



## OS CRIMES CIBERNÉTICOS E O DIREITO A SEGURANÇA JURÍDICA: UMA ANÁLISE DA LEGISLAÇÃO VIGENTE NO CENÁRIO BRASILEIRO CONTEMPORÂNEO

### CYBER CRITICS AND THE RIGHT TO LEGAL SECURITY: AN ANALYSIS OF LEGISLATION IN THE CONTEMPORARY BRAZILIAN SCENARIO

Liara Ruff Dos Santos<sup>1</sup>

Luana Bertasso Martins<sup>2</sup>

Francielle Benini Agne Tybucsh<sup>3</sup>

#### RESUMO

O presente trabalho tem por escopo ressaltar a importância do acesso à internet como meio de ampliação das fronteiras da comunicação, ao mesmo tempo em que apresenta novas possibilidades para a criminalidade, agora virtual ou digital. Diante deste cenário, a pesquisa busca refletir sobre: Quais são os crimes virtuais mais frequentes no Brasil, considerando os estados da federação, no período após a Lei 12.737/2012 denominada Carolina Dieckman entre outras? Para responder a essa questão de pesquisa, a metodologia utilizou-se da pesquisa bibliográfica e do método dedutivo. Assim, o estabelecimento de direitos e deveres cibernéticos, ainda que tardio, é de extrema importância para o combate dos crimes virtuais, uma vez que através dessas normas poderá ser vislumbrada com mais facilidade o que está sendo violado, estabelecendo assim as condutas ilícitas.

Palavras-chave: Crimes Cibernéticos; Segurança; Legislação vigente.

<sup>1</sup> Autora. Acadêmica do Curso de Direito na Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Câmpus de Santiago, RS. E-mail: [liara\\_santos17@hotmail.com](mailto:liara_santos17@hotmail.com)

<sup>2</sup> Autora. Acadêmica do Curso de Direito na Universidade Regional Integrada do Alto Uruguai e das Missões. E-mail: [bertassoluana@gmail.com](mailto:bertassoluana@gmail.com)

<sup>3</sup> Orientadora. Doutoranda em Direito pela Universidade do Vale do Rio dos Sinos - UNISINOS. Mestre pela Universidade Federal de Santa Maria, no Programa de Pós-Graduação em Direito, com ênfase em Direitos Emergentes na Sociedade Global, linha de pesquisa Direitos da Sociobiodiversidade e Sustentabilidade. Possui graduação em Direito pela Faculdade Palotina de Santa Maria - FAPAS. Professora da Universidade Regional Integrada do Alto Uruguai e das Missões - URI/Santiago. Membro da equipe técnica da Revista Direitos Emergentes na Sociedade Global da Universidade Federal de Santa Maria - UFSM. Integrante do Grupo de Pesquisa em Direito da Sociobiodiversidade (GPDS) da UFSM e do Grupo de Pesquisa em Direito, Risco e Ecocomplexidade da UNISINOS. E-mail: [francielleagne@gmail.com](mailto:francielleagne@gmail.com)



## ABSTRACT

The purpose of this paper is to emphasize the importance of access to the Internet as a means of expanding the communication frontiers, while at the same time presenting new possibilities for crime, now virtual or digital. Given this scenario, the research seeks to reflect on: What are the most frequent virtual crimes in Brazil, considering the states of the federation, in the period after Law 12.737 / 2012 named Carolina Dieckman among others? In order to answer this research question, the methodology was based on bibliographical research and the deductive method. Thus, the establishment of cyber rights and duties, even if late, is of extreme importance for the fight against virtual crimes, since through these norms can be seen more easily what is being violated, thus establishing illicit conduct.

Keywords: Cyber Crimes; Safety; Current legislation.

## INTRODUÇÃO

No Brasil, pesquisas demonstram que 36,8 milhões de lares possuem conexão com a internet e que os aparelhos móveis viraram a opção número 1 para o acesso, tornando - se assim o 78º país de 202 com a maior cobertura de rede<sup>4</sup>. Dessa forma, a internet se tornou uma ferramenta de extrema importância para o mundo globalizado, pois além de relacionar pessoas, transmitir informações é também um meio de comércio.

Mas nem só de benefícios vive a Internet, na mesma proporção a quantidade dos ilícitos aumentaram assustadoramente e que por ser um objeto de grande utilidade pode ser usado como veículo para pessoas mal intencionadas e que agem de má fé para a prática de crimes, desse modo busca - se fazer um reconhecimento das normas vigentes para tais crimes.

Portanto, a internet, ao mesmo tempo em que assume no mundo da comunicação contemporânea a condição técnica - científica de maior fonte universal de agilidade no tráfico de informações direcionadas a pesquisas de novos conhecimentos, transforma - se também em instrumentos perigo para a divulgação de acusações falsas e irresponsáveis sendo ameaças, inverdades, violências, sem pouca ou quase nenhuma possibilidade de repressão ou punição aos infratores.

<sup>4</sup> IBGE. Coordenação de Trabalho e Rendimento. **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal**. Rio de Janeiro: IBGE, 2016. Disponível em: <http://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=295753> Acesso em: 10 de agosto de 2017.



Diante deste cenário, o trabalho tem como questionamento refletir sobre: Quais são os crimes virtuais mais frequentes no Brasil, considerando os estados da federação, no período após a Lei 12.737/2012 denominada Carolina Dieckman entre outras? Para responder a essa questão de pesquisa, a metodologia utilizou-se da pesquisa bibliográfica e do método dedutivo. Como método de procedimento, na pesquisa em tela foi utilizado à análise bibliográfica e documental acerca da temática. Como técnica de coleta de dados optou-se pela produção de fichamentos e resumos estendidos.

## 1 O AVANÇO DA TECNOLOGIA E DAS ILICITUDES EM REDE

O primeiro computador digital foi criado em 1946, chamado de ENIAC, ele tinha a simples e única finalidade de automatizar o cálculo de tabelas balísticas. No entanto, desde então podemos perceber as suas inúmeras mudanças e as vantagens trazidas conseqüentemente, seja para comunicação, realizar compras, notícias em tempo real, dentre outras.

O meio virtual tem se apresentado como local de grande incidência da criminalidade, de modo que o desconhecimento de alguns se transforma no poder e lucro para outros. “A internet é uma grande praça pública, o maior espaço coletivo do planeta”<sup>5</sup>.

Porém, apesar das inúmeras ampliações desde a evolução do mundo virtual, abriu - se uma oportunidade também para a prática de crimes, e com a mundialização isto se tornou prático, rápido e corriqueiro.

Ciberespaço é definido como um mundo virtual porque está em presente potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, outra realidade<sup>6</sup>. Os delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão. Os crimes virtuais são cada vez mais comuns porque as pessoas cultivam a sensação de que o ambiente virtual é uma terra sem leis.

<sup>5</sup> CASSANTI, Moisés de Oliveira. *Crimes Virtuais, Vítimas Reais*. Rio de Janeiro: Brasport, 2014, p. 03.

<sup>6</sup> MONTEIRO, Silvana Drumond. O ciberespaço: termo, a definição e o conceito. *Revista da Ciência da Informação*, v 8 n 3 jun/2017.



A falta de denúncias também incentiva fortemente o crescimento do número de golpes virtuais e violência digital (como o cyberbullying). Muito se fala sobre a carência de um conjunto de normas e sanções jurídicas dedicadas somente para os crimes digitais.

Porém, existindo ou não uma legislação específica para este assunto, quando o computador é usado como uma ferramenta para a prática de delitos e violência, estes crimes serão adaptados ao código penal já existente e os agressores e golpistas serão punidos da mesma forma.

### 1.1 Definições de Espaço Virtual e Ciberespaço

Ciber é um prefixo, que para muitos, é sinônimo de novas tecnologias. O Ciberespaço, existente no mundo de comunicação em que não é necessária a presença física do homem para constituir a comunicação, a interconectividade e o espaço que interligam pessoas, documentos e máquinas. Dentre eles a internet pode ser considerada o principal ambiente do ciberespaço (ou espaço virtual), devido à sua popularidade e utilização, mas ele também incorre em outras tecnologias, como outros serviços.

Gibson<sup>7</sup> foi o primeiro a se utilizar desse termo referindo - se a este espaço, em 1984, porém terminologicamente sua origem, da palavra Ciber, vem do grego, que significa controlar ou direcionar; logo o significado da palavra ciberespaço é espaço controlado ou espaço dirigido.

Na definição de Gibson:

Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos...Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infundáveis de dados. Como mares de luzes da cidade<sup>8</sup>.

Conceitua Silvana Drumond Monteiro que:

Ciberespaço é definido como um mundo virtual porque está em presente potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, outra realidade. O ciberespaço existe em um

<sup>7</sup> GIBSON, William. *Neuromancer*. 3. Ed. São Paulo: Aleph, 2003.

<sup>8</sup> GIBSON, William. *Neuromancer*. 3. Ed. São Paulo: Aleph, 2003, p. 67



local indefinido, desconhecido, cheio de devires e possibilidades. Não podemos, sequer, afirmar que o ciberespaço esta presente em nossos computadores, tampouco nas redes, afinal onde fica o ciberespaço? Para onde vai todo esse “mundo” quando desligamos nossos computadores? É esse caráter fluido do ciberespaço que o torna virtual<sup>9</sup>.

Compreende - se que o ciberespaço, é um novo tipo de sociedade aonde se realizam novas formas de relações sociais, a partir de que migramos de um mundo real, onde o território não é demarcado e nem possuem fronteiras, sendo apropriado em subjetividade que simulam uma projeção do mundo real, aonde executar uma tarefa na frente do computador nos possibilita a sensação de estar em um lugar determinado e presente.

Ainda, para Pierre Levy, um dos grandes estudiosos sobre esta temática, o ciberespaço é um espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores, amplia o ambiente. Estes novos meios de comunicação que coletam, manipulam, estocam, simulam, transmitem os fluxos materiais da informação e criam uma nova camada<sup>10</sup>.

Desta forma, como a tecnologia nunca é neutra, este ciberespaço pode ser um espaço de democracia, de expansão da informação ou de controle, e até de crimes virtuais, conforme será dissertado no item 2 deste trabalho.

## 2 CRIMES VIRTUAIS E CIBERCRIMES: Reflexos do *on line* no *off line*

### 2.1 Conceito e Classificação

Jorge e Wendt analisam que os crimes virtuais também chamados de crimes digitais, crimes eletrônicos, ciber crimes, crimes cibernéticos, entre outras nomenclaturas. São os nomes dados à atividade onde um computador ou rede destes é utilizado como base para cometimento de crimes ou facilitação para destes. Podendo se categorizar esses crimes de acordo com a sua forma de cometimento: os crimes que são cometidos utilizando o computador como instrumento para que se cometa a infração e aqueles que o

<sup>9</sup> MONTEIRO, Silvana Drumond. O ciberespaço: termo, a definição e o conceito. *Revista da Ciência da Informação*, v 8 n 3 jun/2017.

<sup>10</sup> LEVY, Pierre. *Cibercultura*. Trad. Irineu da Costa. Rio de Janeiro: Editora 34, 2003, p. 92.



crime é cometido contra o aparelho em si, o objeto é danificado ou violado de alguma forma<sup>11</sup>.

Focalizando-se na Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticada por meio da internet e crimes ou ações que merecem enquanto bem jurídico autônomo.

Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou<sup>12</sup>.

Ainda é possível classificar esses crimes em próprios, que são crimes que só podem ser praticados através dos meios informáticos, não tendo outros meios possíveis, e impróprios, que são crimes que podem ser praticados de qualquer forma, os computadores são apenas mais um meio para a execução destes crimes. No tocante a essas duas categorias, Marcelo Xavier de Freitas Crespo ressalta que:

Temos que para se cometer delitos classificados como impróprios não se verificam grandes diferenças quanto ao modus operandi. Em outras palavras, embora mude o modo pelo qual se pratica a ação delitativa, não se vislumbra a necessidade de conhecimentos técnicos. Já quanto ao ilícitos classificados como próprios, estes sim, dependem de conhecimento específicos de computação<sup>13</sup>.

### 3 PROCEDIMENTO/PROCESSO CRIMINAL NOS CRIMES VIRTUAIS

A existência do Direito está associado a jurisdição, e que sua função jurisdicional de resolução de conflitos entre pessoas e comunidades no espaço virtual, e de tutela jurisdicional do Poder público ou seja esteja conexa ao Estado. Ao que se trata dos crimes

<sup>11</sup> WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p. 10.

<sup>12</sup> GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim IBCCRIM, v. 8, 2000, p. 95.

<sup>13</sup> CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011, p. 94.





virtuais são os delitos praticados por meio da Internet que podem ser enquadrados no Código Penal brasileiro, e os infratores estão sujeitos às penas previstas na lei.

O Brasil é um país que não tem uma legislação definida e que abranja, de forma objetiva e geral, os diversos tipos de crimes cibernéticos que ocorrem no dia a dia e que aparecem nos jornais, na televisão, no rádio e nas revistas.

Na ausência de uma legislação específica, aquele que praticou algum crime informático deverá ser julgado dentro do próprio Código Penal, mantendo-se as devidas diferenças. Se, por exemplo, um determinado indivíduo danificou ou foi pego em flagrante danificando dados, dados estes que estavam salvos em CDs de sua empresa, o indivíduo deverá responder por ter infringido o artigo 163 do Código Penal, que é "destruir, inutilizar ou deteriorar coisa alheia: pena - detenção, de um a seis meses, ou multa".

Dentre os principais crimes cibernéticos, segundo uma pesquisa realizada pelo site Safernet estão: a pornografia infantil, pirataria, fraude e golpes, sabotagem informática, difamação, calúnia, injúria, dano, estelionato, crimes contra o sistema financeiro, ameaça, interceptação do fluxo de dados em tráfego por serviço de telecomunicação, apologia de crime ou de criminoso, violação de direito autoral, tráfico de substâncias estupefacientes, rufianismo, entre outros. Dos crimes citados a cima alguns serão explicados a seguir.

A pornografia infantil é caracterizada por fotografar ou publicar cenas de sexo explícito ou pornográfico que contenham crianças e adolescentes de acordo com o art. 241 do Estatuto da Criança e do Adolescente<sup>14</sup>. Assim, qualquer conteúdo publicado na internet, que possua imagens de crianças e adolescentes em situação pornográfica é caracterizado o crime de pornografia infantil.

Os crimes contra a honra estão elencados nos art. 138, 139 e 140 do Código Penal, e são eles a injúria, difamação e calúnia. Para que se caracterizem os crimes de calúnia e difamação pelo meio da internet, é necessário que a ofensa seja enviada para grande público, não apenas para a vítima, já para que ocorra a injúria, o envio da mensagem é para a própria vítima. Nos dois primeiros casos a ofensa será à sua honra objetiva e no segundo a subjetiva.

<sup>14</sup> DE INELLAS, Gabriel Cesar Zaccaria. *Crimes na Internet*. São Paulo: Juarez de Oliveira, 2004, p. 27.



No caso do crime de dano se fala em três hipóteses. Na primeira o crime acontece quando o agente transmite informação, programa, conteúdo ou comando que resulte em dano ao computador protegido. Na segunda hipótese, se caracteriza o crime quando o agente acessar computadores protegidos e culposamente causar o dano. E na última hipótese é punido o agente que acessar computadores protegidos, sem autorização e causar dano, porém nesta última hipótese o ato de acessar é intencional<sup>15</sup>.

Sendo assim, o dano que é falado seria o vírus transmitido aos computadores, assim caracterizando o crime de dano efetuado pela internet. O crime de estelionato praticado pela internet pode ser denominado como fraudes eletrônicas, ele acontece quando o sujeito ativo usa de meio informático, ou da internet para manter a vítima em erro, assim podendo obter vantagem ilícita para si ou para outrem.

Os crimes de sistema financeiro ocorrem quando, pelo meio da internet, o agente consegue, mediante fraude, financiamento em instituição financeira. Acontece o crime de ameaça através da internet quando, o sujeito ativo envia correio eletrônico a vítima, com a ameaça de mal injusto. Também por modalidade simbólica se caracteriza o crime, como imagens, pois com o uso de scanners, se torna possível o envio de desenhos e fotos para intimidar a vítima.

A interceptação de comunicações telefônicas, informações restritas adquiridas por meio de hackers na internet, ou quebrar segredo de justiça sem a autorização judicial se configura o crime de interceptação do fluxo de dados em tráfego por serviços de telecomunicações.

Também é considerado crime exaltar ou elogiar criminoso ou ato criminoso publicamente, configurando então o crime de apologia de crime ou de criminoso na internet. O crime de violação de direitos autorais, quando cometidos pelo meio de computadores, acontece quando o agente viola direito de autor de programa de computador.

Por fim, no tráfico de substâncias estupefaciente, o crime acontece quando o agente usa da internet para oferecer a consumo, substância entorpecente ou que sujeite indivíduo a dependência física ou psíquica, fazendo a oferta por meio de uma página criada por ele ou mesmo envio de mensagem pelo correio eletrônico. Boa parte dos ataques cibernéticos é executada pelos hackers, esse termo quando aconteceu o seu

<sup>15</sup> DE INELLAS, Gabriel Cesar Zaccaria. *Crimes na Internet*. São Paulo: Juarez de Oliveira, 2004, p. 41.





surgimento, em 1960, era usado para denominar pessoas que tinham o interesse em se aprofundar em programação de computadores, porém o sentido mudou com o surgimento e avanço da internet, passando a ser considerado os hackers como invasores de computadores alheios.

Para Gabriel Cesar Zaccaria de Inellas:

O hacker é considerado o intruso do mundo virtual. A invasão dos Sistemas alheios, pelo hacker, geralmente deve-se a um mero desejo de demonstração de sua perícia em informática e à curiosidade. Normalmente, não possui um ilícito específico. Todavia, sua conduta, por si só, já é considerada ilícita. Seu conhecimento lhes permite avaliar as falhas de um Sistema e violá-lo<sup>16</sup>.

Todo indivíduo considerado hacker sabe que todo Sistema de Segurança possui falhas, então eles se detêm a descobri-las, depois de encontrada, as denominam de porta, a qual será usada para violar o Sistema de determinado usuário. O hacker passa a ser perigoso pelo seu fato de poder, com a sua habilidade em descobrir as falhas dos Sistemas ele tem a possibilidade de modificar conteúdo de Sites, adentrar Sistemas de Governos e também de empresas, invadir computadores alheios, descobrir senhas de cartões de crédito ou contas bancárias e ainda fraudar as senhas de proteção de programas comerciais, sendo assim possível a pirataria de softwares.

Nesse sentido, Roberto Chacon de Albuquerque explana: “A adoção de novos tipos penais pode ter um efeito significativo no combate à impunidade, promovendo também um instituto de abstenção entre os hackers com relação à prática de crimes informáticos, em virtude do receio de serem punidos”<sup>17</sup>.

Neste panorama, pode-se destacar, até então, a atuação relativa do Estado Brasileiro, uma vez que somente em decorrência de alguns casos de grande repercussão midiática voltou sua atenção para esse assunto e procurou normatizar alguns ilícitos cometidos virtualmente.

<sup>16</sup> DE INELLAS, Gabriel Cesar Zaccaria. *Crimes na Internet*. São Paulo: Juarez de Oliveira, 2004, p. 15.

<sup>17</sup> ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática*. São Paulo, J. de Oliveira, 2006, p. 23.



A lei nº 12.737/2012<sup>18</sup>, popularmente conhecida como “Lei Carolina Dieckmann” que incluiu os artigos 154-A e 154-B, criando o crime de invasão de dispositivo informático e alterou os artigos 266 e 298, do Código Penal, exemplifica esta situação, haja vista ter sido criada após a grande repercussão que o vazamento de fotos íntimas dessa atriz teve no cenário nacional. A lei supracitada surgiu como alternativa à Lei Azeredo, a qual foi alvo de várias críticas em razão do temor de supressão da liberdade virtual, e, ao ser promulgada, somente previu a obrigatoriedade dos órgãos da polícia judiciária se estruturarem, para buscarem o combate de ações delituosas no meio virtual. A lei de crimes informáticos (leis 12.735/12 e 12.737/12) entrou em vigor na data de 02 de Abril de 2013, elas alteram o Código Penal para tratar dos crimes cibernéticos. Esta lei, a 12.735/12, transitou no congresso desde 1999 (PL 84/99, na câmara).

Em seu texto original ele era bem extenso e bastante polêmico no sentido da responsabilidade dos provedores de internet, mas apesar disso, durante sua tramitação foi reduzido a quatro artigos, sendo reduzida a dois por veto na sanção, pela presidente Dilma Rousseff.

Além destes existe o Decreto Federal nº 7.962/13, ele entrou em vigor na data de 14 de maio de 2013, seu objetivo era preencher as lacunas no Código de Defesa do Consumidor acerca do comércio em lojas virtuais, ou como é chamado o comércio eletrônico, visto que inexistia legislação específica sobre o processo de compra e venda na internet. “Com as novas regras, as empresas que atuam no comércio eletrônico terão que dispor em suas páginas informações sobre produtos, fornecedores, serviços e aperfeiçoamento do atendimento ao consumidor”<sup>19</sup>

Recentemente, a promulgação do Marco Civil da Internet pode ser estabelecida como um grande avanço na postura governamental em busca da regulamentação dos atos da sociedade civil praticados no meio digital. Esses são alguns exemplos da tentativa do Poder Estatal de se fazer mais presente no que diz respeito ao combate e prevenção dos ilícitos virtuais ainda não tipificados.

<sup>18</sup> BRASIL. Lei Nº 12.737, de 30 de novembro de 2012. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm) Acesso em: 10 de agosto de 2017.

<sup>19</sup> CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Brasport, 2014, p. 94.



### 3.1 Limites da Polícia Brasileira em investigação e combate aos cibercrimes

Após os diversos ilícitos ocorridos vistos, a criação de outros métodos para ao combate aos crimes virtuais tiveram de ser implantados, sendo um deles a criação de divisões especializadas em cibercrimes. A atividade policial seja ela desempenhada no mundo off-line ou no mundo online, seja ela atribuição da Polícia Federal ou Civil, deverá ser orientada por uma política de segurança pública e organizada e estruturada a partir de dados e informações inerentes ao lugar ou a matéria á quais as autoridades policiais estarão vinculadas.

Se tratando do poder e função da Polícia Brasileira no âmbito penal, praticado uma infração, a ela dará a apuração e o esclarecimento dos fatos e circunstâncias a ela etinentes. Em geral, três são os principais modelos de investigação preliminares, classificados de acordo com preside: a) investigação preliminar policial, desenvolvida pela polícia investigativa; b) investigação preliminar judicial, protagonizada pela atuação do juiz instrutor; c) investigação preliminar a cargo da acusação, nesse caso as figuras de investigador e acusador. Em geral é realizada essa função pelo Ministério Público.<sup>5</sup>

A investigação judiciária brasileira é geralmente exercida pela polícia judiciária, em âmbito administrativo. O inquérito policial brasileiro é, via de regra atividade da polícia judiciária. A polícia, apesar de vinculada diretamente ao Executivo, exerce também tarefas em atendimento ao Legislativo e ao Judiciário. Rolim defende que:

Para que esta política possa ser implementada é necessário o acesso a dados fundamentais sobre a incidência dos delitos e de suas circunstâncias, tais como o lugar da ingração, o perfil das vítimas, o horário das ocorrências e o modus operandi do crime. A ausência do atendimento a estes pressupostos resultaria, inevitavelmente, em uma política de segurança na qual se protagonizaria uma série de iniciativas desencontradas e improvisadas. A atividade policial desvinculada dos dados necessários á sua otimização tem como resultado uma baixa produtividade. A proposta de criação de divisões especializadas nas investigações de cibercrimes leva em consideração o aprimoramento científico e acadêmico da atividade policial em detrimento da ampliação quantitativa dos membros de suas corporações. Parte-se da proposição de uma política corporativa que direcione e organize setores, que sejam responsáveis precipuamente pela investigação dos crimes. Esta conjugação de esforços



poderia representar o que denominou de uma nova racionalidade no policiamento<sup>20</sup>.

Diante dessas ideias, podemos perceber que apesar de lenta a perspectiva de resolução dos cibercrimes, presenciamos um aperfeiçoamento do que está se tentando colocar em prática contra esses crimes. O Rio Grande do Sul agora tem uma delegacia especializada em crimes virtuais. Com o aumento de delitos desse tipo no Brasil e, também, na região, Polícia Civil do estado, criou -se em 2006 a Delegacia de Repressão aos Crimes Informáticos (DRCI). Além dos comuns delitos relacionados a fraudes bancárias e com cartões de crédito, a delegacia investigará, também, casos de crimes contra a honra (calúnia, injúria e difamação) e ameaça.

## CONCLUSÃO

Diante da temática conflituosa exposta neste artigo, foi questionado: Quais são os crimes virtuais mais frequentes no Brasil, considerando os estados da federação, no período após a Lei 12.737/2012 denominada Carolina Dieckman entre outras? A fim de abranger o questionamento, a pesquisa dividiu-se em três itens temáticos. O primeiro sendo ele o avanço da tecnologia e das ilicitudes em rede, que buscou fazer uma análise histórica e cronológica dos acontecimentos expostos. Em segundo momento tratou dos cibercrimes em si, apresentando seu conceito e sua classificação. Por terceiro e não menos importante, o procedimento/processo criminal para o combate aos cibercrimes perante a legislação atual.

Desse modo, entende que ainda discute - se sobre uma elucidação e descrição mais notória dos limites da responsabilidade civil ou criminal, e que por tal motivo devido a falta de legislação específica e abrangente acerca do tema, por vezes os Tribunais nacionais posicionam-se de forma não eficiente a esses crimes.

Assim, o estabelecimento de direitos e deveres cibernéticos, ainda que tardio, é de extrema importância para o combate dos crimes virtuais, uma vez que através dessas normas poderá ser vislumbrada com mais facilidade o que está sendo violado,

<sup>20</sup> ROLIM, Marcos. **A síndrome da Rainha Vermelha: Policiamento e Segurança Pública no Século XXI**. Rio de Janeiro: Jorge Zahar, 2006. p 44-61.



estabelecendo assim as condutas ilícitas. Diante disto denota - se que para a sua caracterização, o crime necessita de: a) uma tipificação expressa como crime por lei; b) conduta (comissiva ou omissiva); sendo que expressa como tal, esteja válida e apta a produzir efeitos perante todos (*erga omnes*).

## REFERÊNCIAS

- ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo, J. de Oliveira, 2006.
- BRASIL. **Lei Nº 12.737, de 30 de novembro de 2012**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm) Acesso em: 10 de ago de 2017.
- CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.
- COLLI, Maciel. **Cibercrimes: Limites e Perspectivas á Investigação Policial de Crimes Cibernéticos**. Curitiba: Juruá. 2010.
- CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000.
- CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.
- DE INELLAS, Gabriel Cesar Zaccaria. **Crimes na Internet**. São Paulo: Juarez de Oliveira, 2004.
- FELICIANO, Guilherme Guimarães. **Informática e Criminalidade**. Ribeirão Preto: Nacional de Direito, 2001.
- GIBSON, William. **Neuromancer**. 3. Ed. São Paulo: Aleph, 2003.
- GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim IBCCRIM, v. 8, 2000.
- IBGE. Coordenação de Trabalho e Rendimento. **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal**. Rio de Janeiro: IBGE, 2016. Disponível em: <http://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=295753> Acesso em: 10 de ago de 2017.
- LEVY, Pierre. **Cibercultura**. Trad. Irineu da Costa. Rio de Janeiro: Editora 34, 2003, p. 92.
- MIRABETE, Julio Fabbrini. **Manual do Direito Penal**, volume 1: parte geral - 24 ed São Paulo: Atlas, 2008.
- MONTEIRO, Silvana Drumond. O ciberespaço: termo, a definição e o conceito. **Revista da Ciência da Informação**, v 8 n 3 jun/2017.



PECK, Patricia. **Direito Digital**. São Paulo: Saraiva, 2002.

ROLIM, Marcos. **A síndrome da Rainha Vermelha: Policiamento e Segurança Pública no Século XXI**. Rio de Janeiro: Jorge Zahar, 2006. p 44-61.

SAFERNET: Navegar com segurança é navegar com liberdades. Disponível em: <http://new.safernet.org.br/> Acesso: 10 de ago de 2017.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.