

CIBER CRIMES, DELITOS PRATICADOS POR INTERMÉDIO DE DISPOSITIVOS INFORMÁTICOS

Cristiane Bueno de Almeida e Silva¹
Michelle Marie de Souza²

RESUMO

Com a disseminação do uso da internet e o acréscimo nas tecnologias surgiu uma nova ocorrência na modalidade de crimes: os ciber crimes, ou seja, delitos praticados através de dispositivos informáticos. Sopesando o aparecimento desse novo crime advindo do uso da internet e a importância do Direito em acompanhar as mudanças ocorridas no cotidiano da sociedade, pois estas influenciam o universo jurídico, optou-se por abordar a temática. Os ciber crimes se apresentarão no seguinte contexto: um breve histórico, suas particularidades e as alterações ocorridas na legislação brasileira, os reflexos do delito para o Direito Penal, análise das provas e a necessidade de perícia especializada, algumas modalidades do delito existentes no âmbito de prática do referido crime.

Palavras-chave: Internet, ciber crimes, delito, direito penal.

INTRODUÇÃO

Há cerca de quarenta anos, a Internet não passava de um projeto, o termo “globalização”, não havia se popularizado e a transmissão de dados por fibra óptica não existia.

Informação era um item caro e inacessível, centralizado, poucos a detinham. O cotidiano no mundo jurídico se resumia a papéis, burocracia e prazos. Com as mudanças ocorridas desde então, ingressamos na era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigmas. Essa nova era trouxe transformações em vários segmentos da sociedade, não apenas mudanças tecnológicas, mas também de conceitos, métodos de trabalho e estruturas.

A dinâmica da era da informação nos exige uma mudança profunda e o Direito precisa entender essa prática cotidiana, sendo influenciado por essa realidade nova.

Vivemos um momento único seja no aspecto tecnológico, econômico e social. O profissional de qualquer área, em especial a do Direito precisa estar em harmonia

¹ Acadêmica do Curso de Direito do Centro Universitário de Várzea Grande (Univag). Email: cristiane22bueno@gmail.com.

² Professora do Centro Universitário de Várzea Grande (Univag). Especialista em Direito Agroambiental. Pós Graduada em Perícia Criminal. Advogada. Email: <michellemarie_adv@hotmail.com>.

com essas transformações que ocorrem diariamente.

A internet é mais que um simples meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de Indivíduos. Indivíduos com letra maiúscula, porque estão inseridos em um conceito mais amplo, que abrange uma individualização não só de pessoas físicas, como também de empresas, instituições e governos (PINHEIRO, 2010, p.44).

Diante de tal conjuntura que entendemos oportuna esta reflexão sobre os ciber crimes, delitos praticados por intermédio de dispositivos informáticos. Uma prática recente, que vem trazendo prejuízos incalculáveis a toda a sociedade de um modo geral.

Mister a compreensão dos aspectos relacionados a esse novo delito no Direito Penal, na legislação brasileira, enfim no universo jurídico.

1 BREVE HISTÓRICO, DEFINIÇÃO E CLASSIFICAÇÃO DOS CIBERCRIMES

A sociedade moderna, tem se deparado com uma nova espécie de crime originário da evolução tecnológica, os ciber crimes, ou seja, delitos que vão de atividade criminosas contra dados até infrações de conteúdo e de direitos autorais.

A rede de comunicações que a princípio foi criada para atender um pedido da Força Aérea Americana passou a interligar universidades, órgãos militares e governo. Esse crescimento resultou na internet atual que é um dos principais meios de comunicação da sociedade contemporânea, interligando computadores do mundo todo.

Nos últimos anos é crescente o número de pessoas conectadas à internet. O desenvolvimento tecnológico fez com que a sociedade se tornasse dependente da eficiência e segurança da tecnologia da informação. Isto é, os sistemas informatizados atualmente são tão importantes na sociedade que a maioria das pessoas, seja física ou jurídica, depende de um dispositivo informatizado, seja para uso na esfera comercial, como a execução de ações financeiras pelo computador, seja na esfera empresarial, como a utilização dos bancos de dados para o armazenamento de seus arquivos mais valiosos (DIAS, 2014, p.11).

Várias pesquisas já foram realizadas com o objetivo de demonstrar o crescente uso da internet no Brasil (DIAS, 2014, p.11). Uma pesquisa do Ibope

Media revelou que o Brasil é atualmente um dos principais países no acesso a internet, o quinto país mais conectado à rede. De acordo com o FECOMÉRCIO-RJ/Ipsos, houve um aumento de 27% para 48%, entre 2007 e 2011, de brasileiros conectados à internet. A pesquisa (DIAS, 2014, p.11) especifica também os principais locais de acesso à rede quais sejam a *lan house* (31%), residência (27%) e a casa de parentes e amigos (25%).

Apesar dos benefícios trazidos com o advento da internet (DIAS, 2014, p.11) e o seu crescente desenvolvimento, a evolução tecnológica permitiu também o surgimento de condutas ilícitas praticadas na rede mundial de computadores. A facilidade de acesso à internet permitiu não somente a interconexão entre pessoas do mundo todo, mas também o surgimento de aspectos negativos, novos riscos representados por práticas ilícitas.

Pelos ensinamentos de Sandro D'Amaro (NOGUEIRA, 2009) *apud* (DIAS, 2014, p.11), o rol dos crimes cometidos por meio eletrônico é extenso. Dentre eles estão: os crimes contra a honra - tais como a injúria, calúnia e difamação - os furtos, estelionatos, fraudes com cartão de crédito, desvio de dinheiro de contas bancárias, dentre outros. Várias são as formas utilizadas para a prática desses delitos tais como interceptação de comunicações, modificações de dados, difusão de pornografia infantil, terrorismo.

Decorrentes do avanço tecnológico da sociedade, os crimes virtuais (DIAS, 2014, p.12) são condutas ilícitas praticadas com o auxílio de um computador, seja contra outros computadores e sistemas informáticos ou informações nele contidas, seja como mero instrumento para a prática de um delito. A definição mais comum para os crimes virtuais é:

(...) aquele no qual um ou mais computador (es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais conduta(s) criminalizada(s), ou são alvo(s) desta(s). O homem interagindo com uma máquina – retroalimentando-a com informações por meio de mensagens – através de uma rede de computadores (cibernética) interligados (ciberespaço), agindo conforme uma conduta previamente criminalizada (Crime informático) estereotiparia um modelo de cibercrime. (COLLI, 2010 p.44)

O surgimento de novas condutas ilícitas praticadas através da internet envolvendo a utilização de computadores é cada vez mais intensa e variada, acompanhando o desenvolvimento das novas realidades tecnológicas e sociais. No

entanto, apesar do reconhecimento da existência de tais condutas, não há um consenso quanto à denominação dos crimes de computador. Os chamados crimes virtuais recebem várias denominações em diversos países do mundo; são também chamados de “crimes de informática” ou “*cyber crimes*”, “delitos computacionais”, “crimes eletrônicos”, “crimes telemáticos”, etc, (DIAS, 2014, p.12).

Assim como não há um consenso quanto à denominação dos crimes praticados na rede mundial de computadores, também não há um consenso quanto à classificação dos crimes virtuais (DIAS, 2014, p.12). Os chamados crimes de computador surgiram nas últimas décadas do século XX, em meados dos anos 70, acompanhando o aumento na utilização dos computadores, sendo assim consideradas as condutas efetivadas através da utilização de um computador conectado ou não a uma rede (DIAS, 2014, p.12).

2 A PENA E A COMPETÊNCIA PARA JULGAMENTO DA AÇÃO PENAL

Na ocorrência de *ciber crimes* a pena cominada no preceito secundário do caput do art. 154-A do CP é de detenção de 3 (três) meses a 1 (um) ano, e multa. Para a modalidade qualificada de invasão de dispositivo informático, prevista no § 3.º do art.154-A do diploma repressivo, a pena é de reclusão, de 6 (seis) meses, a 2 (dois) anos (GRECO, 2015, p.614).

Nos termos do § 2º do artigo em análise, aumenta-se a pena de um sexto a um terço se a invasão resulta prejuízo econômico.

De acordo com o § 4º, na hipótese do § 3º, ambos do art.154-A do CP, aumenta-se a pena de um a dois terços se houver a divulgação, comercialização, ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos (GRECO, 2015, p.614).

O § 5º do mesmo artigo (GRECO, 2015, p.615) determina que a pena seja aumentada de um terço à metade se o crime for praticado contra:

- I - Presidente da República, governadores e prefeitos;
- II - Presidente do Supremo Tribunal Federal;
- III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembléia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
- IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Será possível a proposta de suspensão condicional do processo, nos termos do art. 89 da Lei 9.099/95 (GRECO, 2015, p.615).

A competência para o julgamento do crime de invasão de dispositivo informático será, inicialmente, do Juizado Especial Criminal, tendo em vista que a pena máxima cominada em abstrato não ultrapassa os dois anos, mesmo na sua modalidade qualificada, desde que, na hipótese concreta, a aplicação de uma e/ou mais causas especiais de aumento da pena não façam com que esse limite seja ultrapassado (GRECO,2015, p.615).

A ação penal conforme determinação contida no art. 154-B, incluído também pela Lei n.º 12.737 de 30 de novembro de 2012, será de iniciativa pública condicionada à representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estado, Distrito Federal ou Municípios, ou contra empresas concessionárias de serviços públicos (GRECO,2015, p.615).

Ação penal pública condicionada é aquela que depende de representação do ofendido ou da requisição por parte da justiça como condição para a sua instauração.

Importante mencionar que a condicional nesse tipo de ação é o seu desenvolvimento e não a ação. Sendo seu titular o Ministério Público, mas este depende de manifestação da vontade da vítima.

3 DIAGNÓSTICO DA PROVA NOS CIBER CRIMES

Não há nenhuma legislação brasileira que proíba ou vete a utilização de prova eletrônica. Ao contrário, o Código de Civil e o Código de Processo Civil aceitam completamente o seu uso, desde que sejam atendidos os padrões técnicos de coleta e guarda, para evitar que esta tenha sua integridade questionada ou que tenha sido obtida por meio ilícito (PINHEIRO, 2010, p.208-209).

A natureza jurídica da prova é a forma pela qual se apura a verdade em juízo. Trata-se de um meio usado pelas partes para atingir um resultado.

Com o desenvolvimento da tecnologia e o surgimento da 'sociedade da informação', como atualmente somos caracterizados, devido à dependência cada vez mais da eficiência e segurança da tecnologia da informação e de seus recursos tecnológicos (DIAS, 2010, p.22). Tal evolução trouxe alguns benefícios a sociedade, porém demonstrou o lado oposto também, malefícios, como a prática de crimes até então desconhecidos em suas formas e em sua complexidade.

A prova pode ser conceituada como um conjunto de ações praticadas pelas partes destinadas a comprovar ao juiz a ocorrência ou inoccorrência do fato, a veracidade ou não de uma informação. Isto é, “a prova é todo e qualquer meio de percepção empregado pelo homem com o objetivo de comprovar a veracidade de uma alegação” (CAPEZ, 2011, p.344).

Os *ciber* crimes com características diversas com que se apresentam, suscitam uma maior dificuldade para sua comprovação e investigação, muito mais sua comprovação, sendo necessária perícias especializadas e técnicas para se possível identificar ou ao menos rastrear a sua autoria.

4 AS PERÍCIAS ESPECIALIZADAS

Diante da atual necessidade de uso da rede mundial de computadores em todas as tarefas que vamos realizar ao longo dos dias, surge uma nova modalidade de delito, realizada através de dispositivos informáticos. Necessário foi atualizar as formas de apuração dos crimes praticados nesse meio, surgindo então às perícias especializadas.

Coleta se as informações dos dispositivos informáticos para apuração das práticas delituais que serão submetidas a perícias técnicas para então se tornarem meios de prova em um processo. Nasce então a computação forense, que serve para analisar as evidências e os pormenores dos atos ilícitos praticados através dos dispositivos informáticos.

Tais crimes são de grande complexidade e as provas levantadas podem desaparecer com muita facilidade nesse meio. Exige se técnica e conhecimento para evitar o surgimento de uma prova viciada, o que contaminaria todo processo.

Ainda falta muito capital humano para lidar com esse tipo de realidade, policiais preparados para investigar e examinar a existência de tais delitos. Outro ponto é o aparato tecnológico, que precisa ser uma realidade constante de aperfeiçoamento para que as provas produzidas tenha laudos periciais livres de quaisquer vícios.

O Brasil ainda se encontra em um nível de preparação para o combate as práticas de crimes virtuais, seja porque existem poucas delegacias especializadas e um número não suficiente de profissionais habilitados a apurar as ocorrências desses crimes, muito ainda precisa ser feito.

Talvez aí esteja um nicho de mercado a ser explorado pelos profissionais do direito que desejam obter uma carreira de sucesso.

5 ESTELIONATO ELETRÔNICO

A grande utilização do sistema informático fez nascer um novo meio de afetação a bens jurídicos. Da mesma forma que a tecnologia se desenvolve e propicia meios para melhorar a vida em sociedade, constata-se o seu emprego para o aperfeiçoamento de condutas que trazem desconforto social (CHAGAS, 2012).

Modernamente, ao se tratar de ilícitos, pode-se verificar a existência de várias possibilidades de ação criminosa na área da informática, assim entendida no seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados.

O desrespeito ao sigilo ocorre das mais diversas formas pelos *hackers* e *crackers*, que, valendo-se de expedientes fraudulentos, conseguem romper as barreiras protecionistas ofertadas pelos sites e usurpar, apropriar, destruir, obter vantagem ilícita mediante erro e subtrair informações ali encartadas, o que gera a insegurança aos usuários da rede mundial de computadores (CHAGAS, 2012).

Para se ter noção do tamanho crescimento destas atitudes, no Brasil o crime de estelionato eletrônico, juntamente com o de pedofilia, são apontados como os mais comuns na rede (CHAGAS, 2012).

O estelionato eletrônico transcorre de forma ágil e a vítima só terá conhecimento de que foi enganada muito tempo depois, o que assegura ao criminoso realizar outra fraude, com outros usuários.

Em todas essas modalidades, o objetivo é sempre obter vantagem ilícita, por meio fraudulento, induzindo a vítima ao erro. Na preponderância das vezes os criminosos criam páginas falsas, como por exemplo, a página do banco da vítima, induzindo-a em erro, fazendo a vítima realizar transações bancárias nesta página falsa.

Contudo deve haver cautela de onde acessar a rede de internet em que aparelho acessar, pois pode se ter algum vírus ali introduzido e este usurpar todos os seus dados pessoais armazenados ou digitados.

Desta forma, pode-se ver que os crimes supramencionados apenas se utilizam de um meio eletrônico, ou seja, apenas o modo da materialização da

conduta criminosa que é virtual, não o crime, que também pode ocorrer no mundo físico. Nestes casos, não está ocorrendo uma analogia *in malam partem*, pois não há a criação de um novo delito. O delito é o mesmo (estelionato), o que muda é o meio de sua realização e consumação. São as infrações favorecidas pela informática ou, como denominam outros autores, crimes informáticos impróprios (CHAGAS, 2012).

Estes procedimentos podem ser feito por pessoas comuns, sem exigência de alto conhecimento informático (CHAGAS, 2012).

6 DIVULGAÇÃO DE MATERIAL OFENSIVO

Infelizmente outra modalidade de ciber crime crescente e também quase tão antiga como a rede mundial de computadores é a pornografia seja ela do tipo doméstica ou comercial.

A popularidade do acesso à rede mundial de computadores pelas diversas opções existentes (celulares, computadores domésticos, tablets, etc.), juntamente a experiência de uso das redes sociais, tornou o compartilhamento de material pornográfico muito mais veloz que antes da existência destes dispositivos.

A prática de compartilhar esse tipo de material é considerado crime de injúria e difamação segundo o Código Penal Brasileiro em seus respectivos artigos 139 e 140 CP. Se existir um menor nesse material compartilhado em situação de sexo ou pornografia o crime se torna mais grave, como previsto no ECA em seu artigo 241.

Ultimamente tem se praticado com muita frequência outro crime oriundo do meio virtual, o *cyberbullying*, uma espécie de divulgação de imagens e vídeos de nudez, sem consentimento da vítima, que tem provocado casos de suicídios das pessoas expostas a essa situação de vexame.

Além das redes sociais é preciso ter cuidado com os famosos aplicativos de troca de mensagens, também conhecidos como (WhatsApp e ou Telegram, etc.) que facilitam o compartilhamento de materiais eróticos por seus usuários, o que pode ensejar uma responsabilização criminal, uma vez havendo investigações por peritos da polícia, que podem facilmente recuperar dados mesmo quando apagados.

7 DIFAMAÇÃO VIRTUAL

O mundo virtual não pode se diferenciar do mundo real, sendo assim os crimes contra a honra tipificados no Código Penal Brasileiro, também são válidos e

puníveis se praticados via a Internet.

É surpreendente ouvir, a todo o momento, que os crimes praticados no mundo virtual necessitam de uma lei para regular as práticas ilegais. No entanto, não é exatamente assim. O simples envio de um e-mail para sua lista difamando uma determinada pessoa, o que é hoje um fato comum, pode ser enquadrado nas leis atuais com punições já regulamentadas (SOUZA, 2009, p.01)

A calúnia ocorre bem próxima, ou em conjunto com, a difamação, pois a calúnia desacredita alguém publicamente ao atingir sua honra com fatos que não correspondem com a verdade (SOUZA, 2009, p.03).

A difamação se distingue da injúria, pois a primeira é a imputação a alguém de fato determinado, ofensivo à sua reputação – honra objetiva –, e se consuma quando um terceiro toma conhecimento do fato; diferentemente da segunda, em que não se imputa fato, mas qualidade negativa, que ofende a dignidade ou o decoro de alguém – honra subjetiva -, além de se consumir com o simples conhecimento da vítima (SOUZA, 2009, p.03)

Os delitos informáticos podem ser punidos atualmente, não podendo mais os criminosos acreditar que estão em uma terra sem lei e sem punições. Estamos constantemente vigiados através da rede mundial de computadores e o que se digita e publica pode ser punível.

CONSIDERAÇÕES FINAIS

Diante do estudo dos conceitos e características dos ciber crimes, suas particularidades, bem como sua nuance junto ao Direito Penal Brasileiro e a legislação recentemente modificada, a monografia cumpriu com o seu objetivo, qual seja o de entender o contexto jurídico dos delitos praticados por intermédio de dispositivos informáticos no ordenamento jurídico brasileiro.

Depois de exposta a temática se faz necessário a realização de algumas ponderações.

Por anos o Brasil, desde o surgimento da internet, não detinha de mecanismos de proteção para as relações ocorridas entre os indivíduos através desse meio.

No ano de 2012 houve a criação de leis específicas sobre o tema com o intuito de combater a prática destes delitos, mas que não se mostraram capazes

ainda, pois a cada dia surgem novas maneiras de violar os direitos individuais através da Rede mundial de computadores (internet).

O avanço na tecnologia contribuiu significativamente para a melhoria do cotidiano da sociedade, possibilitou avanços, mas também gerou retrocessos, no quesito criminalidade.

A lei 12.737/2012 possibilitou avanços ao tipificar as práticas mais recorrentes no cenário dos crimes cometidos em meios informáticos, sanando alguns problemas, punindo e os controlando em partes. Importante dizer que não serão apenas Leis que combateram a prática de delitos em ambiente virtual.

Necessário a conscientização dos usuários dessas novas tecnologias disponíveis, para prevenir, compreender e se resguardar dos perigos que esta novidade consigo carrega.

O Direito precisa acompanhar essas mudanças sempre se atentando a atualizar os mecanismos de coibição existente.

Porém o mais importante a fazer é traçar planos de investigações e prevenção com material humano capacitado e especializado, em todas as esferas de Poder existente. O que poderá de sobremaneira diminuir esse lado sombrio da Rede.

REFERÊNCIAS

BRASÍLIA (Estado). **Lei n.º 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decretol-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências.

CAPEZ, Fernando. **Curso de Processo Penal.** São Paulo: Saraiva, 2011.

CHAGAS, Fernando Vinicius de Souza. **Estelionato eletrônico: necessidade de tipificação?** Disponível em: <http://www.meuadvogado.com.br/entenda/estelionato-eletronico-necessidade-de-tipificacao.html>.

COLLI, Maciel. Cibercrimes. **Limites e perspectivas à investigação policial de crimes cibernéticos.** Curitiba: Juruá Editora. 2010.

DIAS, Camila Barreto Andrade. **Crimes Virtuais: As inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal.** UNICEUB- Centro Universitário de Brasília. FAJS- Faculdade de Ciências Jurídicas e Sociais, Brasília, 2014.

DICIONÁRIO**INFORMAL.**

Disponível

em: <http://www.dicionarioinformal.com.br/significado/lan%20house/2845>.

GRECO, Rogério. **Curso de Direito Penal: parte especial**. Volume II. 12. ed. Rio de Janeiro: Impetus, 2015.

MAGGIO, Vicente de Paula Rodrigues. **Novo Crime: invasão de dispositivo informático:CP- art.154-A**.

PINHEIRO, Patricia Peck. **Direito Digital**. 4.ed.rev.,atual.e ampli. São Paulo: Saraiva, 2010.

PRASS, Ronaldo. **Entenda os riscos de compartilhar imagens íntimas na internet**. Disponível em: <http://g1.globo.com/tecnologia/blog/tira-duvidas-de-tecnologia/post/crimes-digitais-entenda-os-riscos-de-compartilhar-imagens-intimas-na-internet.html>.

SOUZA, Davi. **Difamação virtual**. Direito Forense. Disponível em: <http://www.direitolegal.org/direito-digital/difamacao-virtual/>.

LEGENDAS

Hackers: é uma palavra em inglês do âmbito da informática que indica uma pessoa que possui interesse e um bom conhecimento nessa área, sendo capaz de fazer hack (uma modificação) em algum sistema informático. Em inglês, a palavra hack é um verbo que significa cortar alguma coisa de forma irregular ou grosseira.

Crackers: Os crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. Em alguns casos, o termo “Pirata Virtual” é usado como sinônimo para cracker.

Cyberbullying é um tipo de violência praticada contra alguém através da internet ou de outras tecnologias relacionadas. Praticar **cyberbullying** significa usar o espaço virtual para intimidar e hostilizar uma pessoa (colega de escola, professores, ou mesmo desconhecidos), difamando, insultando ou atacando.