Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 29.11.2017
Aprovado em: 30.12.2017

A FRAUDE COMETIDA POR MEIOS INFORMÁTICOS SOB O PRISMA DA VITIMODOGMÁTICA

Maria Auxiliadora de Almeida Minahim[1]
Luíza Moura Costa Spínola[2]

RESUMO: Esse trabalho realiza um estudo acerca da influência do comportamento da vítima na fraude cometida pela *Internet*. Explicam-se os riscos criados pela popularização de dispositivos informáticos e o conceito de crimes informáticos. Destacam-se técnicas para cometer fraudes que contam com a colaboração da vítima. Analisam-se quais as situações em que o comportamento da vítima constitui uma peça fundamental para a consumação do delito. Conclui-se que o uso da *Internet* exige uma postura de cuidado que, caso não seja observada pela vítima, pode acarretar redução da pena para o autor e, em casos extremos, gerar a atipicidade da conduta.

PALAVRAS-CHAVE: Direito Penal; Crimes Informáticos; *Internet*; Fraude; Autorresponsabilidade.

THE FRAUD COMMITTED BY COMPUTERISED MEANS UNDER THE OPTICS OF VITIMODOGMATIC

ABSTRACT: This study investigates the influence of victim behavior on Internet fraud. The risks created by the popularization of computer devices and the concept of computer crimes are explained. We highlight the techniques to commit fraud that count with victim's collaboration. Situations in which the behavior of the victim constitutes a fundamental piece for the consummation of the crime are analyzed. It is concluded that the use of the Internet requires a cautious stance that, if it is not observed by the victim, may reduce the sentence for the perpetrator and, in extreme cases, the perpetrator's conduct is not considered criminal.

KEY WORDS: Criminal Law; Cybercrimes; Internet; Fraud; Self-responsibility.

1 INTRODUÇÃO

A sociedade atual, também conhecida como Sociedade da Informação, já não pode ser compreendida sem a existência e uso de novas tecnologias, que facilitam,

[1] Professora Titular de Direito Penal da Faculdade de Direito da Universidade Federal da Bahia.
Doutora em Direito Penal pela Universidade Federal do Rio de Janeiro e pela Universidade Federal do Paraná.
Rua da Paz, s/n - Graça, Salvador - BA, 40150-140.
minahim@terra.com.br

[2] Advogada Graduada em Direito pela Faculdade de Direito da Universidade Federal da Bahia.
Especialista em Ciências Criminais pela Faculdade Baiana de Direito.
Rua da Paz, s/n - Graça, Salvador - BA, 40150-140.
luiza.mcspinola@gmail.com

significativamente, a vida humana, permitindo desenvolver atividades diversas em um futuro de desenvolvimento com amplas possibilidades.

Ao longo da década de 1960, as organizações passaram a encarar o computador não somente como um *meio* para processar informações, mas como *bancos de dados*. O desenvolvimento dessas novas tecnologias deu ensejo ao que se considera Revolução Digital. Essa revolução pode ser explicada como um movimento que viabilizou o emprego de novas tecnologias que mudam e facilitam o cotidiano das pessoas.

Vive-se, atualmente, em uma sociedade na qual a informação possui um papel de destaque. Esse aspecto relevante é fruto da crescente urbanização da sociedade, iniciada com a Revolução Industrial e intensificada ao longo do século XX. A mudança da organização em grupos rurais para a vida em metrópoles tornou a divisão de bens para convivência social adequada mais complexa e passou a exigir o conhecimento acerca do outro como condição para tornar possíveis essas novas relações. Em suma, da mesma maneira que se passou de uma sociedade agrária para uma sociedade industrial, hodiernamente, avança-se dela para uma sociedade informacional.

A popularização do computador, em virtude da constante diminuição de preços e melhor acessibilidade, contribui para que cada vez mais pessoas no mundo tenham acesso a dispositivos informáticos e, por conseguinte, à rede mundial de computadores, a *Internet*. Com a difusão de dispositivos informáticos, os crimes relacionados às Tecnologias da Informação e Comunicação (TIC) se tornaram frequentes e variados.

O chamado *ciberespaço* tornou-se um campo para o cometimento de delitos que já são previstos em ordenamentos jurídicos e viabiliza a prática de condutas que, embora sejam altamente prejudiciais, ainda não são necessariamente incriminadas. A vítima dos delitos informáticos distingue-se das vítimas comuns, pois a conduta de utilizar a *Internet* torna essa espécie de criminalidade possível por ela mesma. O comportamento da vítima para a realização do fato punível ganha em tais crimes um viés especial, que merece ser analisado à luz das modernas teorias de autorresponsabilização do titular do bem jurídico.

Este estudo tem por finalidade analisar quais são as posturas adotadas pelas vítimas em crimes informáticos que podem ser levadas em consideração para determinar o seu grau de responsabilidade nesses crimes, se é que tal participação gera o perigo necessário para a presente reflexão. Inicialmente, será feita uma breve explanação sobre essa categoria de crimes e, em seguida, cuidar-se-á de alguns aspectos da imputação do dano no âmbito da

vítima. Por fim, será respondida à questão principal sobre a atribuição de responsabilidade à vítima em crimes informáticos de fraude.

2 CRIMES INFORMÁTICOS

Os crimes informáticos, por seu caráter atual, apresentam, ainda, certa divergência na sua conceituação e definição de características, bem como na identificação dos bens jurídicos tutelados. A princípio, é necessário esclarecer que não existe consenso no que concerne à denominação dos delitos relacionados à tecnologia. Crespo (2011, p. 48) explica, em sua obra, que na doutrina brasileira encontram-se diversas designações, como "crimes de computação", "crimes virtuais", "crimes digitais" ou "delitos informáticos".

Neste trabalho, fez-se a opção pelo termo "crimes informáticos", pois na linha de Sydow (2015, p. 56) entende-se que se trata de uma criminalidade que não se restringe às tecnologias existentes, nem está limitada à *Internet* ou aos computadores. São condutas que utilizam novas ferramentas em conformidade com a evolução da ciência e sua introdução nas atividades cotidianas, que podem ser a telefonia, a computação ou qualquer outro ramo que crie aparatos facilitadores para as atividades habituais. Crespo (2011, p. 49), por sua vez, também se posiciona nesse sentido, quando admite que não é possível vincular somente o computador às condutas praticadas por meio da informática, vez que se verificam delitos cometidos com o uso das telecomunicações. Por isso, pode-se afirmar que a expressão se refere a um conjunto de atividades ilícitas praticadas com o uso e abuso das tecnologias de informação e comunicação (OXMAN, 2013).

Não se desconhece, porém, que a denominação "crime informático", mais recentemente, sobretudo entre os anglo-saxões, vem sendo substituída por "cibercrime" ou "cibercriminalidade", que, muito propriamente, já contém a ideia do espaço de comunicação universal aberto que é o *ciberespaço*. Assim, a "cibercriminalidade" é um neologismo que abriga uma série de novos fenômenos, mas também inclui a prática da criminalidade tradicional, que se realiza por intermédio de sistemas de redes informáticas de transmissão e troca de dados por *Internet*.

Crespo (2011, p. 50) explica que, à primeira vista, os crimes informáticos seriam de meio, ou seja, delitos tradicionalmente previstos no ordenamento jurídico que, por conta das

facilidades proporcionadas pela tecnologia, passam a ser praticados por meio desta. É o que, frequentemente, ocorre com os crimes de ameaça, contra a honra e estelionato, que podem ser cometidos por *e-mails*, *SMS* (*Short Message Service* ou Serviço de Mensagens Curtas, em tradução livre para o português) e redes sociais. Contudo, a conceituação foi ampliada para abarcar outras condutas em que o alvo é o sistema informático ou o banco de dados, como veremos mais adiante. Dessa forma, tais atividades põem em risco não só bens jurídicos individuais, mas ameaçam, também, redes coletivas.

Essa espécie de criminalidade apresenta certa complexidade na sua prevenção. Os crimes do mundo real ainda são mais fáceis de serem combatidos, pois o agente está limitado ao espaço e pode cometer somente um crime ou uma sequência de crimes por vez, de acordo com Sydow (2015, p. 58). Cometido o fato, o crime real apresenta uma localização precisa, e a polícia pode agir no próprio local onde o delito foi cometido, concentrada no ambiente em que ocorreu. O mesmo não ocorre com os delitos informáticos.

Assim, parece razoável admitir que os crimes informáticos apresentam características peculiares. Sydow (2015, p. 59) leciona que essa categoria de crimes não exige o contato físico entre vítima e ofensor e não necessita de um maior planejamento, como visitação prévia do local onde o crime será cometido, pois esse ocorre em um ambiente sem povo, governo ou território e não acarreta altos riscos para o agente, nem provoca sensação de violência, assim como não há “padrões” para seu cometimento. O criminoso informático pode praticar mais de uma conduta lesiva ao mesmo tempo, em vários lugares simultaneamente, e conta com a vantagem de não existirem profissionais quantitativa e qualitativamente capacitados para realizar as investigações. Ademais, o autor dessa categoria de crimes pode atuar facilmente de forma transnacional.

2.1 QUESTÕES A RESPEITO DO BEM JURÍDICO PROTEGIDO

Crespo (2011, p. 56) ressalta o questionamento acerca da existência de novos bens jurídicos e, ainda, se podem ser tutelados pelo Direito Penal. Ao considerarmos as condutas ilícitas através da informática, constatamos a possibilidade de lesão a outros bens jurídicos. Dessa forma, é possível falar em condutas dirigidas a atingir não apenas os valores que já gozam de proteção jurídica, tais como a honra, o patrimônio e a fé pública, como também as

informações armazenadas e a segurança dos sistemas de redes informáticas ou de telecomunicações.

Em verdade, conforme Llinares (2012, p. 35), a delinquência informática não definia os bens jurídicos comuns protegidos por essa categoria de delitos, mas se reportava a um âmbito de risco derivado da expansão da tecnologia da informática como uma característica comum de tais infrações. Em face da necessidade de prevenir e punir tais comportamentos, houve tentativas no sentido de subsumir-se as condutas aos tipos já existentes e ajustá-los, quando necessário, para que pudesse haver tipicidade na prática das novas ações. Os delitos informáticos, portanto, e segundo o mesmo autor, compreendiam tipologias de condutas, e não novos tipos penais (LLINARES, 2012, p. 37).

Wendt e Jorge (2013, p. 18), por seu turno, aderem à divisão das condutas indevidas praticadas por computador em dois grupos: (i) ações prejudiciais atípicas e (ii) crimes cibernéticos. As ações prejudiciais atípicas são condutas praticadas por meio da *Internet* que podem vir a causar transtornos para a vítima, mas que não são crimes. Como exemplo de uma ação dessa espécie, os autores citam a hipótese de uma pessoa que acessa o computador de um conhecido sem o objetivo de obter, modificar ou excluir dados, ou sem violar um mecanismo de segurança. No entanto, Wendt e Jorge (2013, p. 18) observam que esses transtornos podem ser responsabilizados na esfera civil.

Sydow (2015, p. 88), em sua obra, diferencia *delitos informáticos próprios* de *impróprios*. Delitos informáticos impróprios são delitos comuns cometidos por meio de mecanismos informáticos como ferramentas, sendo que outras formas poderiam ter sido escolhidas para a prática. São delitos de forma livre.

Como exemplo de delito informático impróprio ou crime cibernético aberto, podemos citar o *cyberbullying*. Pérez Martínez e Ortigosa Blanch (2010, p. 15) explicam que essa conduta se configura quando um indivíduo (ou grupo) utiliza tecnologias da informação e da comunicação – como *e-mails*, *SMS*, serviços de mensagens instantâneas – de forma repetitiva e hostil com o intuito de causar danos a outro. O *bullying* pode ser praticado de outras maneiras, mas, quando são utilizadas as tecnologias da comunicação, está configurado o *cyberbullying*, um delito informático impróprio.

Já os crimes informáticos próprios, também chamados de delitos de risco informático, são condutas praticadas contra bens jurídicos informáticos propriamente ditos,

como sistemas informatizados ou de telecomunicações ou dados, conforme leciona Crespo (2011, p. 63). São diferentes dos crimes informáticos impróprios, que se dirigem a bens jurídicos tradicionais, ou seja, não relativos à tecnologia.

Este trabalho centra-se na figura da vítima e sua participação ou colaboração para a produção do resultado lesivo. Assim, os crimes nele tratados são apenas com o fim de caracterizar o cenário no qual se desenvolve essa relação, tendo sido eleitos os mais comuns: a invasão informática, inserção de vírus, interceptação de *e-mail*, *scamming* e *phishing*.

2.2 ALGUMAS ESPÉCIES DE CIBERCRIMES

A invasão informática, também chamada de "acesso não autorizado" ou *hacking*, refere-se ao ingresso não autorizado de um usuário no sistema alheio, que pode ter ou não o objetivo de obter alguma vantagem (SYDOW, 2015, p. 114). O termo *hacking* remete aos chamados *hackers*, pessoas com conhecimentos específicos em informática e responsáveis pela maior parte dos delitos praticados com o uso de computadores e *Internet*, conforme leciona Brito (2013). Entretanto, Sydow (2015, p. 115) ressalta que não necessariamente ocorre o uso de mecanismos de violação dos sistemas alheios para a obtenção de acesso: boa parte dos sistemas operacionais apresenta falhas de programação, os chamados *bugs*, que permitem que usuários acessem informações alheias.

Sobre a inserção de vírus, Crespo (2011, p. 74) explica que se trata de segmentos de códigos de computação que se acoplam a programas ou sistemas de maneira a se propagarem pelos dispositivos informáticos e contaminarem outros sistemas, por meio de *e-mails* remetidos automaticamente ou por transmissão de dados maliciosos por outros métodos. Os vírus mais comuns, segundo Wendt e Jorge (2013, p. 24), são aqueles categorizados como *boot*, que se fixam na parte de inicialização do sistema; o vírus *time bomb*, cuja ativação é deflagrada em determinada data; e o *worm*, que se instala na memória do computador e se replica maquinalmente.

Quanto ao crime de interceptação de *e-mail*, Sydow (2015, p. 133) instrui que esse delito seria representado pela ação de se impedir que a mensagem de correio eletrônico, enviada por um remetente, chegue ao seu destinatário. O art. 10 da Lei nº 9.296 (cf. BRASIL, 1996) prevê como crime o fato de alguém realizar interceptação telefônica, telemática ou

informática sem autorização judicial em desconformidade com a lei, coibindo a conduta de interceptar ilegalmente dados em sistemas informáticos.

O termo *scamming*, por sua vez, vem do verbo inglês *scam*, que significa a ação de defraudar, sendo que a mesma palavra pode significar um esquema fraudulento, conforme explica Sydow (2015, p. 125). Trata-se do ato de valer-se de meio informático para atuar com o intuito de obter alguma vantagem sobre o usuário. Ainda de acordo com o autor, em regra se trata de golpes ou armadilhas, chamadas de *honey pots*, criados para que usuários que não tenham tanto conhecimento sobre o meio cibernético acabem por agir segundo o objetivo do delinquente na *Internet*.

O *phishing* também é um tipo de fraude cometida através do meio da rede mundial de computadores. Trata-se de uma prática advinda da engenharia social, método utilizado para disfarçar a realidade e, assim, explorar ou enganar a confiança de uma pessoa que possua dados aos quais se quer ter acesso, de acordo com Crespo (2011, p. 82). O termo *phishing* vem do vocábulo *fishing*, que significa "pescar". No crime de *phishing*, uma pessoa envia uma mensagem eletrônica a outrem e, valendo-se de pretextos falsos, induz a vítima a fornecer informações relevantes, como número de cartão de crédito e dados de contas bancárias. Wendt e Jorge (2013, p. 21) explicam que, na engenharia social, o autor do crime se concentra nas fragilidades que a vítima possa apresentar em algumas situações do cotidiano. O que facilita a prática desse tipo de crime é a falta de conhecimento do usuário da *Internet*, a ponto de acreditar em todas as informações que chegam até ela.

Pode-se perceber que, alguns crimes informáticos próprios, mais precisamente aqueles que envolvem fraude, contam com a participação da vítima. Na seção seguinte, serão tratados alguns aspectos da participação da vítima na produção do resultado.

3 IMPUTAÇÃO DE RESULTADO À CONDUTA DA VÍTIMA

Desde a Antiguidade, o Direito Penal tem destacado que, em muitos delitos, existe uma inter-relação entre delinquente e vítima, conforme destacam Bustos Ramírez e Pijoan (1993, p. 13). Mencionam o clássico exemplo da fraude em que o autor do crime se aproveita da ânsia de lucro do enganado, a exemplo de venda a preço baixo de um bilhete de loteria premiado, para consumar o delito.

Tem-se ressaltado na doutrina alemã, e também na espanhola, que o titular do bem jurídico tem o dever de zelar pelo mesmo e que tal dever lhe incumbe mais do que a qualquer outra pessoa, na qualidade de ser autônomo e responsável. As construções podem ser descritas como um conjunto de tendências que introduzem uma nova perspectiva no que tange ao comportamento da vítima, pois não se limitam a dar tratamento legal aos conhecimentos precedentes disponibilizados pela Criminologia, segundo Cancio Meliá (1999, p. 28), mas procuram inseri-la na teoria do tipo.

De forma geral, as construções caminham no sentido de que não é possível imputar um resultado ao agente, quando a vítima participou ativa e voluntariamente para sua ocorrência, seja por que se põe em situações de perigo, ou por que, por sua vontade, as aceita. Dentre essas, a vitimodogmática, a imputação de responsabilidade no âmbito da vítima, a autocolocação em perigo e certas formas de heterocolocação.

Diferentemente da perspectiva da Vitimologia, que, apesar de estudar a contribuição do sujeito passivo para o resultado, o faz apenas visando a oferecer elementos para a compreensão do fenômeno do crime e sua prevenção, a vitimodogmática pretende benefícios para o autor da ação em razão da conduta do titular do bem. É bem verdade que os estudos vitimológicos revelam que a vítima não é sempre um sujeito inerte sobre o qual recai a conduta do autor, mas, contrariamente, diversas vezes contribui de forma expressa para a lesão de seu próprio bem jurídico (MINAHIM, 2015, p. 95). Na perspectiva penal vigente, esse modo de atuar deve influir sobre a qualificação jurídico-penal da conduta do autor em termos de atenuar sua responsabilidade.

Esse posicionamento pode ser considerado moderado e é defendido por autores como Hillenkamp e Hassmer, que entendem que o comportamento da vítima pode ser considerado, de modo geral, no âmbito de medição judicial da pena, produzindo uma atenuação da responsabilidade do autor, ainda que dentro do marco penal típico (SILVA SANCHÉZ, 1990, p. 109). O fundamento de tal opção repousa na ideia de que, por vezes, o comportamento da vítima pode diminuir o conteúdo da antijuridicidade da conduta do autor ou a culpabilidade.

A vitimodogmática vai mais adiante, tratando de situações nas quais o autor pode eximir-se da responsabilidade pelo fato a que deu causa em razão do comportamento do titular do bem. Seus maiores expoentes, como Schünemann, Schultz e Hassemer, visam a criação de uma dogmática a partir da figura da vítima.

A hipótese central da vitimodogmática é bem compreendida por Silva Sánchez (1990, p. 107), que a explica como sendo a "dogmática orientada ao comportamento da vítima". Schünemann (2002), principal elaborador da teoria, parte do chamado princípio vitimológico, segundo o qual o autor só deve ser punido se a vítima merecia proteção e dela necessitava. Por sua vez, o titular apenas merece a proteção do Estado, quando atua de forma zelosa com seu bem jurídico: se esse estava em suas mãos e a vítima podia, nas circunstâncias, tê-lo protegido sem maiores esforços, não há por que punir o criminoso. À necessidade de pena, deve corresponder a necessidade de proteção, o que estaria ausente em tais casos. A pena, como *ultima ratio* do Estado, não deve ser aplicada em situações em que a vítima não merece e não necessita de proteção.

Cabe, ainda, explicar alguns conceitos quanto à participação da vítima no resultado danoso. Um deles é o de autocolocação em perigo. Roxin (2012, p. 2) leciona que a autocolocação em perigo ocorre quando alguém sofre um dano por meio de sua própria ação arriscada, ainda que outro também tenha contribuído para produzi-lo. O autor traz como exemplo uma corrida de motos realizadas por A e B em um terreno intransitável, na qual A sofre por sua própria culpa um acidente mortal. B, ainda que tenha cooperado causalmente para a morte de A, não pode ser responsabilizado, uma vez que A se colocou em perigo por sua própria vontade. Em suma, nesse caso a participação do terceiro é impune.

Outra hipótese em que o indivíduo coloca a si mesmo em uma situação de perigo é a heterocolocação em perigo consentida. Trata-se do caso em que alguém coloca outrem em perigo, mas de tal forma que este adere ao perigo conhecido com pleno conhecimento do risco, conforme as lições de Roxin (2012, p. 2). Como exemplo de heterocolocação em perigo consentida, pode-se citar o da pessoa que, após sair de uma festa, pega carona com outra que está alcoolizada e, portanto, não está em condições de dirigir de forma segura. Caso ocorra algum acidente e a vítima venha a sofrer alguma lesão ou mesmo falecer, pretende-se que o motorista não seja responsabilizado.

Já a teoria da imputação à vítima, desenvolvida por Cancio Meliá (1999), parte de alguns pressupostos da vitimodogmática, mas entende que é preciso ajustá-los com vistas a precisar, no plano normativo, os requisitos que permitam a exclusão da responsabilidade do sujeito ativo em razão do comportamento da vítima (MINAHIM, 2015). Partindo da ideia de sujeito autônomo, que pode organizar e usufruir de seus bens da forma que melhor julgar, o

autor também afirma sua responsabilidade com seus bens jurídicos, incumbindo-lhe protegê-los das intervenções de terceiros. Se não o faz, gerando um risco para seus próprios bens, incumbe-lhe, preferencialmente, a responsabilidade pelos danos que possam resultar da ação de outrem por ele permitida.

Há uma característica própria dos crimes de fraude cometidos pela *Internet* que aproxima as vítimas dos estudos já realizados, conforme se verá, uma vez que a contribuição do enganado, por sua falta de cuidado ou mesmo um estímulo quanto à sua proteção no espaço cibernético, é fundamental para que o crime seja cometido. Sendo a informática dependente de comandos dos usuários, conforme destaca Sydow (2015, p. 245), uma parcela considerável da cautela é de responsabilidade do internauta.

4 O COMPORTAMENTO DA VÍTIMA NO CRIME INFORMÁTICO DE FRAUDE

O número de vítimas de crimes informáticos vem crescendo de forma descontrolada. O fato de estar conectado à *Internet* através de um computador, *desktop, notebook, tablet* ou *smartphone* é suficiente para que a pessoa se torne uma vítima em potencial. Nesse sentido, Brito (2013, p. 74) realça que o estudo das vítimas e seus comportamentos na rede mundial de computadores é de extrema relevância para que sejam detectadas as condutas que possam contribuir para o aumento dessa criminalidade.

Para Agustina, (2014, p. 112), a própria natureza humana apresenta essa inclinação à mentira como mecanismo de manipulação e inflição de danos a terceiros, especialmente se a vítima reúne determinadas características que a tornam mais vulnerável, uma vez que o *ciberespaço* promove atitudes de confiança excessivas, marcadas, também, por ingenuidade ou irreflexão.

Considerando a fraude como uma arte antiga, Agustina (2014, p. 112-113) entende que o espaço cibernético permite que sejam atingidas muito mais vítimas, ainda que por um só ofensor. O autor cita a tese do sociólogo norte-americano Orgburn (1964 apud AGUSTINA, 2014, p. 113), segundo a qual surge inicialmente uma mudança tecnológica, seguida de uma mudança sociológica ou cultural e, finalmente, uma mudança no *modus operandi* dos delitos. Para Agustina (2014, p. 113), as transformações tecnológicas potencializam tanto a ingenuidade quanto a estupidez humana.

A vitimização *on-line* constitui um fenômeno relativamente recente associado, em grande parte, à generalização e à alta acessibilidade das novas tecnologias, segundo estudos de Gaméz-Guadix, Orue e Borrajo (2014, p. 161). Ressalta-se que, embora apresentem algumas características comuns com a vitimização presencial, como a presença de agressores e vítimas e a intenção de causar dano, todos os crimes que acarretam a vitimização *on-line* apresentam alguns traços derivados da própria natureza das interações através dos novos recursos tecnológicos.

Na vitimização *on-line,* realça-se o limite temporal, pois uma vez que uma imagem, vídeo ou informação maliciosos são difundidos na *Internet*, provavelmente, permanecerão no *ciberespaço* por tempo indefinido, o que aumenta a possibilidade de dano para os usuários. Ademais, a vitimização *on-line* é indireta, uma vez que vítima e agressor não se conhecem.

Como o agressor não percebe a reação da vítima de forma imediata, isso pode facilitar a insensibilidade e a falta de empatia, o que pode incrementar o desejo de prosseguir na realização da conduta típica (GAMÉZ-GUADIX; ORUE; BORRAJO, 2014, p. 163). Há teorias que embasam essa ideia, destacando que a distância da vítima diminui a dificuldade de censura do agente.

Van Dijk (2014, p. 188) conceitua a "ciberfraude" como o engano a pessoas que realizam transações comerciais por meio da *Internet* com o intuito de conseguir um benefício patrimonial. O autor ainda destaca que em diversos países, principalmente Estados Unidos, Canadá, Austrália, Reino Unido, Japão e Coreia do Sul, a "ciberfraude" se converteu em um tema de interesse político e acadêmico, dando ensejo à criação de mecanismos específicos através dos quais cidadãos ou empresas podem denunciar essas condutas.

A fraude realizada por meios informáticos com o objetivo de obter vantagem ilícita é denominada de *scamming*, de acordo com Sydow (2015, p. 223), conforme já mencionado anteriormente. O autor explica que o *scammer* é um estelionatário virtual, que se vale de armadilhas e golpes elaborados com o objetivo de obter informações geradas a partir de dados, por sua vez, gerados por *bits* (unidades matemáticas virtuais).

As pessoas que cometem esse tipo de crime procuram arquitetar esquemas que gerem credibilidade no usuário. A ideia é convencer a vítima de que aquele *site* ou mensagem são verdadeiros e que merecem atenção, seja por que se trata de uma situação pessoal dolorosa e comovente, seja pelo fato de sinalizarem uma oportunidade única para o internauta, seja por comunicarem um fato sério, como uma audiência criminal, ou, ainda, por apresentarem elementos que levem a vítima a acreditar que se trata de uma mensagem de instituições sólidas, como bancos ou emissoras de televisão (SYDOW, 2015, p. 225).

Brito (2013, p. 76) ensina que alguns bancos já elaboraram campanhas educativas de proteção ao uso da *Internet*, por existirem situações em que os criminosos enviam *e-mails* solicitando dados bancários e até criam páginas que imitam *sites* de bancos, o que está se tornando cada vez mais frequente. Um exemplo ilustrativo foi oferecido pela Revista *Contratacion Eletrónica* (cf. OXMAN, 2013) sobre uma lide entre o Santander e um cliente, na qual a decisão judicial foi no sentido de que o banco não devia responder civilmente por danos ao correntista que forneceu todos os números de seu cartão de crédito, em razão de pedido feito em página da *Web* que simulava ser a página original do mesmo banco. A Corte entendeu que a vítima deveria ter atuado com diligência e buscado informações junto ao

Serviço de Atendimento ao Cliente e, por não ter atendido aos deveres que são exigidos de um cidadão médio, não lhe era devida qualquer indenização por parte do Santander.

Outra situação análoga, desta feita a respeito de histórias de sofrimento, forjadas pelos autores de fraudes através da *Internet*, é oferecida por Van Dijk (2014, p. 202), que menciona, em sua obra, o caso de uma mulher que recebeu um *e-mail* de um homem nigeriano que pedia a sua ajuda para que pudesse poder receber uma herança. A mulher aceitou ajudá-lo, pois o homem havia manifestado a intenção de criar uma organização de caridade para os órfãos da Nigéria com o dinheiro procedente da herança. A vítima chegou a transferir um total de cem mil euros a título de pagamento antecipado e de pagamento de faturas de assistência jurídica. Ocorre que, posteriormente, durante participação em uma pesquisa que reuniu um grupo de pessoas vítimas de "ciberfraude", a mulher não se mostrou incomodada pelas perdas ocasionadas, posto que considerava que havia concordado com a transação.

É possível falar, também, em enganos praticados através do *fake love* ou "amor falso", em tradução livre para o português, no qual se simula uma relação de afeto, geralmente, acompanhada de pedidos de empréstimos e situações dessa natureza (BRITO, 2013, p. 77).

Alguns autores, a exemplo de Sydow (2015, p. 227), afirmam que a pessoa que cai em golpes realizados por meio da *Internet* costuma contribuir para tal ato, uma vez que deixa de se informar das principais ameaças e fraudes da rede, que são constantemente comunicados por meio de jornais, revistas, *e-mails* e pelos *sites* de empresas que têm seus nomes e logotipos frequentemente usados de maneira indevida nesses golpes. Outros autores, a exemplo de Brito (2013, p. 78), também ressaltam que a maioria dos crimes cometidos por meio da *Internet* só é consumada em razão da cooperação proporcionada pelas vítimas.

Não obstante, estudos realizados por Ngo e Paternoster (2011) revelam que características individuais derivadas ou obtidas da teoria geral do crime na Criminologia não são adequadas para explicar as diversas formas de vitimização no espaço cibernético. Suas conclusões resultam de artigo realizado através de revisão bibliográfica séria e partem da Teoria Geral da Vitimização elaborada por Michael Gottfreds, assumindo que pessoas podem influir na propensão ou maior controle para a prática de crimes, realçando a falta de autocontrole. Como resultado secundário dos estudos, os mesmos pesquisadores perceberam

que tal característica colaborava no processo de vitimização. Trabalhos posteriores procuraram aplicar a hipótese e conhecer a correlação entre baixos níveis de controle e vitimização. No entanto, apesar de concluírem por sua fragilidade na compreensão desse fenômeno, revelaram, através de Bossle e de Holtfrete, que há correlações entre baixos níveis de autocontrole e vitimização no espaço cibernético e fraude, respectivamente (NGO; PATERNOSTER, 2011).

Em vista das pesquisas referidas, todavia, a convocação das teorias que procuram imputar à vítima uma corresponsabilidade pelo resultado lesivo causado a si própria pode resultar injusta. É bem verdade que há um nível de ingenuidade não passível de indulgência estatal, mas tal comportamento deve se refletir na pena aplicada ao autor da ação fraudenta, mitigando-a, mas não resultar em isenção de pena.

É possível, como aponta Agustina (2014, p. 135), entender que algumas vezes a fraude é tão óbvia que dá ensejo a uma responsabilização civil, mas poder-se-ia considerar insuficiente o engano para constituir um ilícito penal que teria respeitada sua natureza subsidiária. De certa forma, o pensamento do autor é alinhado com as teorias que atribuem a vítima um dever de cuidado, até mesmo para sair do estado de ingenuidade. Para o mesmo autor, o problema central no delito de fraude em sua modalidade tradicional está no tratamento da perspectiva da responsabilização da vítima para precisar a relevância do erro ou do engano, e se foram suficientes em relação aos deveres de sua autoproteção.

É necessário considerar que a sociedade de riscos exige uma maior atenção de seus integrantes, sendo essa a contrapartida da modernidade e dos avanços tecnológicos (CRESPO, 2011, p. 107). Contudo, há de se levar em consideração que nem todas as pessoas possuem o mesmo discernimento quanto às fraudes que podem ser cometidas em meio virtual, sobretudo as que não têm desenvoltura no trato com a *Internet* e outras tecnologias digitais.

O entendimento de Sydow (2015, p. 328), mais moderado, parece ser mais adequado, já que a apreciação das condutas dos internautas vitimados deve ter importância, e a análise *ex post* é que pode considerar a capacidade de cada usuário lesado frente ao ato sofrido. Essa ponderação poderia levar à atipicidade da conduta, em níveis extremos e em grau moderado, assumida pelo Direito brasileiro, que, por sua vez, poderá conduzir à redução da punibilidade do agente proporcionalmente ao descuido da vítima.

5 CONSIDERAÇÕES FINAIS

Conforme mencionado, o avanço da tecnologia e a popularização de dispositivos com acesso à *Internet* acarretaram um número maior de usuários da rede mundial de computadores, e esse número certamente se tornará cada vez mais elevado com o passar dos anos.

Contudo, um número maior de internautas significa uma cifra crescente de vítimas em potencial de crimes virtuais, especialmente os de fraude, que podem ganhar aspectos diversos, uma vez que as pessoas que praticam esse tipo de crime utilizam-se dos mais diversos artifícios para conseguir obter vantagens das suas vítimas, principalmente vantagens patrimoniais. As estratégias empregadas pelos criminosos vão das mais simples, como a abordagem em *sites* de relacionamentos através de perfis falsos, até a construção de páginas na *Internet* que imitam as de bancos ou lojas conceituadas.

O fato de a mídia alertar constantemente, bem como os sistemas operacionais, para os riscos inerentes à utilização de dispositivos informáticos faz com que determinadas medidas de segurança sejam, supostamente, conhecidas por todos os internautas. Ocorre que nem todos conhecem tais regras. Em verdade, uma parcela considerável dos usuários da *Internet* ignora as normas de segurança e termina por se tornar vítima de fraudes, cometidas das mais diversas maneiras.

Outra parcela de vítimas pode ter o autocontrole diminuído, conforme sugere pesquisa baseada na Teoria Geral da Vitimização, que constata ser maior sua exposição aos enganos utilizados pelos criminosos que se valem da *Internet*. Tal fragilidade requer uma proteção jurídica, e não o abandono do Direito Penal.

O pensamento dos doutrinadores alemães e espanhóis, quanto à possibilidade de exclusão de tipicidade quando a vítima deixa de tomar providências no resguardo e proteção de seus bens, deve ser visto com muita cautela. A não ser numa apreciação *ex post*, que revele ganância ou um total desleixo do lesado, seu comportamento deve apenas influir para o *quantum* de pena a ser aplicado.

REFERÊNCIAS

AGUSTINA, José R. Victimología y Victimodogmática en el uso de las TIC – Desfragmentación del yo em la era digital: “disinhibition effect”, esquizofrenia digital e

ingenuidad en ciberespacio. In: TAMARIT, Josep M.; PEREDA, Noemí (Coord.). *La respuesta de la Victimología ante las nuevas formas de victimizacion*. Madrid: Edisofer S.L., 2014. p. 109-157.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 24 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 2 jul. 2017.

BRITO, Auriney. *Direito Penal Informático*. São Paulo: Saraiva, 2013.

BUSTOS RAMÍREZ, Juan; PIJOAN, Elena Larrauri. *Victimología, presente y futuro*: hacia un sistema penal de alternativas. Barcelona: PPU, 1993.

CANCIO MELIÁ, Manuel. Reflexiones sobre la "victimodogmática" en la Teoría del Delito. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 25, p. 23-57, 1999.

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

GÁMEZ-GUADIX, Manuel; ORUE, Izakun; BORRAJO, Erica. Victimización y acoso a través de las nuevas tecnologías: características, prevalencia y prevención. In: TAMARIT, Josep M.; PEREDA, Noemí. (Coord.). *La respuesta de la Victimología ante las nuevas formas de victimizacion*. Madri: Edisofer S. L., 2014. p. 159-186.

LLINARES, Fernando Miro. El Cibercrimen fenomenología y criminología de la delincuencia en el ciberespacio. Madrid; Barcelona; Buenos Aires; São Paulo: Marcial Pons, 2012.

MINAHIM, Maria Auxiliadora. *Autonomia e frustração da tutela penal*. São Paulo: Saraiva, 2015.

NEUMAN, Elias. *Victimología*: el rol de la víctima en los delitos convencionales y no convencionales. Buenos Aires: Editorial Universidad, 2001.

NGO, Fawn T.; PATERNOSTER, Ray. Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, v. 5, p. 773-793, Jan./July 2011. Disponível em: <https://www.researchgate.net/publication/268410814_Cybercrime_Victimization_An_examination_of_Individual_and_Situational_level_factors>. Acesso em: 21 jul. 2017.

OXMAN, Nicolás. Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Cybercrime Through Internet: on the Accusation of "Phishing" and "Pharming". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, Chile, n. 41, p. 211-262, 2013. Disponível em: <www.scielo.cl/pdf/rdpucv/n41/a07.pdf>. Acesso em: 2 jul. 2017.

PARDO ALBIACH, Juan. Ciberacoso: cyberbullyng, grooming, redes socials y otros peligros. In: García González, Javier (Coord.). *Ciberacoso*: la tutela penal de la intimidad, la integridad y la libertad sexual em Internet. Valencia: Editorial Tirant Lo Blanch, 2010. p. 51-83.

PEREZ MARTÍNEZ, Ana; ORTIGOSA BLANCH, Reyes. Una aproximación al cyberbullying. In: García González, Javier (Coord.). *Ciberacoso:* la tutela penal de la intimidad, la integridad y la libertad sexual em Internet. Valencia: Editorial Tirant Lo Blanch, 2010. p. 13-49.

ROXIN, Claus. *La polémica en torno a la heteropuesta en peligro consentida. Sobre el alcance del princípio de autorresponsabilidad en Derecho Penal*. Madrid, 2012. Disponível em: <https://www.uam.es/otros/afduam/documentos/la%20polemica%20en%20torno%20a%20la%20heteropuesta%20en%20peligro%20consentida.pdf>. Acesso em: 24 mar. 2017.

SCHÜNEMANN, Bernd. *Temas actuales y permanentes del Derecho Penal después del milenio.* Madrid: Tecnos Ed., 2002.

SILVA, Carlos Bruno Ferreira. *Proteção de dados e cooperação transnacional*: teoria e prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes Editores, 2014.

SILVA SÁNCHEZ, Jesús María. *La Victimodogmática en el derecho extranjero*. 1990. Disponível em: <http://www.ehu.eus/documents/1736829/2030810/11+-+Victimodogmatica.pdf>. Acesso em: 23 mar. 2017.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2015.

VAN DIJK, Jan. Fraude en Internet: prevalencia por país e impacto en las víctimas. In: TAMARIT, Josep M.; PEREDA, Noemí. (Coords.). *La respuesta de la victimología ante las nuevas formas de victimizacion*. Madri: Edisofer S. L., 2014. p. 187-212.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes cibernéticos:* ameaças e procedimentos de investigação. 2.ed. Rio de Janeiro: Brasport, 2013.