Cognitio Juris
ISSN 2236-3009

# CRIMES CIBERNÉTICOS NA RELAÇÃO DE CONSUMO

***CYBER CRIMES IN THE RELATIONSHIP OF CONSUMPTION***

**Cognitio Juris**
Ano XI – Número 35 – Junho de 2021
ISSN 2236-3009

Autores:
Márcio Magliano Barbosa[1]
Romulo Rhemo Palitot Braga[2]

RESUMO: Este artigo trata de identificar os crimes praticados contra os consumidores no ambiente virtual, em especial, os relativos a fraudes e falsificações além das práticas ilícitas mais comuns ocorridas na internet por hackers e demais fraudadores no intuito de lesar os consumidores que se utilizam do comércio eletrônico para adquirir produtos ou serviços e com isso vindo a gerar sérios problemas no mercado de consumo em geral. Tais crimes podem ocorrer nas modalidades próprias quando tipificado em lei especifica e imprópria quando previsto em leis especiais e no próprio código penal visto que outros tipos penais passaram a ser evidenciados no ambiente virtual e que também causam danos aos consumidores. A pesquisa do tema avança através de uma metodologia dialética e qualitativa pois busca identificar quais as práticas ilícitas identificadas até o momento, e quais são os crimes cibernéticos, tipificados ou não, que podem resultar danos aos direitos dos consumidores quando da realização de suas transações comerciais junto a internet.

Palavras Chaves: Crimes Cibernéticos. Fraudes e Falsificações. Consumidor. Comércio Eletrônico. Práticas Cibernéticas Ilegais.

ABSTRACT: This article tries to identify the crimes practiced against consumers in the virtual environment, in particular, those related to fraud and counterfeiting, in addition to the most common illegal practices occurred on the internet by hackers and other fraudsters in order to harm consumers who use e-commerce. to purchase products or services and thereby causing serious problems in the consumer market in general. Such crimes can occur in the proper modalities when typified in a specific law and improper when provided for in special laws and in the penal code itself, since other criminal types have become evident in the virtual environment and which also cause harm to consumers. The research of the theme advances through a dialectical and qualitative methodology as it seeks to identify which illicit practices have been identified so far, and which are cyber crimes, typified or not, that may result in damage to the rights of consumers when carrying out their commercial transactions. with the internet.

Keywords: Cyber Crimes. Fraud and Counterfeiting. Consumer. E-Commerce. Illegal Cyber Practices.

## I – INTRODUÇÃO

Os crimes cibernéticos foram regulamentados na Lei nº 12.737/2012, também conhecida como “Lei Carolina Dieckmann” devido ao nome da atriz global que, no ano de 2012, foi alvo de hackers que invadindo os seus dispositivos eletrônicos tiveram acesso a mensagens e fotos – muitas de conteúdo íntimo – trocadas com o seu marido e que acabaram sendo espalhadas e compartilhadas na internet demonstrando a fragilidade do mundo virtual quanto à ocorrência de práticas nocivas e até criminosas.

E devido a esse episódio que ganhou notoriedade internacional, acabou por se acelerar a tramitação existente em outros projetos de leis junto às comissões do Congresso Nacional, especialmente ao Projeto de Lei n 84/1990 que tratava sobre a criminalização das praticas cibernéticas que resultavam na invasão de dispositivos eletrônicos para sequestrar, roubar

ou manipular dados dos seus usuários através da internet além de outras questões sensíveis de segurança nacional a qual ganhou a alcunha de AI-5 Digital.

Sendo assim, no mesmo ano foi publicada a lei n. 12.737/2012 que veio a acrescentar dois novos tipos penais (arts. 154-A e 154-B) e a alteração na redação de outros dois já existentes (art. 266 e art. 298, parágrafo único) no Código Penal.

Pouco tempo depois, também foi publicada a lei n. 12.735/2012, que criou as Delegacias Virtuais, divisão dos órgãos de segurança publica para investigação destes crimes e das praticas virtuais que geram a sua ocorrência.

Pois bem, passados oito anos de vigência das referidas leis, é visível que as pessoas estão cada vez mais dependentes dos dispositivos tecnológicos e das mídias sociais tanto para o entretenimento, como para realização para obtenção de produtos e serviços que atendam as suas necessidades e, justamente nesse ponto, passam a ser alvos de pessoas mal intencionadas e que possuem conhecimento do mundo virtual obtêm, de forma ilícita, dados dos consumidores para realizar os mais diversos crimes de fraude e falsificação que são os mais usuais no mercado de consumo.

No mais, tais crimes estão se tornando cada vez mais difícil de serem identificados e suas formas de repreensão, principalmente, quem são seus infratores em razão dos avanços e desenvolvimentos das praticas cibernéticas utilizadas ao longo dos anos, a ponto de serem tão bem elaboradas que não são detectáveis em um primeiro momento pondo em risco as transações comerciais, demonstrando que nem os consumidores e nem os fornecedores estão seguros no meio virtual.

II – DEFINIÇÃO

Está cada vez mais corriqueiro da internet e dos meios de comunicação a ponto de nossa sociedade atual os considerar como serviços essenciais, já que muitas transações comerciais

e sociais atualmente se desenvolvem e operacionalizam no meio virtual devido a sua praticidade, facilidade e rapidez no cumprimento do objetivo a qual ela se propõe. A ponto de não conseguimos distinguir nossa vida sem ela, afinal, a internet é a mais importante invenção humana do século XX.

Entretanto, com a utilização maciça e cada vez mais usual dos meios eletrônicos, as pessoas – usuários – não estão imunes à ocorrência de práticas infrativas ou até delitos penais que passaram a ocorrer e até mesmo, se desenvolver e inovar no ambiente virtual.

Logo, diante dessa afirmação surge a seguinte indagação: Como os crimes cibernéticos ocorrem e como eles afetam a relação de consumo?

Conforme dito acima, os crimes cibernéticos se operam no ambiente virtual e devido facilidades e comodidades propiciadas ao consumidor no mundo virtual a ponto de adquirirmos bens e serviços, dos essenciais aos supérfluos, sem a necessidade de ausentarmos de nossos lares, pois, com a pena um clique temos o acesso às ofertas e a aquisição destes produtos ou serviços.

Logo, o mercado de consumo – consumidores e fornecedores em geral – não estão imunes de serem vítimas de crimes ocorridos neste ambiente definidos tanto no código penal como em outros ordenamentos jurídicos já conhecidos do mercado de consumo e que antes ocorriam no mundo físico, mas que também passaram a ser vistos e operacionalizados no ambiente virtual.

Nesse diapasão, FABRICIO ROSA[3] (2017) afirma que diante do avanço tecnológico propiciado pela internet e pelos meios de comunicação os crimes de falsificação e fraudes que anteriormente ocorriam no mundo físico também passaram a ocorrer no ambiente virtual além do surgimento de novos tipos penais.

Portanto, não podemos ficar só atrelados ao conceito de crimes cibernéticos existentes só

com o advento de lei própria, mas, de outros crimes já existentes que passaram a existir no ambiente criminal.

III – CONSUMIDOR VIRTUAL

Inicialmente, antes de aprofundarmos no tema, é preciso revisitar institutos essenciais que dão suporte ao consumo ocorrido no ambiente virtual, especialmente, o que seja o comercio virtual (e-commerce) e a de consumidor no ambiente virtual.

Inicialmente trataremos do conceito de consumidor no ambiente virtual, demonstrando a sua evolução e consequente conceituação doutrinária.

Devido aos avanços tecnológicos, o comércio de consumo não mais se resume a consumidor-loja, mas se diversifica nas mais variadas transações, da mais simples a mais complexa, criando um novo tipo de consumidor que, muito embora utilize o mesmo fundamento já identificado no Código de Defesa do Consumidor (art. 2º) teve o seu conceito ampliado em razão dessa nova vertente conceitual do consumidor e com vozes na doutrina que já identificam o consumidor virtual.

E qual seria a definição de consumidor virtual?

O consumidor virtual é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço, no ambiente virtual, como destinatário final.

Portanto, partindo deste raciocínio e definição, será considerado consumidor virtual:

toda e qualquer pessoa física ou jurídica que adquire produtos ou serviços;

através do ambiente virtual (E-commerce);

como destinatário final (não têm a intenção de revenda);

É preciso salientar que tal conceituação se deve as evoluções do conceito do consumidor em razão da sua interação com a tecnologia e dos contínuos avanços tecnológicos que fizeram com que tal conceito sofresse uma mutação.

TEXEIRA[4] e RODRIGUES[5] (2019) em um brilhante artigo sobre o tema apresentam uma classificação evolutiva e deveras interessante quanto ao conceito de consumidor interligado com os avanços tecnológicos:

CONSUMIDOR 1.0 – O consumidor que utilizada à internet apenas como ferramentas de busca, tem acesso reduzido, e o fornecedor detém o poder do consumo;

CONSUMIDOR 2.0 – O consumidor passou a ter acesso a informação dos produtos e serviços oferecidos, escolhendo o fornecedor ampliando o seu poder de compra; foi neste momento que surgiu os Serviços de Atendimento ao Consumidor (SAC);

CONSUMIDOR 3.0 – O consumidor passou a ter maior acesso as informações compartilhando suas opiniões sobre produtos e serviços adquiridos com outros consumidores; os fornecedores passaram a correr atrás dos consumidores; surgimento da propaganda virtual e das lojas virtuais;

CONSUMIDOR 4.0 – O consumidor passou a ser mais rigoroso e seletivo em suas escolhas, tendo um maior poder de opinião e influência no consumo; compartilha informações com outros usuários na internet e nas redes sociais; surgimento dos sites de compras coletivas, desenvolvimento das práticas de marketing, valorização da exclusividade; atual fase.

CONSUMIDOR 5.0 – Fase futura a qual se encaminha o consumidor em razão do desenvolvimento da tecnologia e de sua interação com a criação da realidade aumentada (AR), inteligência Artificial (IA) e da Internet das Coisas (IOT) propiciando ao consumidor uma maior imersão de sentidos no ambiente virtual.

Sendo assim, podemos perceber que o conceito de consumidor virtual é fruto não só de

mutação e interpretação extensiva do conceito legal de consumidor, mas também da evolução da tecnologia e do aumento de sua acessibilidade aos consumidores de todas as classes e de todos os níveis.

Isto é, a tecnologia gerou a popularização dos meios eletrônicos e do desenvolvimento dos meios de comunicação a ponto de, conforme dito anteriormente, não conseguimos mais distinguir nossas vidas e nossas relações sem as benesses do mundo virtual.

Ao contrário, com o evoluir da tecnologia, cada vez mais intensa é a imersão humana que o mundo virtual já se prepara para nos propiciar maiores sensações sensoriais e até mesmo, a realidade virtual como demais tecnologias que eram temas de livros e filmes de ficção cientifica já são realidade.

Em suma, caminhamos a passos largos para perda de distinção entre o mundo real do mundo virtual.

IV – COMÉRCIO ELETRÔNICO (E-Commerce)

Em tempo, passada a definição do que seria consumidor virtual nos cabe, agora, definirmos o que seria o comercio eletrônico (e-commerce) e como o mesmo se originou.

Quanto a sua origem, o e-commerce se originou da necessidade dos fornecedores poderem ter acesso cada vez maior aos consumidores, de expandir as suas práticas comerciais a ponto de que fronteiras territoriais físicas que muitas vezes os separavam dos consumidores não mais existirem.

E com isso, acabou propiciar também a evolução das transações comerciais que se tornaram mais ágeis, céleres e menos burocráticas e de fácil fiscalização ampliando a concorrência fazendo com que os mercados buscassem se inovar para se tornarem cada vez mais competitivos.

Isto é os meios eletrônicos, em especial a internet, se tornaram os catalizadores da Quarta Revolução Social.

Sendo assim, feito as considerações acima, qual seria, então, a definição deste novo modelo de transações comerciais conhecido como e-commerce?

VALLE[6] (2009) ao publicar um artigo que foi publicado na revista eletrônica Empreendedores, apresenta uma definição do que seria e-commerce:

“O E-commerce é toda e qualquer transação que tenha origem em equipamentos eletrônicos, ou seja, transações que possuem inicio no ambiente on line, o que envolve desktops, dispositivos mobiles e mais recentemente os wherables, como relógios conectados à internet.”

Em suma, todas as práticas comerciais que gerem a comercialização, aquisição, oferta e contratação que não se enquadre como relação de trabalho e que se desenvolva por meio de instrumentos eletrônicos com acesso a internet será conhecido como e-commerce e com isso dinamizando as relações comerciais.

Tais relações comerciais além de serem evidenciadas nas relações privadas também passaram a ser realizadas também, mas em menor ênfase, nas relações publicas principalmente da prestação de serviços públicos que, em regra, são serviços especiais até mesmo na contratação desses serviços.

Assim como, de forma inversa, quando o setor público também busca no meio privado a contratação de serviços ou produtos inerentes as suas atividades.

V – AS PRÁTICAS VIRTUAIS ILICITAS

Uma vez esclarecidos os conceitos e definições de E-commerce e do consumidor no mundo virtual é salutar concluir que diante dos benefícios propiciados pelo desenvolvimento dos

meios tecnológicos tais como: facilidade, comodidade e um grande e vasto meio de escolhas de produtos e serviços, inversamente, como a outra face de uma moeda, a mesma também trouxe as suas mazelas.

Isto é, as intenções dolosas que antes eram ocorrentes no meio físico passaram a ser identificadas no meio virtual através de agentes mal intencionados (Hackers) que se utilizam de seus conhecimentos sobre a computação e programação para criar práticas que tem como único objetivo de lesar os consumidores despreparados que objetivam adquirir produtos e serviços pela internet.

Tais meios, por sua vez, sãos as práticas virtuais criminosas que tem como único objetivo gerar comportamentos contrários vindos a resultar na ocorrência de ilícitos, em especial, os relativos à fraude, furto/roubo e falsificações. As mais comuns e corriqueiras nos meios virtuais praticadas contra a ordem de consumo.

Logo, podemos concluir que as práticas virtuais ilícitas, embora não sejam ilícitos penais propriamente ditos, são meios de execução necessários para a consumação dos crimes cibernéticos.

Entretanto, tais práticas muitas vezes acabam sendo complexas e de difícil identificação em razão do dinamismo corrente dos meios virtuais e principalmente das alterações, modificações e invocações (atualizações) que são realizadas para impedir a sua identificação.

Para tanto, relatamos algumas das práticas mais comuns identificadas no meio virtual:

VÍRUS – A primeira e talvez uma das mais corriqueiras, trata-se de um programa malicioso obtido inadvertidamente pelos usuários – portanto, consumidores – quando da navegação pela internet. Sendo instalado no dispositivo eletrônico passa a infectar na intenção de obter dados.

SPAM – Trata-se de um aperfeiçoamento do vírus. Isto é, trata-se de um programa que é

enviado através de um link enviado ao e-mail do usuário como uma mensagem indesejada ou apelativa que, uma vez clicada, se instala automaticamente no dispositivo eletrônico para roubar dados.

WORM – Também semelhante a um vírus, mas com uma diferença, uma vez instalado ele passa a se replicar, isto é, não precisa de um programa hospedeiro pois é autossuficiente e ataca mesmo quando o dispositivo está desativado e não sendo perceptível a um primeiro momento e com isso vindo a causar enormes danos, e.g.: roubar dados, deletar arquivos e etc.

STORM WORM/BONET – trata-se de uma inovação do Worm e de difícil rastreamento, sendo transmitido pela internet através de links indesejados e que é ativado por um determinado número de IP.

PISHING – Trata-se da fraude eletrônica propriamente dita, pois tem como rotina cópia e reproduzir a página de um site confiável (e.g. bancos), em que o mesmo espelhas as informações apresentadas pelo usuário e com isso obtém tais informações. É muito comum em fraudes bancárias ocorridas no meio virtual.

SPYWARE – também conhecido como programa espião, trata-se de um programa em que o mesmo ao invés de espelhar os dados obtidos como pishing, ele os recolhe e armazena para serem usados pelo hacker em um momento posterior, em especial, para venda destes no futuro.

ROOTKIT – trata-se de uma ferramenta que pode vim ou não acompanhada junto a um spyware que além de permitir o acesso remoto ao dispositivo eletrônico e com isso obter os dados do usuário, ele permite a sua alteração. Além de dificultar a localização de quem utiliza esse meio.

RASONWARE: o mais nova prática virtual e a mais maléfica até agora identificada, trata-se de

um malware que alia as características do spyware e do rootkit que permite o acesso alteração dos dados impossibilitando o acesso e com isso os sequestrando, o hacker passa a pedir um resgate do dados, com pagamento de um determinado valor que vai aumentando cada vez mais. É uma das ferramentas mais procuradas e comercializadas na Deep Web.

Passados a descrições das principais práticas virtuais, analisaremos cada um dos crimes virtuais que podem ser cometidos contra os consumidores.

VI – CRIMES CIBERNÉTICOS CONTRA O CONSUMIDOR

Uma vez entendidos as práticas virtuais ilícitas e que as mesmas são meios de execução para os crimes cibernéticos, iremos analisar cada um deles e de como os mesmos são capazes de gerar tantos danos aos consumidores.

Logo, mais uma vez VIANA[7] (2007) assim conceitua os crimes cibernéticos: "(…) crimes virtuais são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização do sistema de informática."

No mesmo sentido, afirma VIDAL[8] (2013): "os crimes virtuais podem ser definidos como às condutas de acesso não autorizado a sistemas informáticos, interceptação de comunicações, alteração de dados, discriminação entre outros."

Conforme mencionado antes não só serão os crimes cibernéticos os definidos na lei especial relativa ao tema mas também, aqueles previstos em outros ordenamentos jurídicos tais como o Código Penal e o Código de Defesa do Consumidor e sua legislação extravagante, visto que com a introdução das práticas virtuais os mesmos acabaram por ganhar uma nova roupagem.

Sendo assim, visando um melhor entendimento, iremos definir os crimes cibernéticos contra o consumidor em 2 modalidades: próprios e impróprios.

VII – CRIMES CIBERNÉTICOS CONTRA O CONSUMIDOR “PRÓPRIOS”

São os crimes previstos no ordenamento específico, no caso, a lei dos crimes cibernéticos que veio a acrescentar novos tipos penais ao código penal e invariavelmente também afeta aos consumidores quando estes realizam as suas transações econômicas ou comerciais através do meio virtual, sendo vitimas de, furto, adulteração, destruição, violação e indisponibilidade dos seus dados digitais

Sendo assim, eis os tipos penais:

Invasão de Dispositivo Informático

Art.154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º. Na mesma pena incorre quem produz, oferece, distribui, vende e difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º.Aumenta-se a pena de um sexto a um terço se da invasão resultar prejuízo econômico.

§ 3º. Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais, industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constituir crime mais grave.

§ 4º. Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação,

comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações;

Logo se percebe que o tipo penal acima é bastante amplo, posto que visa punir aquele que se utiliza dos meios eletrônicos/virtuais quem além de invadir, obter, adulterar ou destruir os dados dos usuários sem sua autorização (art.154-A, caput).

Bem como vemos que a pena será aumentada quando da violação houver a produção, distribuição, difusão ou venda (art.154-A, § 1º).

E também, duas causas agravantes quando resultar em prejuízo econômico ou violação da privacidade das informações, dever de sigilo ou expor segredos de natureza comercial ou industrial (art.154-A, §§ 2º, 3º e 4º)  ou quando houver repercussão social (divulgação a terceiros).

Ademais, podemos concluir que do tipo penal descrito, de sua simples leitura aliada das práticas virtuais também anteriormente descritas, vimos que o legislador teve a preocupação de mantê-lo de forma atualizada e ampla a ponto de que com o surgimento de novas práticas comerciais infrativas no meio virtual essas também se enquadrem no respectivo tipo penal.

Falsificação de Cartão

Art. 298. (...)

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

O artigo in comento, foi acrescentado com o advento da lei do crime cibernéticos, criando uma nova hipótese de para o crime de falsificação de documento particular.

Isto é, a partir da referida lei o cartão de crédito, seja ele de débito ou crédito, passou a ser considerado como um documento particular e em caso de sua falsificação o mesmo ocorrerá

nas penas do referido artigo.

Tal crime subsiste no meio virtual em decorrência dos avanços tecnológicos, visto que as instituições financeiras, preocupadas em manter a segurança dos serviços prestados (concessão de crédito e facilitação de pagamentos), criou mecanismos para evitar a sua falsificação (e.g., chip de identificação e atualmente, o surgimento do cartão virtual).

Todavia, conforme falamos anteriormente, em razão do desenvolvimento dos meios fraudulentos no mundo virtual, tal crime acabou ganhando nova roupagem, posto que como se tornou fácil invadir qualquer dispositivo eletrônico, concomitantemente, passou-se a obter, com facilidade dados bancários e relativos ao cartão, possibilitando a sua falsificação e sua clonagem.

VIII – CRIMES CIBERNÉTICOS CONTRA O CONSUMIDOR “IMPRÓPRIOS”

Trata-se dos crimes previstos no Código Penal e em sua legislação extravagante que, com os avanços tecnológicos, ganharam nova roupagem passando a serem comuns à sua ocorrência também no âmbito virtual.

O primeiro deles será o furto de dados, quando o hacker, através dos meios virtuais, com abuso de confiança, fraude ou destreza (habilidade) subtrai para si ou para outrem coisa alheia móvel pertencente ao consumidor e assim ocorrendo o furto de dados (art.155, §4º, II/CP) caraterística qualificadora do crime de furto.

Furto

Art. 155. Subtrair, para si ou para outrem, coisa alheia móvel:

Pena – reclusão, de um a quatro anos;

FURTO QUALIFICADO

§ 4º. A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:

II – com abuso de confiança, ou mediante fraude, escalada ou destreza;

Tal tipo penal é muito comum quando há subtração de valores e sem consentimento da vitima, mediante transferência fraudulenta via internet.

Ademais, tal hipótese já foi inclusive confirmada pela 3ª Turma da 5ª Seção do Superior Tribunal de Justiça quando do julgamento do Conflito de Competência Negativo nº 145.576/MA, cuja ementa segue abaixo:

CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSUAL PENAL. FURTO MEDIANTE FRAUDE. TRANSFERÊNCIA BANCÁRIA VIA INTERNET SEM O CONSENTIMENTO DA VÍTIMA. CONSUMAÇÃO NO LOCAL DA AGÊNCIA ONDE O CORRENTISTA POSSUI A CONTA FRAUDADA. COMPETÊNCIA DO JUÍZO SUSCITADO.

1. A Terceira Seção desta Corte Superior firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4o, inciso II, do Código Penal – CP.

2. O delito em questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, nos termos do art. 70 do Código de Processo Penal – CPP; no caso, na Comarca de Barueri/SP.

3. Conflito de competência conhecido para declarar competente o Juízo de Direito da 1a Vara Criminal de Barueri/SP, o suscitado.

Pois bem, passaremos agora a analisar o tipo penal impróprio mais comum quando da ocorrência dos crimes cibernéticos. O estelionato.

Estelionato

Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena – reclusão, de um a cinco anos, e multa.

É importante lembrar que o tipo penal supra descreve que a ação cometida deve-se realizar diretamente pelo seu autor, isto é, a vantagem ilícita em detrimento do réu poderá se realizar sem a necessidade de utilização de meios informatizados.

Porém, existe uma peculiaridade que faz com que o estelionato possa também ocorrer no ambiente virtual. E isso ocorre quando o infrator, no caso, o hacker, utiliza de seus conhecimentos sobre os meios tecnológicos para criar artifícios para iludir ou enganar as suas vítimas. (e.g. simular página de bancos e com isso obter os dados bancários do usuário, simular evento promocional para enganar eventuais consumidores, comuns em campanhas como a Black Friday) através da utilização da prática de pishing para que possa ocorrer no ambiente virtual.

De certo, que não existe, ainda, uma modalidade virtual tipificada para o crime de estelionato e por isso, os tribunais quando se deparam com esses casos acabam fazendo uso da analogia com a sua forma comum prevista no artigo 171 para justificar a sua ocorrência.

Todavia, há um consenso doutrinário de que apenas tipificar o tipo penal não vai suprir todos os problemas, para restringir este delito, é necessário que o estado aja de maneira que informe as pessoas sobre como evitar cair nas arapucas do estelionato virtual.

Nesse sentido, afirma BITTENCOURT[9] (2007):

“O Direito Penal é bastante caracterizado por ter o objetivo de prevenir delitos estabelecendo leis que tem como caráter proibitivo, assim procurando se evitar a pratica de delitos,

distanciando desse modo o transgressor. (...)

Com o surgimento de novos delitos, a legislação também teria que evoluir se criando leis que contemplem as condutas não tipificadas ainda. Se atualizasse a legislação vigente existiria uma melhora na situação mas mesmo assim por mais completa que seja, não seria capaz de contemplar todas as hipóteses de delitos que surgem no dia a dia."

Porém, há um consenso de que apenas tipificar o tipo penal não vai suprir todos os problemas, para restringir este delito, é necessário que o estado aja de maneira que informe as pessoas sobre como evitar cair nas arapucas do estelionato virtual.

E visando solucionar tal problemática, existem vários projetos de leis tramitando nas comissões do Congresso Nacional, em especial o polêmico Projeto de Lei nº 84/99, conhecido como "AI-5 Digital", que além de modificar alguns artigos do código penal tipifica alguns delitos que venham a ocorrer no ambiente virtual, em especial, o do estelionato virtual que possui a seguinte redação:

"difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado".

Tal projeto de lei, no ano de 2005, foi convertido na Lei nº 12.735/2012, que prevê a tipificação de condutas mediante o sistema eletrônico ou digital, com dos 23 artigos originais do respectivo projeto, somente quatro foram sancionados, acabando com qualquer hipótese de inclusão do estelionato digital.

Entretanto, mesmo sem a referida codificação, o crime de estelionato quando ocorrido no meio virtual continuará a utilizar, de forma analógica, a tipificação do caput do artigo 171do Código Penal, bem como o autor (hacker) será punido na mesma pena quantificada para os casos cometidos no meio físico.

Argumente-se ainda que tirando o crime de estelionato, existem outros tipos penais previstos

no próprio Código de Defesa do Consumidor quanto em sua legislação extravagante (e.g. Lei dos crimes contra a economia popular e a lei dos crimes contra a ordem econômica).

Sendo assim, passaremos a analise dos crimes previstos no Código de Defesa do Consumidor:

Lei nº 8.078/1990 (Código de Defesa do Consumidor)

Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:

Pena – Detenção de seis meses a um ano ou multa.

Tal modalidade foi identificada pela primeira vez, no ano de 2018, quando hackers invadiram o sistema de banco de dados do Serasa, alterando o seu código fonte, e vindo a apagar o registro de quase 500.000 (quinhentos mil) devedores de seus bancos de dados causando a indisponibilidade do sistema e prejuízos para o comércio em geral.

Lei nº 1.521/1951 (crimes contra a econômia popular)

Art. 2º. São crimes desta natureza:

IX – obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos (“bola de neve”, “cadeias”, “pichardismo” e quaisquer outros equivalentes);

Pena – detenção, de 6 (seis) meses a 2 (dois) anos, e multa, de dois mil a cinquenta mil cruzeiros.

O tipo penal acima, refere-se a casos de compra em sites na internet (compras coletivas) bem como ao famoso esquema de Pirâmide Financeira onde ao final do investimento somente uma pessoa acaba por sair lucrando com a prática, no caso, quando o ocorre no

ambiente virtual, somente o hacker. Tal crime é muito comum quando da informação recebidas por e-mail como: “ganhe dinheiro trabalhando em casa”, “invista na bolsa”, “aumente sua renda”, “promoção imperdível”, “veja quantas pessoas já adquiriram” entre outros.

Nesse sentido, o Superior Tribunal de Justiça (STJ), ao julgar o Conflito de Competência n º 133.534/SP formou o entendimento de que quando a intenção de se criar um site sob falso pretexto para vender mercadorias e não entregá-las configura-se como crime contra econômia popular e não crime de estelionato, visto que a conduta não induz ao engano uma vitima, mas sim, toda uma coletividade:

CONFLITO NEGATIVO DE COMPETÊNCIA. JUÍZES ESTADUAIS DE COMARCAS DE ESTADOS DIFERENTES. INQUÉRITO POLICIAL. ASSOCIAÇÃO CRIMINOSA. CRIAÇÃO DE SITE NA INTERNET PARA COMERCIALIZAR MERCADORIAS QUE JAMAIS SERIAM ENTREGUES: CONDUTA QUE SE AMOLDA MAIS AO CRIME CONTRA A ECONOMIA POPULAR DO QUE AO ESTELIONATO. CONEXÃO TELEOLÓGICA E INSTRUMENTAL ENTRE OS DELITOS. COMPETÊNCIA DEFINIDA PELO LOCAL DA INFRAÇÃO QUE TEM A PENA MAIS GRAVE (ART. 78, II, “A”, CPP).

1. A criação de site na internet por quadrilha, sob o falso pretexto de vender mercadorias, mas sem a intenção de entregá-las, amolda-se mais ao crime contra a economia popular, previsto no art. 2o, inciso IX, da Lei n. 1.521/1951, do que ao estelionato (art. 171, caput, CP), dado que a conduta não tem por objetivo enganar vítima(s) determinada(s), mas, sim, um número indeterminado de pessoas, vendendo para qualquer um que acesse o site.

2. Nos termos do art. 2o, IX, da Lei n. 1.521/1951, constitui crime contra a economia popular “obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos (“bola de neve’, ‘cadeias’, ‘pichardismo’ e quaisquer outros equivalentes)”.

3. Verificada estreita conexão teleológica (art. 76, II, CPP) e probatória (art. 76, III, CPP) entre

a associação criminosa e o crime contra a economia popular, no caso concreto, a definição da competência segue a regra posta no art. 78, II, “a”, do CPP (local da infração à qual foi cominada a pena mais grave).

4. Dado que o crime de associação criminosa possui pena mais grave (reclusão de 1 a 3 anos) do que a atribuída ao crime contra a economia popular (detenção de 6 meses a 2 anos e multa) e a associação criminosa consumou-se em Goiânia, pois seis dos sete investigados residiam naquela cidade, é forçoso reconhecer a competência do Juízo estadual de Goiânia para conduzir o inquérito policial.

5. Conflito conhecido, para declarar a competência do Juízo de Direito da 8a Vara Criminal de Goiânia/GO, o suscitado.

Pois bem, passaremos agora a analise da ultima modalidade de crime cibernético impróprio contra o consumidor.

Lei nº 8.137/1990

(crimes contra a ordem tributária, ordem econômica e contra as relações de consumo)

Art. 7° Constitui crime contra as relações de consumo:

VII – induzir o consumidor ou usuário a erro, por via de indicação ou afirmação falsa ou enganosa sobre a natureza, qualidade do bem ou serviço, utilizando-se de qualquer meio, inclusive a veiculação ou divulgação publicitária;

Pena – detenção, de 2 (dois) a 5 (cinco) anos, ou multa.

Embora previsto nos crimes contra a ordem tributária, tal regramento legal também prever crimes contra as relações de consumo e que, em tese, também poderá ocorrer no meio virtual.

Pois bem, o tipo penal acima descreve que aquele que induzir consumidor/usuário a erro, através de ardil que indique ou faça afirmação falsa sobre o serviço, sua natureza ou qualidade e por qualquer meio, inclusive o virtual, incorrerá no tipo penal acima descrito.

Tal crime ocorre, no meio virtual com o envio de informes publicitários que escondem malwares que acabam por induzir ao erro o consumidor na compra ou utilização do consumidor ou serviços.

Podemos citar, à titulo de exemplo, quando de compra de produtos ou sites em compras coletivas, a qual o hacker altera dados essências da compra, tais como, o valor, preço do frete entre outros.

Saliente-se que tal crime possui condições agravantes que poderão fazer a sua pena base ser aumentada até 1/3, conforme descrito abaixo:

Art. 12. São circunstâncias que podem agravar de 1/3 (um terço) até a metade as penas previstas nos arts. 1°, 2° e 4° a 7°:

I – ocasionar grave dano à coletividade;

II – ser o crime cometido por servidor público no exercício de suas funções;

III – ser o crime praticado em relação à prestação de serviços ou ao comércio de bens essenciais à vida ou à saúde.

Igualmente, visando dar maior amplitude a investigação e auxiliando na instrução e consequente punição dos crimes acimas previstos, tanto no meio físico quanto virtual, o artigo 16 afirma que qualquer pessoa poderá provocar o Ministério Público, bem como fornecer informações sobre a autoria e materialidade demonstrando a ampla participação social na sua repreensão:

Art. 16. Qualquer pessoa poderá provocar a iniciativa do Ministério Público nos crimes descritos nesta lei, fornecendo-lhe por escrito informações sobre o fato e a autoria, bem como indicando o tempo, o lugar e os elementos de convicção.

Da mesma forma, aquele que seja coautor, participe ou membro de associação criminosa criada para cometer os delitos tipificados nesta lei que confessarem espontaneamente à autoridade policial ou judicial de sua participação no crime terá a sua pena reduzida de um a dois terços, funcionando como uma verdadeira delação premiada, in verbis:

Art. 16. (...).

Parágrafo único. Nos crimes previstos nesta Lei, cometidos em quadrilha ou co-autoria, o co-autor ou partícipe que através de confissão espontânea revelar à autoridade policial ou judicial toda a trama delituosa terá a sua pena reduzida de um a dois terços.

Portanto, esses são os crimes cibernéticos das modalidades próprias ou impróprias, em principal, relativas a fraudes e falsificações que podem ser cometidos contra os consumidores.

IX – AÇÃO PENAL CABIVEL

Diante dos tipos penais explanados acima, qual seria a ação penal cabível para a persecução penal destes crimes, seriam eles são de ação publica ou privada?

No tocante aos crimes cibernéticos próprios (art.154-A/CP) relativos à invasão de dispositivo eletrônico, o próprio artigo 154-B afirma:

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

Logo, da dicção do referido artigo podemos concluir que, via de regra, a ação será pública condicionada à representação. E, caso seja cometida contra os membros da administração direta (União, Estado, Distrito Federal ou Município) e da administração indireta (autarquias, fundações, empresa pública, sociedade de economia mista e as concessionárias de serviço público) a ação será pública incondicionada.

Outrossim, quanto aos demais crimes próprios tais como, furto de dados (art.155, &4º, II/CP) e falsificação de Cartão de Crédito (art.298, parágrafo único/CP) a ação será privada quando se tratar de um ente individualizado, no caso de ocorrer a indeterminação da vitima com base na coletividade ou em se tratando de autoridade pública, a ação passará a ser pública incondicionada.

Já quanto aos crimes cibernéticos impróprios, tais como os especificados no Código de Defesa do Consumidor, Lei dos Crimes contra a Econômia Popular e a Lei dos Crimes Contra a Ordem Tributária, Econômica e contra as Relações de Consumo, essas seguiram o determinado no artigo 100, § 1º do Código Penal:

Art. 100. A ação penal é publica, salvo quando a lei expressamente declara privativa do ofendido.

§ 1º. A ação publica promovida pelo Ministério Público, dependendo, quando a lei o exige, de representação do ofendido ou de requisição do Ministro da Justiça.

Isto é, nos crimes impróprios previstos no Código de Processo Civil e em legislação extravagante a ação penal será, via de regra, pública condicionada à representação.

X – COMPETÊNCIA PARA JULGAMENTO

Nessa questão existe grande discursão sobre o tema, haja vista que como a execução desses crimes se dar por meio remoto, podendo ser feita até mesmo de outro pais, fica a dúvida se a própria autoridade brasileira é competente para o processamento e julgamento.

Como se trata de crimes cibernéticos praticados contra os consumidores, o regramento previsto no próprio Código de Defesa do Consumidor para definir a sua competência (art.101/CDC) não poderá ser aplicado haja vista que o mesmo somente define os danos de responsabilidade civil, pecando quanto aos danos morais.

Nos crimes definidos contra a econômia popular e a própria relação de consumo, previstos nas legislações especais, são omissas quanto a esse ponto, fazendo-nos crer que seguirá as regras de definição e fixação e competência definidas no Código Penal qual seja o local de ocorrência da infração ou do domicilio do réu mas mesmo assim, o mesmo não poderá ser aplicado quando estes são cometidos no território brasileiros por hackers em outros países, posto que a noção de extraterritorialidade brasileira (arts. 5º e 7º/CP) são restritas a acordos internacionais ou contra autoridades publicas representativas do estado.

Entretanto, como são crimes que não ocorrem no meio físico e muitas vezes, é impossível saber quem é o agente ou até mesmo, este se encontre em outro país, quem será competente para o seu julgamento.

Parece-nos que a Lei 12.965/2014[10], que instituiu o marco civil da internet, nos apresenta uma hipótese de solução e de definição de competência para apuração desses crimes:

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa

jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Logo podemos concluir que se houver ao menos um terminal esteja localizado no país ou se o serviço ele for ofertado ao publico brasileiro então será a autoridade judiciária brasileira competente para apuração do crime.

XI – CONCLUSÃO

Ante tudo o que foi dito acima, estas são as hipóteses mais corriqueiras de crimes cibernéticos, tanto na modalidade própria quanto na modalidade imprópria, que podem ocorrer nas relações de consumo, bem como ainda se é necessário a apresentação de uma legislação mais abrangente que preveja todas as possíveis práticas criminosas que podem ocorrer no ambiente virtual capazes de gerar dano no mercado de consumo.

Esclarecemos ainda, contudo, que de acordo com o evoluir dos meios digitais e consequentemente do surgimento ou aperfeiçoamento de novas práticas virtuais ilícitas outras hipóteses tipificadas tanto no Código Penal como em legislações especiais podem vim a ocorrer.

Para isso é necessária uma intensa vigilância sobre os meios eletrônicos a fim de coibir a ocorrência e a proliferação destes crimes através de criação de órgãos de investigação e repressão especializados contra estes tipos de crimes.

REFERÊNCIAS

ALMEIDA, João Batista de. A proteção jurídica do consumidor. 7. ed. São Paulo: Saraiva, 2009.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal: parte geral. São Paulo, 2007.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro, RJ, 7 dez. 1940.

BRASIL. Lei nº 1.521, de 26 de dezembro de 1951 Legislação vigente sobre crimes contra a economia popular. Rio de Janeiro, RJ, 26 dez. 1951.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF, 11 set. 1990.

BRASIL. Lei nº 8.137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Brasília, DF, 27 dez. 1990.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera O Decreto-lei no 2.848, de 7 de Dezembro de 1940 – Código Penal, O Decreto-lei no 1.001, de 21 de Outubro de 1969 – Código Penal Militar, e A Lei no 7.716, de 5 de Janeiro de 1989, Para Tipificar Condutas Realizadas Mediante Uso de Sistema Eletrônico, Digital Ou Similares, Que Sejam Praticadas Contra Sistemas Informatizados e Similares; e Dá Outras Providências.. Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe Sobre A Tipificação Criminal de Delitos Informáticos; Altera O Decreto-lei no 2.848, de 7 de dezembro de 1940 – Código Penal; e Dá Outras Providências. Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e

deveres para o uso da Internet no Brasil. Brasília, DF, 23 abr. 2014.

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

GARCIA, Leonardo de Medeiros. Código de Defesa do Consumidor: código comentado. 6ª ed., Niterói: Impetus, 2010.

MARQUES, Cláudia Lima. Confiança no Comércio Eletrônico e a Proteção do Consumidor. São Paulo: Revista dos Tribunais, 2004.

MINISTÉRIO PÚBLICO FEDERAL, Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, vol.3, Criminal. – Brasília: MPF, 2018.

POZZEBOM, Rafaela. SEGURANÇA DIGITAL. Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit. 2015. Disponível em: <https://www.oficinadanet.com.br/segurança/>. Acesso em: 12 nov.2020.

RODRIGUES, Viviane. CONSUMIDOR 4.0: SAIBA QUEM ELE É E VEJA COMO SE RELACIONAR COM ELE. 2018. Disponível em: <https://blog.iclips.com.br/consumidor-4.0>. Acesso em: 05 jun. 2020.

ROSA, Fabrízio. Crimes de Informática. 2.ed. Campinas: BookSeller, 2006.

ROVER, Aires José. Direito e Informática. Barueri: Manole, 2004.

TEIXEIRA, Rafael Fialho. Consumidor 3.0: entenda o perfil do consumidor atual e como atendê-lo. 2017. Disponível em: <https://blog.deskmanager.com.br/consumidor-3-0/>. Acesso em: 15 jun. 2020.

VALLE, Alberto. O que é e-commerce: definição e variantes de modelos de comércio eletrônico. 2017. Disponível em:

<https://www.empreendedoresweb.com.br/o-que-e-e-commerce/>. Acesso em: 12 jun. 2020.

VIANA, Tulio Lima. Do delito de dano e de sua Aplicação ao direito penal informático. Revista dos Tribunais, São Paulo, a. 92, v. 807. janeiro 2003. VIDAL, Carlos Antônio. Crimes Informáticos, Saraiva: São Paulo, 2013.

---

[1] Advogado. Especialista em Direito Processual Civil. Especialista em Direito do Consumidor. Mestrando em Direito.

[2] Doutor em Direito Penal pela Universitat de València- Espanha; Professor Permanente do Programa em Direito e Desenvolvimento do Centro Universitário de João Pessoa – PPGD/UNIPÊ e do Programa de Pós-Graduação em Ciências Jurídicas da UFPB – PPGCJ-UFPB; Advogado; Presidente da Associação Nacional da Advocacia Criminal – PB, e Presidente do Superior Tribunal de Justiça Desportiva – STJD, da Confederação Brasileira de Automobilismo – CBA.

[3] ROSA, Fabrízio. **Crimes de Informática.** 2.ed. Campinas: BookSeller, 2006.

[4] TEIXEIRA, Rafael Fialho. **Consumidor 3.0: entenda o perfil do consumidor atual e como atendê-lo**. 2017. Disponível em: <https://blog.deskmanager.com.br/consumidor-3-0/>. Acesso em: 15 jun. 2020.

[5] RODRIGUES, Viviane. **CONSUMIDOR 4.0: SAIBA QUEM ELE É E VEJA COMO SE RELACIONAR COM ELE**. 2018. Disponível em: <https://blog.iclips.com.br/consumidor-4.0>. Acesso em: 05 jun. 2020.

[6] VALLE, Alberto. **O que é e-commerce: definição e variantes de modelos de comércio eletrônico**. 2017. Disponível em: <https://www.empreendedoresweb.com.br/o-que-e-e-commerce/>. Acesso em: 12 jun. 2020.

[7] VIANA, Tulio Lima. **Do delito de dano e de sua Aplicação ao direito penal informático**. Revista dos Tribunais, São Paulo, a. 92, v. 807. janeiro 2003

[8] VIDAL, Carlos Antônio. **Crimes Informáticos**, Saraiva: São Paulo, 2013.

[9] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte geral.** São Paulo, 2007.

[10] BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF, 23 abr. 2010.