
Curso de Direito

FRAUDE ELETRÔNICA: FURTO OU ESTELIONATO?
ELECTRONIC FRAUD: THEFT OR SWINDLE?

Lucas Levi Marceno da Silva¹, Carla Figueiredo Garcia Queiroz²,

1 Alunos do Curso de Direito

2 Professora mestre do Curso de Direito

RESUMO

Os crimes digitais são aqueles praticados na internet ou com auxílio de algum equipamento eletrônico. A prática de delitos no meio virtual é convidativa aos criminosos que estão migrando para o ambiente cibernético e adaptando suas práticas delituosas para a internet devido ao anonimato nas redes sociais. Nesse sentido, objetiva-se diferenciar crimes virtuais próprios e impróprios, bem como identificar a conduta de estelionato cibernético. A pesquisa sobre delitos praticados na internet será baseada em um estudo bibliográfico descritivo, com coletas de informações de artigos, livros e doutrinas, transcorrendo sobre fatos observados em decorrência do alto índice de crimes virtuais na sociedade. A problematização da pesquisa parte do questionamento sobre a diferença entre furto mediante fraude eletrônica e estelionato por fraude eletrônica. Assim, a análise da Lei 14.155/2021, além de refletir a preocupação com os crimes virtuais, majorando o estelionato digital, também contribui com a conscientização a respeito desse tema, para que estes crimes se tornem menos atrativos aos criminosos que acreditam que a internet é "terra sem lei".

Palavras-chave: estelionato virtual; furto mediante fraude eletrônica; Lei 14.155/2021.

ABSTRACT

Digital crimes are those committed on the Internet or with the aid of some electronic equipment. The practice of crimes in the virtual environment is inviting criminals who are migrating to the cyber environment and adapting their criminal practices to the internet due to anonymity on social networks. In this sense, it aims to differentiate their own and inappropriate virtual crimes. Well, with identifying the conduct of cyber swindle. The research on crimes committed on the Internet will be based on a descriptive bibliographic study, with information collection of articles, books and doctrines, based on facts observed as a result of the high rate of virtual crimes in society. The problematization of the research is part of the questioning about the difference between theft through electronic fraud and swindle for electronic fraud. Thus, the analysis of Law 14.155/2021, in addition to reflecting the concern with virtual crimes, majoring the digital swindle, also contributes to the awareness about this topic, so that these crimes become less attractive to criminals who believe that the internet is "land without law".

Keywords: virtual swindle; theft by electronic fraud; Law 14.155/2021.

INTRODUÇÃO

O presente trabalho tem como objeto de estudo A Lei 14.155 de 2021 que fez alterações nos crimes patrimoniais previstos no Código Penal, inserindo qualificadoras nos crimes de furto e de estelionato por fraude eletrônica.

Esse tema traz a problemática: qual a diferença entre o furto mediante fraude eletrônica e o estelionato por fraude eletrônica? O número de crimes cibernéticos tem crescido em grande escala, devido ao avanço da tecnologia, e o meio virtual parece

convidativo para criminosos devido a sensação de anonimato. Por esse motivo, existem pessoas que utilizam de nomes, contas ou páginas falsas, no ambiente virtual, para cometer crimes.

O estelionato cibernético é a fraude cometida com as informações fornecidas pela vítima ou por terceiros, mediante erro ocorrido por meio de redes sociais, contatos telefônicos ou envio de correio fraudulento.

Logo a pesquisa tem como objetivo geral: diferenciar crimes virtuais próprios e impróprios. Como objetivos específicos: diferenciar o estelionato cibernético de furto mediante fraude eletrônica e mostrar as sanções penais para estas modalidades. Para isso, a pesquisa foi bibliográfica descritiva, por meio da análise de livros, sites, artigos e revistas, utilizando a coleta de informações adquiridas de forma imparcial em face de um assunto que já possui determinada relevância para o mundo jurídico.

Esse tema é importante para apresentar a população brasileira, o qual faz utilização dos meios virtuais, os riscos que a tecnologia e as redes sociais tem apresentado no decorrer dos anos. Dessa forma, a internet não é uma “terra sem lei”, pois existe norma específica sobre o assunto, bem como delegacias especializadas para combate aos crimes virtuais. E a sensação de impunidade é falsa, pois existem meios para descobrir o autor do delito cibernético.

REFERENCIAL TEÓRICO

1. Crimes cibernéticos

Sabe-se que a Internet teve início em plena guerra fria, e foi utilizada como uma arma norte-americana de informação militar. E possuía como principal função interligar todas as centrais de computadores dos postos de comando estratégicos, fazendo com que os americanos, se prevenissem de um suposto ataque. Nos dias atuais, podemos notar que a Internet interliga milhões de computadores, e a mesma se tornou uma teia de aranha, contribuindo assim, para o acesso a todo tipo de informação e transferência de dados.

Nos últimos anos a informática passou a fazer parte do dia-a-dia da maioria da população mundial, e no Brasil não foi diferente, pois, a velocidade com que a tecnologia é criada é algo impressionante e inexplicável. Pode-se afirmar que são inúmeros os

benefícios da tecnologia, como o avanço nos setores de produção e a forma instantânea que as notícias chegam para todo o mundo. Todavia, a utilização, alcance e a praticidade da internet trouxeram muitos benefícios para a humanidade, mas também criou novas formas de criminosos atacarem suas vítimas através de crimes virtuais.

Atualmente a Lei 12.965 de 2014 conhecida como Marco Civil da Internet conceituou no seu artigo 5º, o termo internet como:

[...] sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. (BRASIL, 2014)

O crime virtual pode ser chamado de crime cibernético, crime tecnológico, ou crime no ambiente virtual. Estes crimes são caracterizados pela utilização dos meios eletrônicos para conseguir diversas vantagens indevidas sobre vítimas, que não precisam estar necessariamente próximas do sujeito ativo.

Para Barreto e Brasil (2016):

Os crimes tecnológicos são aqueles que envolvem o uso de tecnologias (computador, internet, caixas eletrônicos), sendo, em regra, crimes meios – ou seja, apenas a forma em que são praticados é que é inovadora. Têm como subespécie os crimes virtuais, informáticos ou cibernéticos (praticados pela internet), onde, apesar de se concretizarem em ambientes virtuais, os delitos trazem efeitos no mundo real. (BARRETO e BRASIL, 2016)

Esta modalidade de delito vem atraindo criminosos que encontraram na sensação de anonimato, o ponto motivador para a prática de crimes utilizando ferramentas informatizadas. Estes indivíduos veem no ambiente virtual a possibilidade de obter ganhos consideráveis em pouco tempo, e com mais segurança, seja pela falta de confrontos armados ou até mesmo pela atuação do Estado que é relativamente menor.

Existem crimes que utilizam a tecnologia apenas como ferramenta para atingir os seus objetivos, esses crimes já são conhecidos do Direito Penal e a internet apenas deu apoio para que as práticas delituosas obtivessem mais êxito, são os chamados crimes cibernéticos impróprios ou impuros. Os exemplos mais recorrentes são os crimes

contra a honra, a pedofilia, as ameaças, e os estelionatos, que de forma cada vez mais frequentes são praticados na internet. Inclusive, a tendência é que estes delitos migrem para ambiente virtual cada vez mais, tornando assim sua prática no mundo real como uma exceção à regra.

Para Vianna, (2003) os crimes cibernéticos impróprios são:

[...] aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa à bem jurídica inviolabilidade da informação automatizada (dados), como por exemplo, os crimes contra a honra (calúnia, injúria e difamação), praticados nas redes sociais ou através do envio de um e-mail. (VIANNA, 2003, p.13)

Assim, os crimes virtuais impróprios não precisam necessariamente da internet ou de qualquer dispositivo informático para sua consumação, no entanto, ele ocorre neste ambiente com frequência.

É importante notar que em nenhum destes delitos há qualquer ofensa à bem jurídica inviolabilidade das informações automatizadas, razão pela qual são considerados delitos informáticos impróprios. (VIANNA)

Já os crimes cibernéticos próprios ou puros, existem exclusivamente com apoio dos sistemas informáticos. Basicamente esses delitos necessariamente precisam violar o bem jurídico, “dados”, isto é, as informações automatizadas.

Para Barreto e Brasil (2016), estes podem ser conceituados como:

[...] aqueles em que os sistemas informatizados, bancos de dados, arquivo ou terminais (computadores, *smartphone*, *tablets*, por exemplo) são atacados pelos criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou, ainda, por engenharia social (golpista engana a vítima, fazendo com que forneça informações pessoais e/ou estratégicas). Aqui o dispositivo informatizado e/ou seu conteúdo é o alvo dos criminosos. (BARRETO e BRASIL, 2016)

Os crimes cibernéticos próprios geralmente possuem como sujeito ativo alguém com conhecimento um pouco mais técnico ou um acesso a informações importantes, a exemplo do funcionário ou servidor público que possui conhecimento acerca de dados sigilosos que transitam na sua rede de trabalho. Ademais, nessa

modalidade é bem comum a utilização de programas maliciosos como vírus de computador que facilitam o serviço.

Mas nem todos os crimes virtuais são praticados por hackers e experts da tecnologia. Atualmente têm crescido exponencialmente os golpes de WhatsApp e aplicativos de entrega, por exemplo, que costumam ter como suas principais vítimas pessoas comuns com pouco conhecimento de tecnologia. Os autores, nesses casos, usualmente são pessoas estado de reclusão, com fácil acesso a telefones mesmo dentro das unidades prisionais.

2. Lei 14.155/2021 e o estelionato cibernético

Em 2021, foi sancionado a Lei 14.155, que inseriu no Código Penal o artigo 154-A, o crime de Invasão de dispositivo informático:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

O crime de invasão de dispositivo informático é um crime cibernético puro ou próprio, pois trata de uma conduta, onde necessariamente precisa da internet, para obtenção de dados, no qual só se consuma no ambiente virtual.

Além disso, foi criado o crime de furto mediante fraude eletrônica e o estelionato com fraude eletrônica. Em 2021, a Lei 14.155 inseriu, no crime de furto, os parágrafos 4º-B e 4º-C, no artigo 155 do Código Penal:

Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
Pena - reclusão, de um a quatro anos, e multa.

[...]

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:

I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;

II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

O furto é um crime de ação penal pública incondicionada, basta registrar um boletim de ocorrência, para que o Ministério Público, por meio de um inquérito policial, possa oferecer a denúncia. O núcleo do tipo penal do furto é a subtração, ou seja, surrupiar, pegar escondido, sem o consentimento da vítima.

Contudo, o foco dos crimes virtuais é o furto qualificado pela fraude eletrônica, com a pena de 04 a 08 anos de reclusão. O furto mediante fraude, ocorre com a subtração do patrimônio da vítima que teve sua vigilância iludida pela fraude.

Essa mesma Lei inseriu os parágrafos 2º-A e 2º-B no artigo 171 do Código Penal, que cuidam de forma específica dos estelionatos ocorridos no ambiente virtual:

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, de quinhentos mil réis a dez contos de réis.

[...]

§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Pode-se dizer que o estelionato é um delito já conhecido no mundo real e que possui facilidade de aplicação na internet pela conhecida sensação de anonimato oferecida pela rede. E atualmente tem uma pena de 4 a 8 anos se ocorrer no mundo virtual. Para ocorrer o crime de estelionato, quem pratica, deve obrigatoriamente cometer o delito para obter vantagem ilícita para si ou outra pessoa, causar prejuízo a alguém e utilizar de artimanha induzindo a pessoa ao erro.

É um crime que, apesar da pena de reclusão, vem crescendo muito nos últimos tempos, principalmente no ambiente virtual devido ao aumento exponencial da tecnologia. Os requisitos para a caracterização do estelionato são: cometer o crime visando a obtenção de vantagem ilícita para si ou para outra pessoa; causar prejuízo a alguém; utilizar da artimanha para enganar; induzir alguém ao erro. Dessa forma, se não

estiverem presentes todos esses elementos na conduta criminosa, não existirá o crime de estelionato.

Além disso, por se tratar de um crime em que obrigatoriamente a intenção é lesar o outro, não se admite a modalidade culposa, apenas a dolosa. Como exemplos: cobrar por um serviço, receber o pagamento não o realizar; vender bijuteria afirmando se tratar de uma joia a fim de enganar a vítima; clonagem de Whatsapp, com artimanhas para persuadir a vítima a passar um código de verificação que chega por mensagem; e a nova modalidade de estelionato, o golpe do amor, também chamado de estelionato sentimental.

Ademais, com a alteração promovida pelo Pacote Anticrime (Lei 13.964/2019), o delito de estelionato passou a ser de ação penal pública condicionada à representação, ou seja, a vítima precisa dar a condição de procedibilidade para que o Ministério Público possa oferecer a denúncia contra o acusado.

Segundo Renato Brasileiro de Lima:

Isso significa que o Ministério Público permanece sendo o órgão responsável por promover a Ação Penal, todavia, para que possa exercer a função acusatória, passa a ter a condição de haver representação por parte da vítima ou seu representante legal, manifestando possuir interesse na persecução penal do autor do crime.

Sendo assim, a ausência de representação inviabilizará o início da Ação Penal por parte do Ministério Público.

Destarte, a Lei 14.155/2021 inseriu a fraude eletrônica em dois crimes patrimoniais, o furto e o estelionato. E em ambos os casos a pessoa é vítima de um golpe nas redes sociais. Logo a diferença está no núcleo do tipo penal dos referidos delitos, ou seja, no furto há a subtração do patrimônio, enquanto que no estelionato há a entrega do bem. Assim, quando a vítima entrar em uma página falsa do banco e fazer uma transação bancária, por meio da rede virtual fraudulenta, haverá a subtração, a retirada do patrimônio, o que caracteriza o furto mediante fraude eletrônica. E quando, a vítima por meio de um telefonema, whatsapp, confia seus dados, ou faz uma transferência bancária, um pix, achando que é para um amigo, para comprar algo na internet, ou para campanha de doação na rede social, nessa situação há a entrega do patrimônio por acreditar no embuste, o que caracteriza o estelionato pela fraude eletrônica, também conhecido por estelionato cibernético.

3. Prevenção ao estelionato virtual

Criminosos buscam a todo momento obter informações e dados acerca das vítimas, e a internet é um “prato cheio”, pois a todo o momento, no mundo inteiro, pessoas compartilham e guardam seus dados digitalmente. Todos os dias, as pessoas compram e vendem objetos e serviços, cadastram senhas, trocam mensagens, participam de grupos, acessam redes sociais e se utilizam de vários meios que, de alguma forma, armazenam suas informações pessoais. Todas essas formas de utilização da internet podem parecer inofensivas, mas, em muitos casos, oferecem riscos aos usuários, quando estes se deparam com pessoas mal-intencionadas.

Em uma reportagem passada no Jornal Primeiro Impacto (SBT), no Estado do Rio de Janeiro, o crime de estelionato virtual cresceu em média de 116% em relação ao ano de 2021, ficando somente atrás do crime de furto. Sendo possível afirmar que ocorre um caso, a cada 04 minutos. Ainda assim, há uma grande dificuldade na identificação dos criminosos, ficando evidente que a sociedade precisa de alterações na lei para coibir a prática de tais crimes.

Para que um crime digital seja investigado é necessário que a vítima junte todas as provas possíveis, como por exemplo, os prints de tela. A investigação é feita de forma técnica por meio de uma rede que interliga os computadores, tais computadores são achados através de um endereço IP, que é único para cada aparelho. E para isso, existem delegacias especializadas no combate aos crimes cibernéticos, que através de equipamentos e pessoal qualificado buscam identificar e combater tais criminosos. O objetivo destas delegacias é identificar o agente ativo e preservar quaisquer vestígios da materialidade da conduta, principalmente pelo fato de que, as provas presentes em ambiente virtual podem ser facilmente descartadas pelos criminosos ou até mesmo pela imperícia da vítima.

Essa fragilidade das provas nos crimes virtuais, muitas vezes, não produz eficientes resultados nas investigações criminais. Dessa maneira, existem dez passos para uma pessoa ter proteção nas compras on line, e não ser vítima do estelionato cibernético.

Primeiro, pesquisar a idoneidade da empresa. Conferir os dados comerciais da empresa de comércio eletrônico. Os canais de venda virtuais são obrigados a fornecer

dados como razão social, endereço, telefone e CNPJ, de preferência, em sua página principal. Desconfiar de sites que não seguem essa regra.

Segundo identificar as informações de contato. Quanto mais fácil localizar telefones, endereços e e-mail para entrar em contato com o comércio eletrônico, tirar dúvidas ou encaminhar problemas, mais confiável o site é, e menos provável de ser um golpe virtual. Alguns sites, inclusive, oferecem chat online pelo qual pode conversar com um atendente em tempo real.

Terceiro, ficar de olho na certificação digital. As lojas virtuais, que se preocupam com a segurança de seus clientes, buscam obter selos de segurança e certificações digitais. Conferir se a página inicial apresenta essa informação. Além disso, os endereços de sites de comércio eletrônico devem começar com “https” e não “http”.

Quarto, atentar para a qualidade dos textos. Procurar pistas de golpe no site. Erros de português e fotos de má qualidade são bons indícios de sites que não são idôneos, construídos de forma amadora e com a finalidade exclusiva de tirar dinheiro das pessoas.

Quinto, conhecer a reputação da empresa. Pesquisar o que as pessoas andam falando sobre a empresa. Sempre que estiver com o pé atrás com algum comércio eletrônico, consultar a idoneidade do site nos órgãos de proteção ao consumidor como o “Reclame Aqui”. O Procon, por exemplo, mantém uma lista das empresas que recomenda evitar. As redes sociais também são ótimas ferramentas para descobrir se existem reclamações em torno destes serviços e conhecer a opinião de outros consumidores. Nas *fanpages* das empresas no Facebook existem comentários de clientes e avaliações com estrelas. Além disso, pode ver se a empresa responde os comentários deixados pelo público e se ela se importa em resolver os problemas que são relatados.

Sexto, pedir indicações. Não pense duas vezes antes de pedir indicações de parentes e amigos, sobretudo daqueles que já têm o hábito de comprar pela internet.

Sétimo, ler a política do site. Essas informações são úteis para conhecer as medidas de segurança como também o sistema de trocas e devolução. Quanto mais confiança melhor será a compra e mais protegido estará o CPF.

Oitavo, utilizar wifi, computador ou smartphone seguros. Nunca fazer compras virtuais por meio de computadores de outras pessoas ou usando redes públicas de wi-fi. Isso só aumenta a chance de ação de pessoas mal-intencionadas.

Nono, fugir de promoções mirabolantes. Se um determinado produto está com o preço tentador, abaixo do mercado, deixar de comprar. Preços muito reduzidos podem ser sinal de tentativa de fraude.

Décimo, guardar os comprovantes das compras. Imprimir ou salvar no computador as telas que indicam que a compra foi realizada. Anotar códigos de confirmação e guardar e-mails com dados da transação, pois podem ser úteis no futuro.

CONSIDERAÇÕES FINAIS

Os cibercrimes, como também são chamados, são as infrações penais que acontecem no ambiente virtual. O estelionato cibernético se tornou algo muito comum em nossa sociedade e muitas pessoas sofrem com a falta de segurança e orientação. As formas que são aplicadas estes golpes são; Ligação premiada, Envelope de banco vazio, Anúncio de veículo, são alguns dos golpes registrados no território brasileiro. As histórias são as mais diversas, como falsos sorteios e promoções, sobrinho distante que está a caminho da cidade e precisa de dinheiro para consertar o carro na estrada e até confirmação de resgate de carro roubado. Os golpes normalmente são aplicados por quem está atrás das grades.

Para se proteger, o cidadão precisa tomar alguns cuidados, como obter informações sobre a tal da premiação, ligar para os parentes antes de enviar qualquer tipo de dado e em hipótese alguma, depositar o dinheiro, que ocorre pedidos nas redes sociais. Em premiações que você não está participando, não tem como ganhar. Em caso de empréstimos via rede sociais oferecidas, verifique o serviço buscando informações concretas e sempre buscar ajuda especializada, excepcionalmente da polícia.

A criação de novos tipos penais é algo cotidiano nos dias atuais, considerando que quase toda conduta fraudulenta praticada em meio virtual se encaixa a um crime já existente. A atuação legislativa, portanto, tem sido no sentido de endurecimento de penas, criando causas de aumento da penalidade e formas qualificadas de crimes, quando praticados em ambiente cibernético.

A lei 14.155, de 27 de maio de 2021, acrescentou e alterou alguns artigos do Código Penal. A referida Lei acrescentou o crime de invasão de dispositivo informático e acrescentou a fraude eletrônica nos crimes patrimoniais de furto e estelionato.

A fraude eletrônica é um requisito para ambos os crimes, a diferença está na conduta, pois no furto a fraude é utilizada para iludir a vítima e poder subtrair seu patrimônio pelo meio eletrônico. E no estelionato a fraude é utilizada para enganar a vítima, para que a mesma pague algo, ou entregue seu patrimônio, de forma iludida, usando as redes sociais.

O uso da internet e das redes sociais, se tornou algo de fácil manuseio, e essa simplicidade na utilização, juntamente com o anonimato que a rede possibilita, são os principais incentivos para os criminosos. Porém, com alguns cuidados, como verificar o site, a origem da informação, pode-se evitar o estelionato cibernético.

REFERÊNCIAS

BRASIL. Código Penal: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm>.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2019-2022/2021/lei/L14155.htm.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. 1. ed. São Paulo: Brasport, 2016.

LIMA, Renato Brasileiro. Estelionato e representação da vítima. Ministério Público do Estado do Paraná. Centro de apoio operacional das promotorias criminais. Disponível em: https://criminal.mppr.mp.br/arquivos/File/Estudo_-_Estelionato_e_representacao_da_vitima_versao_final.pdf

O IMPACTO. Jorna eletrônico. Crimes virtual: proteja-se contra os principais golpes. Disponível em: <https://oimpacto.com.br/2022/02/06/crime-virtual-proteja-se-contra-os-principais-golpes/>



VIANNA, Túlio Lima. Fundamentos de direito penal informático. 1. ed. Rio de Janeiro: Forense, 2003.