena. ***O Direito da internet: o nascimento de um novo ramo jurídico***. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2245>. Acesso em: 8 fev 2012.

[2] TANABE, Silvio. ***MARKETING DIGITAL | PUBLICIDADE NA INTERNET É O QUE MAIS INFLUENCIA NAS COMPRAS.*** Disponível em: < http://clinicamarketing8ps.com.br/marketing-digital-publicidade-na-internet-e-o-que-mais-influencia-nas-compras/>. Acesso em: 9 ago. 2012.

[3] JR, Fredie Didier; Cunha, Leonardo. ***Curso de Direito Processual Civil***, p. 606.

apenas o computador e o conhecimento técnico, ou não, para concretizar as condutas delitivas.

Por isto, na medida em que a internet concentra, processa e transfere qualquer tipo de informação e dados, também se transformou em um meio eficaz para a realização de crimes ou certas condutas que agridem bens relevantes do homem. Auriney Uchôa de Brito, com acerto, explana sobre esta influência da infomática a serviço do crime:

> Alguns fatores como a intensificação dos relacionamentos via internet, a produção em série de computadores, a popularização do comércio eletrônico (*e-commerce*) e o aumento de transações bancárias, estão diretamente ligados ao aumento de ocorrências de crimes conhecidos, mas que praticadas pela internet ao surgimento de novos valores e logicamente à novas condutas delitivas.[4]

Eis que em um intervalo ínfimo de tempo, um *cracker* pode acessar de um computador alheio a conta bancária de um usuário que esteja manuseando dados de sua conta bancária e ao tempo em que ele identifica a sua senha e dados bancários, este *expert* da informática, utilizando de técnica e conhecimento específico pode furtar a importância contida na conta bancária. Cria-se, assim, um novo instrumento para a consecução de crimes já consagrados no ordenamento pátrio.

Sucede que, ao tempo em que a internet proporcionou um incremento delitivo para àquelas condutas já consagradas em nosso ordenamento penal, a comunidade jurídica se atentou para discussão acerca do surgimento de novos bens jurídicos violados quando cometidos na internet e que não havia uma regramento sobre tais condutas.

Assim, aos fatos que já possuem tipificação legal e consequentemente, bem jurídico protegido pelo ordenamento, com a internet, ficaram vistos apenas como uma nova instrumentalização da modalidade delitiva. É o caso dos crimes cometidos contra à honra, fraude, furto e estelionato.

Por outro lado, novas condutas que violam os direitos e garantias da sociedade e que vão além dos bens jurídicos tutelados pelo Direito Penal como dano informático, violação ao dispositivo infomático dentre outros que não possuem seus bens jurídicos abarcados em nossa legislação, pela falta de previsão legal, quando ocorria alguma ofensa a estes bens

[4] BRITO, Auriney Uchôa de. ***O bem jurídico-penal dos delitos informático***, p. 14.

não havia como punir, na medida em que, como cediço, o Direito Penal não tipifica conduta por analogia em nome do princípio da legalidade, conforme disposto em nossa Carta Magna, em seu art. 5º, XXXIX "***Não há pena sem lei anterior que o defina****, nem pena sem prévia cominação legal".*

3. Tratativas procedimentais e a nova Lei 12. 737/2012

O tema ora em debate fez surgir discussão farta no cenário jurídico até a chegada da Lei 12. 737/2012. Hoje, com a inserção de dispositivos no diploma penal através da lei citada, os debates sobre o tema ganharam novos contornos.

Conforme aponta Uchôa, "para ser legitima a tutela penal é necessário que o bem seja 'digno' dessa proteção, e que sua lesão ou ameaça efetivamente mereça uma sanção penal" [5]. Assim sendo, a doutrina especializada considerou por bem apaziguar o entendimento de que há bens jurídicos tutelados no Direito Penal que são violados na consecução de práticas delituosas na internet que, frisa-se, se constitui apenas como um instrumento do crime. *In casu*, a internet é utilizada para a realização de um delito já configurado no Código Penal. É o que expõe o doutrinador Luiz Flávio Gomes:

> (...) os crimes informáticos dividem-se em crimes contra o computador; e crimes por meio do computador, em que este serve de instrumento para atingimento da meta optada. O uso indevido do computador ou de um sistema informático (em si um fato "tipificável") servirá de meio para a consumação do crime-fim.[6]

Portanto, o que modifica é apenas o meio, a sua instrumentalização. Crimes como estelionato, furto, extorsão, ameaça, por exemplo, possuem bens jurídicos já tutelados no Código Penal e por isto o que diferencia é apenas quanto ao meio utilizado. Corrobora com este entendimento o insigne Vicente Grego Filho (2000) citado por Auriney Brito (2009) que aduz: "não importa se instrumento utilizado é a informática, a internet ou uma

[5] BRITO, Auriney Uchôa de. ***O bem jurídico-penal dos delitos informático,*** p. 14.
[6] ARAS, Vladimir. ***Crimes de informática. Uma nova criminalidade.*** Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2250>. Acesso em: 4 set. 2012.

'peixeira'."[7]. Este, inclusive, é o posicionamento dos Tribunais Superiores, dentre eles o Superior Tribunal de Justiça.[8]

E de fato, este entendimento prevalecente no STJ tem pertinência, uma vez que vista a internet como uma rede mundial de computadores, a criminalidade se fará cada vez mais presente e por isto coube o Poder Judiciário ter a percepção de que a maioria dos delitos cometidos já possuem seus bens tutelados pelo regramento jurídico cabendo, então, realizar uma intepretação a luz da legislação pátria em vigor. [9]

Ocorre que, a problemática que circundava o tema era em relação às novas condutas ilegítimas que o Direito Penal se mostrava atado no tocante a sua punição. Foi em razão dessa lacuna na legislação penal que foi criada a Lei 12. 737/2012.

Entrementes, importante mencionar que, as discussões que levaram ao nascimento da referida lei foi fruto de fervorosos embates no cenário jurídico-político. Senão vejamos.

Antes da Lei 12. 737/2012, que deu ensejo a um novo tipo penal e algumas alterações no Código Penal, existiram diversos outros projetos de lei no cenário político brasileiro na tentativa de dirimir tais condutas.

Dentre estes, houve o Projeto de Lei n. 89/2003 que chegou a tramitar por mais de 10 anos no Congresso Nacional e teve sua redação final aprovada pelo Senado Federal somente nos idos de 2008, na forma de um substitutivo. Tal projeto, todavia, desencadeou intensos embates jurídicos sobre o seu conteúdo, inclusive, recebeu inúmeras críticas dos internautas ativistas que, conforme apontou o jornal câmara vinculado a Câmara dos Deputados, chegou a circular uma petição contrária a aprovação deste projeto com mais de 165 mil assinaturas.[10] **.** Em razão disto, o projeto ficou conhecido como "AI-5 Digital",

---

[7] BRITO, Auriney Uchôa de. ***O bem jurídico-penal dos delitos informáticos***, p. 14.

[8] SUPERIOR TRIBUNAL DE JUSTIÇA. **Local de hospedagem do site define competência para ação por calúnia em blog jornalístico**. . Brasília: 2001. Disponível em: <. http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=101559>. Acesso em: 5 mai. 2012.

[9] SUPERIOR TRIBUNAL DE JUSTIÇA. Disponível em: <http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=90108>. Acesso em 25, jun. 2012.

[10] HAJE, Lara. **ESPECIAL - Proposta sobre crimes cibernéticos tramita há 12 anos no Congresso.** Disponível em: < **http://www.camara.gov.br/internet/jornalcamara/default.asp?selecao=materia&codMat=70377> .**Acesso em: 4 mai. 2012.

.

uma vez que suprimia a liberdade de expressão dos internautas e porventura enquadraria na tipificação penal um simples *download*.

Sendo assim, em 2011 foi aprovado pela Câmara dos Deputados outro projeto, a saber, o Projeto de Lei n. 2793/2011 que, frisa-se, teve seu nascimento justamente para combater o Projeto de Lei n 89/2003 considerado, então, defasado e prolixo.

Em verdade, os autores deste projeto acreditavam que este seria mais proveitoso para a sociedade, haja vista que continha poucas disposições legais sobres os cibercrimes ao ser comparado com o já mencionado Projeto de Lei n. 89/2003. Os autores do PL 2793/2011 argumentavam que boa parte dos delitos já praticados com o auxílio ou não da rede mundial de computadores já implicam numa repressão estatal prevista no ordenamento jurídico. Daí, a iniciativa em criar somente delitos que violavam certo bem jurídico ainda não amparado na legislação penal.

A problemática que circundava os projetos de lei, todavia, só teve fim com o episódio envolvendo a atriz global Carolina Dieckmann. Esta foi vítima de *crakers* que, em razão de seu computador estar vulnerável, ou seja, sem um sistema de segurança ativo contra vírus e *spams*, obtiveram a senha do seu e-mail e por consequência, diversas fotos da atriz seminua e em posições em que expunha sua intimidade. Tais fotos foram disseminadas aquém dos delinquentes e foram parar, inclusive, em *sites* pornográficos.

Os agentes criminosos foram presos e juntamente com eles foram apreendidos os computadores e demais instrumentos do crime. Ocorre que em meio a suas condutas, tais agentes foram indiciados pelo crime de furto, o que não deixa de ser curioso tal enquadramento penal.

Isto porque este crime, previsto no art. 155 do Código Penal trata da subtração de coisa alheia móvel e este "móvel" remonta algo material, que possa ser tocado e por isto a importância de uma reflexão se realmente tal imputação condiz com a realidade fática, haja vista que o crime em questão está relacionado a bem jurídico imaterial; a conduta violou a intimidade e imagem da atriz.

A partir deste acontecimento as autoridades legislativas se mobilizaram e nasceu, assim, a Lei 12. 720/2012. Esta lei, ao contrário dos anteriores projetos de lei, traz poucas alterações ao Código Penal, senão vejamos:

O único dispositivo criado que tipifica determinada conduta como crime é o art. 154-A que trata da "invasão de dispositivo informático". Entende que pratica-se esse crime, o agente que comete a seguinte conduta: "*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".*

Deste crime há de se notar algumas observações. Percebe-se que a vítima não necessariamente precisa ser a proprietária do dispositivo informático, figurando no mesmo sentido aquela vítima que utiliza o computador em *lans houses*, por exemplo. E mais, vale apontar que constitui um indiferente penal o fato do dispositivo estar ou não conectado à internet.

O crime em questão possui duas finalidades não cumulativas. A primeira é a conduta de invadir dispositivo informático, mediante violação indevida de mecanismo de segurança, *com o fim de obter, adulterar ou destruir dados ou informações.* Já a segunda conduta corresponde a invadir dispositivo informático para instalação de *vulnerabilidades para obter vantagem ilícita*.

Sucede que o dispositivo em comento demonstra falhas, pois não conceitua expressões técnicas da seara informática como "dispositivo infomático" e "vulnerabilidades" (esta útilma expressão deve ser entendida como vírus, cavalos de tróia dentre outros). Ademais, como a lei criou um tipo com finalidades especiais, se o agente, dolosamente, invade um computador, analisa documentos e imagens da vítima, porém não danifica qualquer documento o fato é considerado atípico.

Vale apontar ainda que para o cometimento do fim especial do tipo, o agente tem que "quebrar" o sistema de segurança do dispositivo informático, o que demonstra, portanto, que se o computador estiver sem qualquer dispositivo de segurança ativo, como por exemplo, antivírus, a conduta na repercutirá efeitos ao enquadramento penal. Assim aponta o advogado Auriney Brito:

> Um detalhe importante que deve ser observado, que difere este tipo penal de outros tipos penais comuns, é a elementar mediante *violação indevida de mecanismo de segurança.* Isso significa que só haverá o crime do Art.

> 154 do CP se o autor da conduta usar sua habilidade para superar a proteção do sistema informático, por mais simples que ela seja. E se o dispositivo estiver completamente desprotegido? Neste caso a invasão não poderá ser punida por não ter ocorrido *mediante violação de segurança*.[11]

Por fim a presente lei alterou a redação dos arts. 266 e 298 do Código Penal para adequá-los a realidade cibernética.

O art. 266 teve a sua titulação alterada para inserir a interrupção quanto aos serviços informáticos. Agora tal dispositivo trata do seguinte delito "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública"**.**

Quanto ao art. 298, em seu parágrafo único, o legislador equiparou como documento particular os cartões de crédito e débito no delito de falsificação de documento.

Percebe-se que em razão do fato ocorrido com a atriz global ter ganhado repercussões midiáticas, a lei em comento foi criada na pressa, sem ao menos possibilitar a responsabilidade penal de provedores e dispor de outras condutas que possivelmente possam violar bens considerados relevantes para o homem moderno, como dano informático, o acesso não autorizado e a obtenção ilegal de dados/engenharia social.

E mais, estudiosos sobre o tema ainda afirmam que uma alteração no Código Penal não é uma *conditio sine qua non* para que se possa combater e coibir de forma eficaz os cibercrimes. O professor de Direito Penal da Faculdade Federal de Minas Gerais e Mestre em Ciências Penais pela UFMG Túlio Lima Vianna assevera que o nosso ordenamento não necessita de leis regulamentadoras e sim, um aparato técnico e específico nas investigações forenses por parte das polícias quanto a estes delitos e uma ação conjunta entre os diversos entes que corporificam o Poder Judiciário e o Ministério Público. Observe tal entendimento:

> Por todo o exposto, defendemos a tese de que o problema da prevenção e repressão aos crimes pela Internet é, antes de tudo, um problema técnico e não jurídico. De nada adiantará acrescentarmos o tipo penal de violação de computadores em nossa legislação se nossas polícias não estiverem treinadas para investigarem e instruírem efetivamente um inquérito sobre tais crimes.

---

[11] BRITO, Auriney. **Análise da Lei 12. 737/12- " Lei Carolina Dieckmann"**. Disponível em: <http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>. Acesso em 20 jun. 2013

> Não podemos encarar a necessidade de uma reforma legislativa como uma conditio *sine qua non* para a repressão dos crimes pela Internet. É preciso que se aja desde já, criando-se delegacias especializadas no combate a crimes por computador e procurando punir os crimes já tipificados em nosso ordenamento jurídico.
> O problema da prevenção dos crimes pela Internet no Brasil é antes de mais nada o problema da repressão, ou seja, da efetiva aplicação da lei penal já existente às novas circunstâncias que se apresentam. De nada vale criarmos leis para reprimirmos os novos crimes se elas não puderem ser aplicadas por falta de treinamento de nossos policiais, de nossos promotores e de nossos magistrados. O melhor meio de se prevenir um crime é indubitavelmente o exemplo dado pela efetiva e correta aplicação da norma repressiva. [12]

Este também significa o entendimento do autor Fabrízio Rosa ao asseverar que mais do que lei, deve existir uma atuação conjunta dos principais instituições organizadas que integram o Poder Judiciário no âmbito nacional e internacional:

> É imperioso frisar, por derradeiro, que nenhum combate sério aos "Crimes de Informática" se esgota no processo tipificador. Sem a cooperação internacional, sem a melhoria do aparelhamento policial e judicial e sem o aperfeiçoamento profissional dos que operam nessas áreas, a simples existência de uma adequada tipificação não tem o menor significado prático e não basta para tutelar a sociedade contra tão lesiva atividade criminosa. Resta concluir, portanto, que o controle dos "Crimes de Informática" deve merecer uma atenção especial. Temos, pois, como uma observação realmente consistente na ciência penal e que como tal deveria ser levada em maior conta pelo legislador, o fato de que tanto um excesso de tutela penal quanto seus defeitos podem prejudicar que se atinja o objetivo teleológico do sistema.[13]

O autor Marcelo Crespo, em sua obra *Crimes Ditiais,* realizada antes da Lei 12. 720/2012, quando então era favorável a aprovação de uma lei sobre o tema, já fazia severas críticas quanto a construção teórica de novos delitos, principalmente no tocante a redação do texto e a responsabilidade dos provedores, senão vejamos tal observação:

> Nota-se que são muitas as propostas de inovação. Todavia, apesar de o projeto ser salutar, porque pretende punir condutas que cada vez mais trazem prejuízos e muitos problemas a todos os que usam tecnologia, peca pela má redação dos dispositivos, muitas vezes ignorando modelos ou

[12] VIANNA, Túlio Lima**. .Do delito de dano e de sua aplicação ao Direito Penal informático**. Disponível em: < http://www.buscalegis.ufsc.br/revistas/files/anexos/6027-6019-1-PB.pdf>. Acesso em: 5 mai. 2012.
[13] ROSA, Fabrízio**. *Crimes de informática***. 1.ed., p. 72.

> fórmulas já usados por nossas leis. Em suma, projeto que trate do assunto "crimes digitais" e assuntos correlatos é desejável, todavia, é necessário amadurecer algumas ideias, especialmente quanto à redação dos tipos penais e, ainda, da imposição de obrigações aos provedores de acesso.[14]

4. Problemáticas na seara dos crimes cibernéticos

Pensar na consecução dos crimes na internet vai além da disciplina disposta em um ordenamento jurídico. Chama atenção da doutrina e da jurisprudência que alguns crimes digitais para a uma persecução eficiente, requerem especialização técnica nas investigações para facilitar a identificação dos agentes delituoso (virtuais) e uma compreensão maior de como o crime acontece e consequente processamento. Vejamos.

4.1 Autoria

A identificação dos autores que cometem crimes no sistema de informação é um dos trabalhos mais áduos desempenhados pelas autoridades policiais e frisa-se, dificuldade esta encontrada não só pelo Brasil, como também pela comunidade internacional.

Importante salientar, primeiramente, que, em sua maioria, os autores destas práticas delituosas são dotados de conhecimentos específicos e já foram batizados pela comunidade cibernética como os agentes delituosos no cometimento destes crimes. Ocorre que existem hoje diversas denominações para estes vilões do crime. Senão vejamos alguns tipos destes *ciberdelinquentes.*

4.1.1 Craker

No cenário da informática existem os termos *hacker* e *cracker* que não podem ser confundidos, pois são elementos que trabalham em lados opostos. O *hacker*, termo que significa "pirata", invade um sistema em benefício próprio, mas que não comete condutas delituosas, ao contrário, criam novos programas e utilizam suas habilidades na consecução de sistemas.

---

[14] CRESPO, Marcelo Xavier de Freitas. ***Crimes Digitais,*** p. 170.

Por outro lado, o *cracker* é aquele *expert* que utiliza de seus conhecimentos para provocar um prejuízo alheio. Acrescenta Crespo (2011) que o *cracker* "é aquele que "quebra" um sistema de segurança, invadindo-o".

Por isto, a diferença, então, reside na utilização, porque enquanto o *hacker* utiliza os seus conhecimentos para o bem, o *cracker*, segundo dado extraído do *site Sisnema* são:

> (...) elementos mal intencionados, que estudam e decodificam programas e linguagens a fim de causar danos a computadores alheios. A intenção é invadir e sabotar sistemas, quase sempre objetivando a captação de dados passíveis de render cifras. Ou seja, roubo eletrônico, estelionato ou o que quer que seja. A intenção é definitivamente ruim.[15]

4.1.2 Carder

São os especialistas em estelionato. Ao se aproveitarem das falhas no sistema de segurança das administradoras de cartão de crédito e da negligência dos usuários criam programas para realizar compras em cartões de crédito alheio.

Segundo Crespo (2011), este criminoso depois de ter subtraído os números correspondentes dos cartões de crédito, "os distribui no IRC's[16] a fim de não ser descoberto, porque dessa forma muitas pessoas podem ter acesso aos números, sendo muito difícil saber quem os subtraiu".

A título ilustrativo, o Procurador da República Vladimir Aras cita que, de acordo com Associação Brasileira das Empresas de Cartões de Crédito e Serviços — Abecs:

> (...) as perdas com fraudes no ano passado atingiram R$200 milhões. No ano anterior, o prejuízo foi de R$ 260 milhões e, em 1998, de R$300 milhões". A Abecs tem se preocupado com os cibercrimes praticados mediante o uso fraudulento de cartões de crédito e está introduzindo no mercado os cartões com chips eletrônicos, que têm alto nível de segurança.[17]

---

[15] Disponível em: <http://: http://sisnema.com.br/Materias/idmat014717.htm> .Acesso em: 3 set. 2011.

[16] IRC's significa Internet Relay Chat e equivalem a salas de bate papo. Disponível em: < http://www.infoescola.com/internet/internet-relay-chat-irc/>. Acesso em: 8 fev. 2012.

[17] ARAS, Vladimir. ***Crimes de informática. Uma nova criminalidade***. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2250>. Acesso em: 4 set. 2012.

4.1.3 Phreaker

Nome dado aos *experts* em telefonia para modificar internamente as linhas telefônicas. Isto ocorre, pois utilizam de seus domínios informáticos para fazer ligações gratuitas e escutas telefônicas clandestinas.

In casu, o criminoso utiliza de mecanismo no computador capaz de que quando um telefone almejado toque possibilite a ele que escute toda a conversa; já no tocante às ligações gratuitas, o *phreaker*, segundo Crespo (2011) "fazem com que as operadoras se confundam quanto à origem de uma ligação" permitindo, assim, que o usuário legítimo que utiliza os serviços de determinada telefonia pague pela ligação realizada pelo delinquente.

Assim explicitado, é importante mencionar que a atuação destes agentes delituosos é cometida no anonimato e por isto, a polícia encontra muitas vezes dificuldade na identificação destes. Em outros casos, estes agentes utilizam pseudônimos, dados falsos para praticar os delitos.

Assim, segundo Vladimir Aras:

> O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário.[18]

4. 2 Lugar do crime

Lugar do crime, comumente conhecido pela doutrina penalista, corresponde ao local em que o crime está sujeito à lei penal de determinado país. Segundo o ilustre Damásio de Jesus, "como cada Estado possui sua própria soberania, surge o problema da delimitação espacial do âmbito de eficácia da legislação penal".[19]

---

[18] ARAS, Vladimir. *Crimes de informática.* ***Uma nova criminalidade.*** Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2250>. Acesso em: 4 set. 2012.
[19] JESUS, Damásio E.de. ***Direito Penal.*** 27. ed., p. 121.

Acerca do tema, o Código Penal, previsto em seu art. 6º, adotou a teoria da ubiquidade em que o território de um país pode abraçar a qualquer dos momentos do crime, seja os atos executórios seja os atos consumativos do delito.

Neste sentido, ainda de acordo com o doutrinador Damásio:

> Assim, quando o crime tem início em território estrangeiro e se consuma no Brasil, é considerado praticado no Brasil. Nestes termos, aplica-se a lei penal brasileira ao fato de alguém, em território boliviano, atirar na vítima que se encontra em nosso território, vindo a falecer; como também ao caso de um estrangeiro expedir a pessoa que viva no Brasil um pacote de doces envenenados, ou uma carta injuriosa. Do mesmo modo, tem eficácia a lei penal nacional quando os atos executórios do crime são praticados em nosso território e o resultado se produz em país estrangeiro.[20]

Diante disto, a respeito das novas práticas delituosas cometidas no âmbito da internet, é importante mencionar que o conceito supramencionado teve de se adaptar a esta nova modalidade delituosa, isto porque com o surgimento do chamado mundo virtual, a noção de espaço transcende o ambiente físico, hoje conhecido por *ciberespaço.*

O "lugar" dos crimes cibernéticos pode ser analisado sob diversos olhares, pois em um dado território pode ocorrer todos os *inter* crimes ou haver um rompimento das etapas do crime, como acontece nos chamados crimes fronteiriços em que abraçam diversos países. O autor Marcelo Crespo cita um exemplo elucidativo da questão:

> Sob uma ótica prática, uma pessoa que vive no Brasil pode modificar dados armazenados na Itália, transferindo-os para a Alemanha de modo a obter vantagem ilícita. Da mesma forma um vírus de computador pode ser desenvolvido em um país e disseminado por milhares de máquinas por todo o globo terrestre. A transmissão de dados pode envolver diversos países, de modo que o lugar do crime seja determinado de forma quase fortuita.[21]

Por isto, é perceptível que nos crimes cometidos no âmbito da internet as práticas delituosas podem ser cometidas facilmente entre países, visto que, diferente do seu aspecto físico, aqui os territórios não possuem fronteiras a serem respeitadas, o que exige dos países

[20] JESUS, Damásio E.de. ***Direito Penal***. 27. ed., p. 129**.**
[21] CRESPO, Marcelo Xavier de Freitas. ***Crimes Digitais***, p. 117**.**

um compromisso muito maior em detectar a territorialidade da internet e posterior combate aos cibercrimes.

4.3 Competência

Para definir o foro competente se faz necessário perceber qual circunstância e foro o crime foi concebido. Segundo Celson Valin apud Aras, a problemática em torno da territorialidade da internet "reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?".[22]

Em regra, de acordo com a nossa atual jurisdição processual penal, nos moldes do art. 70 do Código de Processo Penal, a competência é definida pelo lugar em que a infração for consumada, ou, no caso de tentativa, pelo local em que foi praticado o último ato de execução.

Diante o exposto há de se constatar a primeira problemática, pois nos crimes cometidos na internet, o grau de dificuldade encontrado pelas autoridades policiais é imensurável na identificação do local em que se deu o crime.

Isto porque, o agente delituoso geralmente não utiliza seu próprio computador para cometer as mais diversas infrações e sim, de lanhouses, bibliotecas em universidades, *shoppings*, ou seja, lugares públicos. Ainda assim, no processo investigatório é perceptível a utilização de dados e *e-mails* falsos e até mesmo a proliferação de vírus a fim de mascarar as condutas delitivas.

Neste sentido, a jurisprudência dos Tribunais Superiores já vem consolidando, em alguns julgados, determinadas diretrizes processuais no âmbito cibernético. A este tema, o Superior Tribunal de Justiça entendeu que a competência para processal e julgar crimes de racismo praticado na internet é o do local onde partiram as mensagens de cunho ofensivo racista, conforme anuncia o art. 70 do CPP. Entrementes, caso a conduta seja praticadas por diferentes agentes e em lugares diversos, mas contaram com o mesmo *modus operandi*

[22] ARAS, Vladimir. ***Crimes de informática. Uma nova criminalidade.*** Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2250>. Acesso em: 4 set. 2012.

restará configurado o nexo probatório e portanto a competência será daquele juízo que conheceu primeiro os fatos, sob o fundamento. Confira o julgado:

> PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE RACISMO PRATICADO PORINTERMÉDIO DE MENSAGENS TROCADAS EM REDE SOCIAL DA INTERNET.USUÁRIOS DOMICILIADOS EM LOCALIDADES DISTINTAS. INVESTIGAÇÃODESMEMBRADA. CONEXÃO INSTRUMENTAL. EXISTÊNCIA. COMPETÊNCIA FIRMADAPELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAMINÍCIO.
> 1. A competência para processar e julgar o crime de racismopraticado na rede mundial de computadores estabelece-se pelo localde onde partiram as manifestações tidas por racistas. Precedente daTerceira Seção.
> 2. No caso, o procedimento criminal (quebra de sigilo telemático) teve início na Seção Judiciária de São Paulo e culminou naidentificação de alguns usuários que, embora domiciliados emlocalidades distintas, trocavam mensagens em comunidades virtuaisespecíficas, supostamente racistas. O feito foi desmembrado emoutros treze procedimentos, distribuídos a outras seçõesjudiciárias, sob o fundamento de que cada manifestação constituíacrime autônomo.
> 3. Não obstante cada mensagem em si configure crime único, háconexão probatória entre as condutas sob apuração, pois acircunstância em que os crimes foram praticados - troca de mensagensem comunidade virtual - implica o estabelecimento de uma relação deconfiança, mesmo que precária, cujo viés pode facilitar aidentificação da autoria.
> 4. Caracterizada a conexão instrumental, firma-se a competência pelaprevenção, no caso, em favor do Juízo Federal de São Paulo - SJ/SP,onde as investigações tiveram início. Cabendo a este comunicar oresultado do julgamento aos demais juízes federais para onde osfeitos desmembrados foram remetidos, a fim de que restituam osautos, ressalvada a existência de eventual sentença proferida (art. 82 do CPP).
> 5. Conflito conhecido para declarar a competência do Juízo Federalda 9ª Vara Criminal da Seção Judiciária de São Paulo, o suscitante. (CC 116926 SP 2011/0091691-2 Relator(a): Ministro SEBASTIÃO REIS JÚNIOR, S3 - TERCEIRA SEÇÃO, DJe 15/02/2013)

É válido mencionar aqui a competência da Justiça Federal, nas situações de crimes fronteiriços ou demais crimes federais. É certo que a nossa Constituição Federal, em seu art. 109, inciso IV, estabeleceu competência aos juízes federais julgar as infrações praticadas em detrimento de bens, serviços ou interesses da União ou de suas entidades autárquicas ou empresas públicas. Assim, competente é a Justiça Federal para julgar os crimes cibernéticos contra a Administração Pública, a exemplo do art. 313-A do Código Penal (inserção de dados falsos em sistema de informação).

Também determinou a estes juízes federais o julgamento de crimes previstos em tratados ou convenção internacional, quando a infração for iniciada no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente, conforme art. 109, inciso V da Constituição Federal.

Desta forma, crimes de racismo e pedofilia, por exemplo, que estão previstos em convenções internacionais, ficariam sujeitos a julgamento dos juízes federais em caso destes crimes serem cometidos no âmbito da internet e que os atos de execução do crime ou até a sua consumação fosse além das fronteiras nacionais. Observe o entendimento do Tribunal Regional Federal da 1º Região:

> PROCESSUAL PENAL - CRIME PREVISTO NO ART. 241 DA LEI 8.069/90 - CONVENÇÃO SOBRE OS DIREITOS DA CRIANÇA, SUBSCRITA PELO BRASIL - TRANSNACIONALIDADE DO CRIME DE INSERÇÃO DE FOTOGRAFIAS PORNOGRÁFICAS DE CRIANÇAS, NA REDE INTERNACIONAL - COMPETÊNCIA DA JUSTIÇA FEDERAL - ART. 109, V, DA CF/88 -PRECEDENTES - RECURSO PROVIDO. I - O art. 109, V, da CF, estabelece que compete aos juízes federais processar e julgar "os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente". II - A competência da Justiça Federal para processar e julgar o crime previsto no art. 241 da Lei 8.069, de 13/07/1990 é da Justiça Federal, por ser o Brasil signatário da Convenção sobre os Direitos da Criança, promulgada pelo Decreto nº 99.710, de 21/11/1990, desde que presente a transnacionalidade do delito. III - "Diante de existência de tratado ou convenção internacional que prevê o combate à prática de atividades criminosas, envolvendo menores, e, sendo o Brasil signatário da Convenção sobre os Direitos da Criança, a competência para processar e julgar o feito é da Justiça Federal. A inserção de fotos pornográficas de crianças na rede internacional permite a publicação instantânea, seja no Brasil seja no exterior, o que dá lugar à competência da Justiça Federal". (RSE 2007.38.00.025788-1/MG, Rel. Des. Federal Tourinho Neto, 3ª Turma do TRF/1ª Região, unânime, e-DJF1 de 19/12/2008, p. 395) IV - A transnacionalidade de tais delitos, cometidos pela Internet, é inerente ao próprio ambiente da rede, que permite o acesso de qualquer pessoa à página do ORKUT, em qualquer lugar do mundo, desde que conectada à rede e pertencente à referida rede social. V - Recurso provido, para reconhecer a competência da Justiça Federal. (RSE 201040000007873, DESEMBARGADORA FEDERAL ASSUSETE MAGALHÃES, TRF1 - TERCEIRA TURMA, e-DJF1 DATA:06/08/2010 PAGINA:35.)

5. Conclusão

Nota-se que o chamado *ciberespaço* é tido por agentes delituosos como um meio bem proveitoso para o cometimento de delitos que já estão previstos no ordenamento penal, afetando toda a sociedade.

A Lei 12. 737/2012 trouxe uma inovação ao cenário jurídico penal atendendo aos anseios da comunidade jurídica e de toda a sociedade que presenciavam determinadas condutas na internet, consideradas lesivas ao homem, porém mantiam-se silentes quanto ao combate destas em virtude da ausência de tipificação penal.

É preciso, contudo, observar que a lei em comento não possui o condão de aniquilar com os crimes cometidos na internet. Isto porque, vivemos no mundo em constante evolução tecnológica e assim, o Código Penal tende a não acompanhar a possível chegada de novas condutas lesivas a bens considerados relevantes para uma sociedade moderna.

Diante disto, resta evidente que a inovação criminológica requer muito mais que um diploma legal regulamentando contudas delituosoas, Tais crimes necessitam também serem enfrentados por um poder investigatório mais apurado, pois muitos dos crimes cometidos na internet envolvem a atuação de agente com aguçado conhecimento informático e assim, de nada vale uma lei que insira no ordenamento jurídico pátrio novos tipos penais ao Código Penal e o Poder Judiciário, Ministério Público e as polícias civil e federal não estejam empenhados e preparados tecnicamente na prevenção e repressão destes crimes.

Afinal, a lei sozinha não produzirá a eficácia necessária já que depende de uma atuação conjunta dos órgãos mencionados a fim de melhor regulamentá-la, principalmente um investimento na criação de novas delegacias especializadas e no treinamento de policiais no tocante as investigações forenses.

REFERÊNCIAS

ADAMI, Anna. **Internet Realy Chat (IRC**). Disponível em: < http://www.infoescola.com/internet/internet-relay-chat-irc/>. Acesso em: 8 fev. 2012.

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2250>. Acesso em: 4 set. 2012.

BRASIL. **Constituição Federal**. In: Vade Mecum: Universitário de Direito. Organização de Anne Joyce Angher. 11. Ed. Atual. São Paulo: Rideel, 2012.

_____. **Código Civil**. In: Vade Mecum: Universitário de Direito. Organização de Anne Joyce Angher. 11. Ed. Atual. São Paulo: Rideel, 2012.

_____. **Código de Defesa do Consumidor**. In: Vade Mecum: Universitário de Direito. Organização de Anne Joyce Angher. 11. Ed. Atual. São Paulo: Rideel, 2012.

_____. **Código Penal**. In: Vade Mecum: Universitário de Direito. Organização de Anne Joyce Angher. 11. Ed. Atual. São Paulo: Rideel, 2012.

_____. **Código de Processo Civil**. In: Vade Mecum: Universitário de Direito. Organização de Anne Joyce Angher. 11. Ed. Atual. São Paulo: Rideel, 2012.

_____. **Projeto de Lei nº 84/99**. Disponível em: <http:// http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028> Acesso em: 2 set.2011.

_____. **Projeto de Lei nº 89/2003**. Disponível em: <http:// http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=63967> Acesso em 2 set.2011.

_____. **Projeto de Lei nº 2793/2011**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 14 mai. 2012.

_____. **Anteprojeto Código Penal**. Disponível em: < http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=100768> . Acesso em: 21 mai. 2012.

BRITO, Auriney Uchôa de. ***O bem jurídico-penal dos delitos informáticos***. Boletim-Publicação Oficial do Instituto Brasileiro de Ciências Criminais, n° 199, junho/2009, p14-15.

_____. **Análise da Lei 12. 737/12- " Lei Carolina Dieckmann"**. Disponível em: < http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/> . Acesso em 20 jun. 2013.

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

HAJE, Lara. **ESPECIAL - Proposta sobre crimes cibernéticos tramita há 12 anos no Congresso.** Disponível em: < **http://www.camara.gov.br/internet/jornalcamara/default.asp?selecao=materia&codMat=70377> .**Acesso em: 4 mai. 2012.

JESUS, Damásio E.de. **Direito Penal**. 27. ed.v.1. São Paulo: Saraiva, 2003.

JR, Fredie Didier; Cunha, Leonardo. **Curso de Direito Processual Civil**. 2 ed. v.5. Salvador: Jus Podivm, 2010.

PINTO, Marcio Morena. **O Direito da internet: o nascimento de um novo ramo jurídico**. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2245>. Acesso em: 8 fev 2012.

ROSA, Fabrízio. **Crimes de informática**. 1.ed. Campinas: Brooksleller, 2002.

SISNEMA, Informática. **Cracker e Hacker: Experts trabalhando em sentidos opostos**. Disponível em: < http:// http://sisnema.com.br/Materias/idmat014717.htm> Acesso em: 12 jan. 2012.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Local de hospedagem do site define competência para ação por calúnia em blog jornalístico**. . Brasília: 2001. Disponível em: <. http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=101559> . Acesso em: 5 mai. 2012.

_____. **Justiça usa Código Penal para combater crime virtual**. Brasília. 2008. Disponível em: < http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=90108>. Acesso em: 25 jun. 2012.

TANABE, Silvio. **MARKETING DIGITAL | PUBLICIDADE NA INTERNET É O QUE MAIS INFLUENCIA NAS COMPRAS**. Disponível em: < http://clinicamarketing8ps.com.br/marketing-digital-publicidade-na-internet-e-o-que-mais-influencia-nas-compras/>. Acesso em: 9 ago. 2012.

_____. **Do delito de dano e de sua aplicação ao Direito Penal informático**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/anexos/5988-5980-1-PB.pdf>. Acesso em: 5 mai. 2012.

http://www.jf.jus.br/juris/unificada/.

http://www.jusbrasil.com.br/jurisprudencia.